Corso di Specializzazione Professionale

Esperto in Sicurezza Urbana, Sistemi di Videosorveglianza e Tecniche Investigative di Indagine

Sulla Gazzetta Ufficiale n. 61 del 14/03/2018 è stato pubblicato il **Decreto del Presidente della Repubblica n. 15 del 15/01/2018**, recante "*Regolamento a norma dell'articolo 57 del Decreto Legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia*", in vigore dal 29/03/2018.

Tale decreto è stato adottato in virtù dell'art. 57 del D. Lgs. n. 196 del 30 giugno 2003 (c.d. Codice della privacy) che prevede che vengano individuate le modalità di attuazione del trattamento dei dati effettuato per le finalità di polizia dal Centro elaborazioni dati e da organi, uffici o comandi di polizia. L'art. 57 del Codice privacy prevede l'adozione di specifico decreto che individua le modalità di trattamento dei dati personali per finalità di polizia che ai sensi dell'art. 53 del Codice. Ne deriva che il regolamento non riguarda i trattamenti effettuati per finalità amministrative.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 3

Il decreto ha lo scopo di riguardare:

- il principio secondo cui la raccolta dei dati è correlata alla specifica finalità perseguita, in relazione alla prevenzione di un pericolo concreto o alla repressione di reati;
- l'aggiornamento periodico dei dati, le diverse modalità relative ai dati trattati senza l'ausilio di strumenti elettronici e le modalità per rendere conoscibili gli aggiornamenti da parte di altri organi e uffici cui i dati sono stati in precedenza comunicati;

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 4

- i presupposti per effettuare trattamenti per esigenze temporanee o collegati a situazioni particolari e l'individuazione delle categorie di interessati e la conservazione separata da altri dati che non richiedono il loro utilizzo;
- l'individuazione di specifici termini di conservazione dei dati in relazione alla natura dei dati o agli strumenti utilizzati per il loro trattamento;
- la comunicazione ad altri soggetti, la loro diffusione;
- l'uso di particolari tecniche di elaborazione e di ricerca delle informazioni, anche mediante il ricorso a sistemi di indice.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 5

Viene sancito il divieto alla raccolta e al trattamento dei dati sulle persone per il solo fatto della loro origine razziale o etnica (inclusi quelli genetici e biometrici), la fede religiosa, l'opinione politica, l'orientamento sessuale, lo stato di salute, le convinzioni filosofiche o di altro genere, l'adesione a movimenti sindacali.

Il trattamento di tale particolare categoria di dati è consentito unicamente qualora vi siano esigenze correlate ad attività informative, di sicurezza, o di indagine di polizia giudiziaria o di tutela dell'ordine e della sicurezza pubblica, ad integrazione di altri dati personali.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 6

Vengono disciplinati :

- i casi in cui è consentita la comunicazione dei dati tra Forze di polizia,
- i casi in cui i dati raccolti possono essere condivisi e trasmessi a pubbliche amministrazioni o enti pubblici e ai privati. In pratica tale possibilità viene circoscritta alle situazioni in cui la comunicazione delle informazioni è supportata dall'esigenza di evitare pericoli gravi e imminenti alla sicurezza pubblica e di assicurare lo svolgimento dei compiti istituzionali per le finalità di polizia.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 7

SISTEMI DI VIDEOSORVEGLIANZA, RIPRESA FOTOGRAFICA, VIDEO AUDIO

L'art. 22 del D.P.R. n. 15/2018 tratta in modo particolare dei sistemi di videosorveglianza, di ripresa fotografica, video e audio. L'utilizzo di questa tecnologia per finalità di polizia è dato per assodato a condizione che non comporti una ingerenza ingiustificata nei diritti e nelle libertà fondamentali.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 8

Occorre però prestare particolare attenzione in quanto molti impianti oggi esistenti, **essendo di proprietà comunale potrebbero non essere annoverati all'interno di tale possibilità** *(pur essendo di norma le polizie locali un apparato con poteri di vigilanza e presidio)*, ad eccezione dei casi in cui **l'amministrazione abbia sottoscritto un patto per la sicurezza urbana integrata** e **disciplinato l'utilizzo di tali sistemi all'interno di esso**.

A tal proposito sarà molto interessante osservare l'imminente recepimento della Direttiva Ue 2016/680 che riguarda i dati trattati dalle pubbliche amministrazioni ai fini di prevenzione, accertamento e perseguimento dei reati.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 9

L'utilizzo delle immagini sicuramente consentito per finalità di polizia, quando necessario per documentare specifiche attività preventive e repressive di reati

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 10

Una particolare attenzione è stata posta dal legislatore relativamente alla **diffusione** di dati ed immagini prevedendo tale possibilità solo nei casi in cui sia necessaria per le finalità di polizia, fermo restando il rispetto degli obblighi di segretezza e, in ogni caso, con modalità tali da preservare la dignità della persona interessata. In buona sostanza, il regolamento consente la diffusione solo se la persona ha espresso il proprio consenso o se è necessario per la salvaguardia della vita o dell'incolumità fisica ovvero se è giustificata da necessità di giustizia o di polizia.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 11

Vengono individuati specifici termini massimi di conservazione dei dati, quantificandoli in relazione a distinte categorie

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 12

Tali termini sono aumentati di due terzi quando i dati personali sono trattati nell'ambito di attività preventiva o repressiva relativa ai reati di criminalità organizzata, con finalità di terrorismo e informatici.

Decorsi i termini di conservazione fissati, i dati personali, se soggetti a trattamento automatizzato, sono cancellati o resi anonimi (diritto all'oblio)

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 13

Continuano invece ad essere disciplinati dalle disposizioni sullo scarto dei documenti d'archivio delle PP.AA. i dati non soggetti a trattamento automatizzato.

Infine viene introdotta la facoltà per la persona interessata di chiedere la conferma dell'esistenza di dati personali che la riguardano, la loro comunicazione in forma intelligibile, l'aggiornamento, rettifica, cancellazione, blocco o trasformazione in forma anonima dei dati trattati in violazione di vigenti disposizioni di legge o di regolamento

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 14

COMUNICAZIONE DEI DATI TRA FORZE DI POLIZIA

L'art. 12 del regolamento disciplina unicamente la comunicazione dei dati tra forze di polizia comprese nella Legge 121/1981 non considerando le polizie locali e non allineandosi agli indirizzi legislativi contenuti nel D.L. 14/2017 convertito nella Legge n. 48/2017.

L'art. 9 disciplina la possibilità per gli organi di polizia di acquisire dati collegandosi alle banche dati pubbliche e private estranee alle forze dell'ordine. In tale disciplina rientrano i varchi di lettura targhe in dotazione alla polizia locale ad ai comuni.

DPR 15/01/2018, n. 15

Art. 12 Comunicazione dei dati tra Forze di polizia

1. La comunicazione dei dati tra organi, uffici e comandi delle Forze di polizia di cui all'articolo 16 della legge n. 121 del 1981, **per le finalità di polizia di cui all'articolo 3, è consentita quando è necessaria per lo svolgimento dei compiti istituzionali, fermi restando gli obblighi di segretezza che incombono sugli ufficiali e agenti di polizia giudiziaria** in relazione alle indagini svolte, come stabilito dal codice di procedura penale.

DPR 15/01/2018, n. 15 - Art. 3 Finalità dei trattamenti

1. I trattamenti di dati personali si intendono effettuati per le finalità di polizia, ai sensi dell'articolo 53 del Codice, **quando sono direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati.**

2. E' compatibile con le finalità di polizia, di cui al comma 1, l'ulteriore trattamento, ai sensi dell'articolo 99 del Codice, per finalità storiche, scientifiche e, previa trasformazione in forma anonima, per finalità statistiche, anche per le esigenze di analisi dei fenomeni criminali e dei risultati dell'azione di contrasto al crimine, nonché dell'attività di tutela dell'ordine e della sicurezza pubblica.

3. Il trattamento dei dati personali per le finalità storiche e scientifiche di cui al comma 2 è consentito ai soli operatori a ciò abilitati e designati, incaricati del trattamento secondo profili di autorizzazione predefiniti.

Sui tempi per la conservazione dei dati per finalità di polizia il dispositivo risulta molto flessibile, in conformità alle diverse esigenze investigative in atto. Per l'attivazione di tali collegamenti gli organi, uffici e comandi di polizia possono avvalersi, ai sensi dell'art. 54 del Codice, di **convenzioni** sottoscritte sulla base di schemi adottati dal Ministero dell'interno, su conforme parere del Garante.

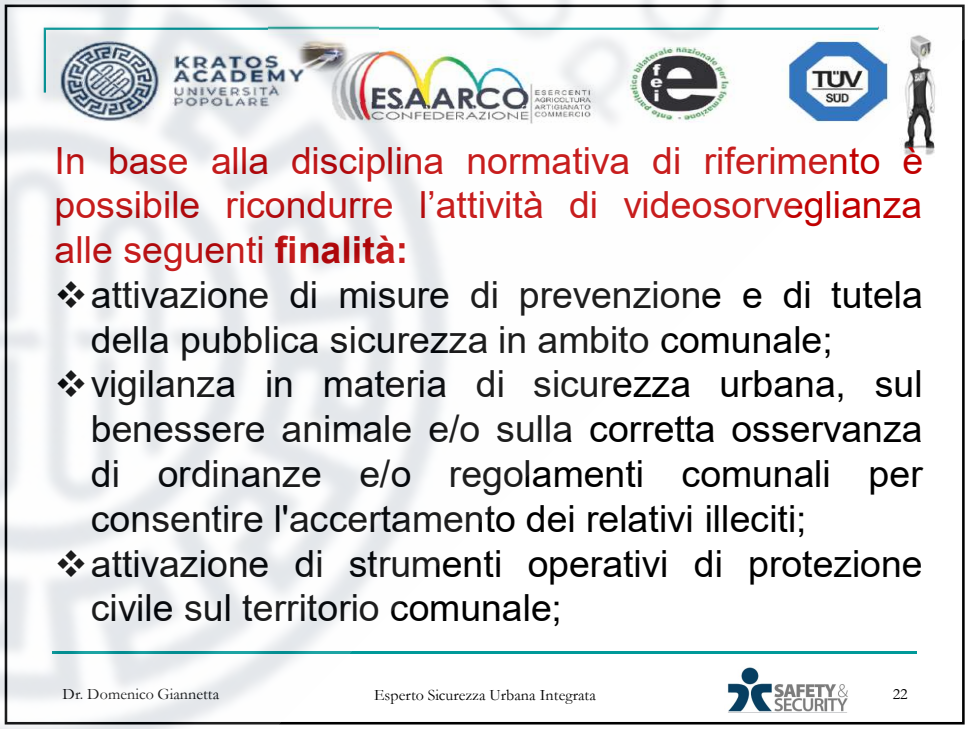
NON SI APPLICA ALLA POLIZIA LOCALE

- Il DPR fa riferimento espresso all'art. 53 del Dlgs 196/2003 che riguarda il "trattamento di dati personali effettuato dal Centro elaborazione dati del Dipartimento di pubblica sicurezza o da forze di polizia;
- La Polizia locale NON fa parte della definizione tecnica di "forze di polizia" (art. 3 Legge 07/03/1986, n. 65);
- Il regolamento non si applica ai trattamenti di dati personali effettuati per finalità amministrative.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 19

La risposta decisiva viene dal GARANTE PRIVACY che nel «Parere su uno schema di D.P.R. ai sensi dell'art. 57 del Codice, in tema di modalità attuative dei principi di protezione dei dati personali relativamente ai trattamenti effettuati per finalità di polizia da Organi, Uffici e Comandi di polizia – 02/03/2017» dice :
Lo schema di D.P.R., quindi, non si applica direttamente ai trattamenti effettuati, ad esempio, dalle Prefetture, dagli uffici dell'Agenzia delle Dogane, ecc., difettando per essi l'attributo "di polizia" né alla polizia municipale, cui l'articolo 1 della legge 7 marzo 1986, n. 65, recante «Legge-quadro sull'ordinamento della polizia municipale», attribuisce il compito istituzionale di «svolgere funzioni di polizia locale». Tale "funzione di polizia locale", prosegue la relazione illustrativa, in base alle disposizioni legislative (art. 159, d.lgs. 112 del 1998) e costituzionali (art. 117, comma 1, lett. h, Cost.) e anche alle indicazioni offerte dalla Corte Costituzionale, sarebbe riconducibile ad attività meramente amministrative, finalizzate ad assicurare l'osservanza di norme pubblicistiche collocate in materie di competenza regionale (sanità, turismo, ecc.).
La "polizia amministrativa locale" (polizia sanitaria, polizia urbanistica, ecc.), quindi, si esplica con lo svolgimento di attività non assimilabili affatto al mantenimento dell'ordine pubblico e della sicurezza in senso stretto e di prevenzione dei reati, la quale, al contrario, contraddistingue l'attività delle forze di polizia (ex articolo 16 della legge n. 121 del 1981), svolta sotto la guida del Ministero dell'interno".


Quale è quella vera?
Sistemi di videosorveglianza e di ripresa fotografica, audio e video
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
21


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
In base alla disciplina normativa di riferimento è possibile ricondurre l'attività di videosorveglianza alle seguenti **finalità:**
❖attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale;
❖vigilanza in materia di sicurezza urbana, sul benessere animale e/o sulla corretta osservanza di ordinanze e/o regolamenti comunali per consentire l'accertamento dei relativi illeciti;
❖attivazione di strumenti operativi di protezione civile sul territorio comunale;
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
22

- verifica del rispetto degli accessi in zone a traffico limitato e corsie riservate;
- rilevazione delle infrazioni al codice della strada;
- monitoraggio della circolazione stradale al fine di intervenire prontamente per prevenire ingorghi o blocchi del traffico;
- tutela della sicurezza urbana;
- promozione turistica o pubblicitaria anche con l'utilizzo di webcam o camera on-line.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 23

L'**art. 22 del D.P.R. n. 15 del 15/01/2018** tratta in modo particolare dei sistemi di videosorveglianza, di ripresa fotografica, video e audio, stabilendo che:

"L'utilizzo di sistemi di videosorveglianza è consentito ove ***necessario per le finalità di polizia di cui all'articolo 3*** *e* ***a condizione che non comporti un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali delle persone interessate****.*
Gli organi, uffici e comandi di polizia, nel rispetto dei principi richiamati dagli articoli 4, 5 e 6, raccolgono solo i dati strettamente necessari per il raggiungimento delle finalità di cui all'articolo 3, ***registrando esclusivamente le immagini indispensabili.****"*

Sul punto giova dunque evidenziare che **sul territorio comunale possono essere installati sistemi integrati, sistemi intelligenti e sistemi per rilevare le violazioni al C.d.S.**

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 24

Art. 3 - Finalità dei trattamenti

1. I trattamenti di dati personali si intendono effettuati per le finalità di polizia, ai sensi dell'articolo 53 del Codice, **quando sono direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati.**
2. E' compatibile con le finalità di polizia, di cui al comma 1, l'ulteriore trattamento, ai sensi dell'articolo 99 del Codice, per finalità storiche, scientifiche e, previa trasformazione in forma anonima, per finalità statistiche, anche per le esigenze di analisi dei fenomeni criminali e dei risultati dell'azione di contrasto al crimine, nonché dell'attività di tutela dell'ordine e della sicurezza pubblica.
3. Il trattamento dei dati personali per le finalità storiche e scientifiche di cui al comma 2 è consentito ai soli operatori a ciò abilitati e designati, incaricati del trattamento secondo profili di autorizzazione predefiniti.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 25

D.Lgs. 30 giugno 2003, n. 196

Art. 53 Ambito applicativo e titolari dei trattamenti

1. Al trattamento di dati personali effettuato dal Centro elaborazione dati del Dipartimento di pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento, non si applicano le seguenti disposizioni del codice:
a) artt. 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5 e da 39 a 45;
b) artt. da 145 a 151.
2. Con decreto del Ministro dell'interno sono individuati, nell'allegato C) al presente codice, i trattamenti non occasionali di cui al comma 1 effettuati con strumenti elettronici, e i relativi titolari.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 26

I sistemi integrati collegano telecamere tra soggetti diversi, sia pubblici che privati, o che consentono la fornitura di servizi di videosorveglianza "in remoto" da parte di società specializzate (es. società di vigilanza, Internet providers) mediante collegamento telematico ad un unico centro, sono obbligatorie specifiche misure di sicurezza (es. contro accessi abusivi alle immagini).

È NECESSARIA LA VERIFICA PRELIMINARE DEL GARANTE!

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 27

I sistemi intelligenti sono dotati di software che permettono l´associazione di immagini a dati biometrici (es. riconoscimento facciale) **o in grado, ad esempio, di riprendere e registrare automaticamente comportamenti o eventi anomali e segnalarli** (es. motion detection).

È NECESSARIA LA VERIFICA PRELIMINARE DEL GARANTE!

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 28

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

2. TRATTAMENTO DEI DATI PERSONALI E VIDEOSORVEGLIANZA: PRINCIPI GENERALI

La raccolta, la registrazione, la conservazione e, in generale, l´utilizzo di immagini configura un trattamento di dati personali (art. 4, comma 1, lett. b), del Codice).

È considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 29

Le immagini costituiscono dati personali

«Invero, **non appare possibile dubitare del fatto che l'immagine costituisca dato personale rilevante ai sensi dell'art. 4 comma 1 lett b) del D Lgs n 196 2003 trattandosi di dato immediatamente idoneo ad identificare una persona, a prescindere dalla sua notorietà.** Del resto, già questa Corte (Cassazione n 14346 2012 ha affermato che «non può dubitarsi, nonostante in dottrina sia stato sollevato qualche dubbio al riguardo, che anche l'immagine di una persona, in sé considerata, quando in qualche modo venga visualizzata o impressa, possa costituire "dato personale" ai sensi dell'art 4 lett b), del d lgs n 196 del 2003 noto anche come «codice privacy». In tal senso, invero, depongono specifiche decisioni del Garante per la protezione di dati personali 21 ottobre 1999 4 ottobre 2007 18 giugno 2009 n 1623306 nonché la decisiva circostanza della previsione, nell'ambito del codice privacy, di una specifica norma (art 134 in materia di videosorveglianza»

Corte di Cassazione, Sezione II civile, 2 settembre 2015 n .17440

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 30

La videosorveglianza in ambito pubblico

Il Garante è stato più volte chiamato a pronunciarsi in merito al trattamento di dati personali effettuato tramite sistemi di videosorveglianza in ambito pubblico. Tra i molteplici chiarimenti forniti, si segnalano quelli riguardanti le modalità di installazione di impianti di videosorveglianza all'interno di centri abitati da parte dei comuni, in particolare in relazione agli impianti volti a contrastare l'abbandono incontrollato di rifiuti urbani attraverso i dispositivi denominati foto trappola (predisposti per rilevare delle immagini solo al verificarsi di condizioni predefinite)

In proposito, è stato evidenziato che, **a fronte dell'inefficacia di strumenti e sistemi di controllo alternativi, l'utilizzo di impianti di videosorveglianza risulta lecito anche per accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose nonché per monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente** (cfr art 13 l 24 novembre 1981 n 689 e punto 5 2 provv 8 aprile 2010 doc web n 1712680. In questo ambito, un caso oggetto di segnalazione ha riguardato la presunta assenza di informativa rispetto ad un sistema di videosorveglianza collocato in un piazzale per controllare il regolare deposito dei rifiuti. Dalle informazioni acquisite, è risultato che il cartello recante l'informativa era stato collocato, in modo ben visibile anche durante le ore notturne, a qualche decina di metri dall'area interessata dal raggio di azione della telecamere e pertanto il trattamento dei dati è stato ritenuto conforme alla disciplina in materia di protezione dei dati personali.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 31

È stato evidenziato che **il supporto con l'informativa non deve essere necessariamente collocato a stretto contatto con gli impianti, ma nelle sue immediate vicinanze e comunque, prima dell'area interessata dalle riprese** (cfr punto 3 1 del citato provvedimento generale)

In casi come quello descritto, anche quando il sistema di videosorveglianza è impiegato per la prevenzione dei reati ambientali (riconducibile all'ambito applicativo dell'art 53 del Codice e per ciò stesso quindi esonerato dall'obbligo di informativa), **si è ritenuto di raccomandare agli enti pubblici di collocare comunque i cartelli contenenti l'informativa perché rendere palese l'utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una ulteriore ed efficace funzione di deterrenza, oltre quelle specificamente perseguite** (cfr punto 3 1 2 del provvedimento generale)generale)(nota 18 gennaio 2017 Garante Privacy Relazione annuale attività 2017

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 32

Violazione degli obblighi d'informativa

«Rilevato che il Consorzio di Polizia Locale Valle Agno, sulla base delle considerazioni sopra richiamate, **ha effettuato un trattamento di dati personali ai sensi dell'art 4 comma 1 lett a) e b), del Codice, per mezzo di un sistema di videosorveglianza mobile in assenza dell'informativa di cui all'art 13**

ORDINA

Al Consorzio di Polizia locale Valle Agno con sede in Valdagno (Corso Italia n 63 / in

persona del legale rappresentante protempore, di pagare la somma di **euro 10.400,00 a titolo di sanzione amministrativa pecuniaria** per le violazioni indicate in motivazione»

INGIUNGE

Al medesimo di pagare la somma di euro 10.400,00 secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art 27 della legge n 689 81 »

Garante Privacy Ordinanza di ingiunzione 9 novembre 2017 Registro dei provvedimenti n 466 del 9 novembre 2017

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 33

Violazione degli obblighi d'informativa

«Rilevato che il Comune di Reggio Emilia ha quindi effettuato un trattamento di dati personali (art 4 comma 1 lett a) e b) del Codice) omettendo di rendere l´informativa di cui all´art 13 del Codice, nella forma semplificata prevista dal provvedimento in materia di videosorveglianza datato 8 aprile 2010

Visto l ´ art 161 del Codice, che punisce la violazione dell´art 13 del medesimo Codice con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro,

Considerato che, ai fini della determinazione dell´ammontare della sanzione pecuniaria, occorre tenere conto, ai sensi dell´art 11 della legge n 689 81 dell´opera svolta dall´agente per eliminare o attenuare le conseguenze della violazione, della gravità della violazione, della personalità e delle condizioni economiche del contravventore e che pertanto l ´ ammontare della sanzione pecuniaria deve essere quantificato nella misura di euro 2 400 00

ORDINA

Al Comune di Reggio Emilia Comando Polizia municipale, in persona del legale rappresentante pro tempore, di pagare la somma di euro 2 400 00 a titolo di sanzione amministrativa pecuniaria per la violazione prevista dall ´ art 161 del Codice indicata in motivazione

INGIUNGE

Al medesimo Comune di pagare la somma di euro 2 400 00 secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l ´ adozione dei conseguenti atti esecutivi a norma dall ´ art 27 della legge n 689 81 prescrivendo che, entro il termine di giorni 10 (dal versamento, sia inviata a questa Autorità, in originale o in copia autentica, quietanza dell ´ avvenuto versamento»

Garante Privacy Ordinanza di ingiunzione 30 gennaio 2014 Registro dei provvedimenti n 43 del 30 gennaio 2015

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 34

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Un´analisi non esaustiva delle **principali applicazioni** dimostra che la videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti **ambiti generali**:

1. **protezione e incolumità degli individui**, ivi ricompresi i profili attinenti alla sicurezza urbana, all´ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;
2. **protezione della proprietà**;
3. **rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici,** nel quadro delle competenze ad essi attribuite dalla legge;
4. **acquisizione di prove.**

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

La necessità di garantire, in particolare, un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, purché ciò non determini un´ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati. Naturalmente l´installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell´ordinamento applicabili, quali ad es. le vigenti norme dell´ordinamento civile e penale in materia di interferenze illecite nella vita privata, sul controllo a distanza dei lavoratori, in materia di sicurezza presso stadi e impianti sportivi, o con riferimento a musei, biblioteche statali e archivi di Stato, in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali e, ancora, nell´ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell´ambito delle linee di trasporto urbano.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

In tale quadro, pertanto, è necessario che:

a) il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici da un lato (svolgimento di funzioni istituzionali: artt. 18-22 del Codice) e, dall´altro, per soggetti privati ed enti pubblici economici (es. adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi" -v., in proposito, punto 6.2.- o consenso libero ed espresso: artt. 23-27 del Codice). Si tratta di presupposti operanti in settori diversi e che sono pertanto richiamati separatamente nei successivi paragrafi del presente provvedimento relativi, rispettivamente, all´ambito pubblico e a quello privato;

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

b) ciascun sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., configurando il programma informatico in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone). Lo impone il principio di necessità, il quale comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l´utilizzazione di dati personali (art. 3 del Codice);

c) l´attività di videosorveglianza venga effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (art. 11, comma 1, lett. d) del Codice).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3. ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI

3.1. Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).

A tal fine, il Garante ritiene che si possa utilizzare lo stesso **modello semplificato di informativa "minima",** indicante il titolare del trattamento e la finalità perseguita, già individuato ai sensi dell´art. 13, comma 3, del Codice nel provvedimento del 2004 e riportato in fac-simile nell´allegato n. 1 al presente provvedimento.

Il modello è ovviamente adattabile a varie circostanze. In presenza di più telecamere, in relazione alla vastità dell´area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

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.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Il Garante ritiene auspicabile che l´informativa, resa in forma semplificata avvalendosi del predetto modello, poi rinvii a un testo completo contenente tutti gli elementi di cui all´art. 13, comma 1, del Codice, disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, messaggi preregistrati disponibili digitando un numero telefonico gratuito). In ogni caso **il titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un´informativa adeguata, contenente gli elementi individuati dall´art. 13 del Codice.**

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 41

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3.1.1. Informativa e sicurezza

Talune disposizioni del Codice, tra le quali quella riguardante l´obbligo di fornire una preventiva informativa agli interessati, **non sono applicabili al trattamento di dati personali effettuato**, anche sotto forma di suoni e immagini, dal "Centro elaborazione dati del Dipartimento di pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell´ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento" (art. 53 del Codice).

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 42

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Alla luce di tale previsione del Codice, i predetti titolari del trattamento di dati personali devono osservare i seguenti principi:

a) l´informativa può non essere resa quando i dati personali sono trattati per il perseguimento delle finalità di tutela dell´ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati;

b) il trattamento deve comunque essere effettuato in base ad espressa disposizione di legge che lo preveda specificamente.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3.1.2. Ulteriori specificazioni: l´informativa eventuale nella videosorveglianza effettuata per finalità di tutela dell´ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati

Il Garante, al fine di rafforzare la tutela dei diritti e delle libertà fondamentali degli interessati, ritiene fortemente auspicabile che l´informativa, benché non obbligatoria, laddove l´attività di videosorveglianza sia espletata ai sensi dell´art. 53 del Codice, sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati.

Ciò naturalmente all´esito di un prudente apprezzamento volto a verificare che l´informativa non ostacoli, ma anzi rafforzi, in concreto l´espletamento delle specifiche funzioni perseguite, tenuto anche conto che rendere palese l´utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una efficace funzione di deterrenza.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

A tal fine i titolari del trattamento possono rendere nota la rilevazione di immagini tramite impianti di videosorveglianza attraverso forme anche semplificate di informativa, che evidenzino, mediante l´apposizione nella cartellonistica di riferimenti grafici, simboli, diciture, l´utilizzo di tali sistemi per finalità di tutela dell´ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. In ogni caso resta fermo che, anche se i titolari si avvalgono della facoltà di fornire l´informativa, resta salva la non applicazione delle restanti disposizioni del Codice tassativamente indicate dall´art. 53, comma 1, lett. a) e b). Va infine sottolineato che deve essere obbligatoriamente fornita un´idonea informativa in tutti i casi in cui, invece, i trattamenti di dati personali effettuati tramite l´utilizzo di sistemi di videosorveglianza dalle forze di polizia, dagli organi di pubblica sicurezza e da altri soggetti pubblici non siano riconducibili a quelli espressamente previsti dall´art. 53 del Codice (es. utilizzo di sistemi di rilevazioni delle immagini per la contestazione delle violazioni del Codice della strada).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Principi generali

- **Informativa:** i cittadini che transitano nelle aree sorvegliate devono essere informati con cartelli della presenza delle telecamere, i cartelli devono essere resi visibili anche quando il sistema di videosorveglianza è attivo in orario notturno. Nel caso in cui i sistemi di videosorveglianza installati da soggetti pubblici e privati (esercizi commerciali, banche, aziende etc.) siano collegati alle forze di polizia è necessario apporre uno specifico cartello (allegato n. 2), sulla base del modello elaborato dal Garante. Le telecamere installate a fini di tutela dell´ordine e della sicurezza pubblica non devono essere segnalate, ma il Garante auspica comunque l´utilizzo di cartelli che informino i cittadini.
- **Conservazione:** le immagini registrate possono essere conservate per periodo limitato e fino ad un massimo di 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a indagini. Per attività particolarmente rischiose (es. banche) è ammesso un tempo più ampio, che non può superare comunque la settimana. Eventuali esigenze di allungamento dovranno essere sottoposte a verifica preliminare del Garante.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3.1.3 Informativa da parte dei soggetti privati che effettuano collegamenti con le forze di polizia

I trattamenti di dati personali effettuati da soggetti privati tramite sistemi di videosorveglianza, direttamente collegati con le forze di polizia, esulano dall´ambito di applicazione dell´art. 53 del Codice. Pertanto, **l´attivazione del predetto collegamento deve essere reso noto agli interessati.** A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia- individuato ai sensi dell´art. 13, comma 3, del Codice e riportato in fac-simile nell´allegato n. 2 al presente provvedimento. Nell´ambito del testo completo di informativa reso eventualmente disponibile agli interessati, tale collegamento deve essere reso noto.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Al predetto trattamento si applicano le prescrizioni contenute nel punto 4.6.

La violazione delle disposizioni riguardanti l´informativa di cui all´art. 13, consistente nella sua omissione o inidoneità (es. laddove non indichi comunque il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia), è punita con la sanzione amministrativa prevista dall´art. 161 del Codice.

Le diverse problematiche riguardanti le competenze attribuite ai comuni in materia di sicurezza urbana sono esaminate al punto 5.1.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3.2. Prescrizioni specifiche

3.2.1. Verifica preliminare

I trattamenti di dati personali nell´ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti da questa Autorità come esito di una verifica preliminare attivata d´ufficio o a seguito di un interpello del titolare (art. 17 del Codice), quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare.

In tali ipotesi devono ritenersi ricompresi i sistemi di raccolta delle immagini associate a dati biometrici. L´uso generalizzato e incontrollato di tale tipologia di dati può comportare, in considerazione della loro particolare natura, il concreto rischio del verificarsi di un pregiudizio rilevante per l´interessato, per cui si rende necessario prevenire eventuali utilizzi impropri, nonché possibili abusi.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

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.

Un analogo obbligo sussiste con riferimento a sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell´interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza (artt. 3 e 11 del Codice).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Deve essere sottoposto a verifica preliminare l´utilizzo di sistemi integrati di videosorveglianza nei casi in cui le relative modalità di trattamento non corrispondano a quelle individuate nei punti 4.6. e 5.4. del presente provvedimento.
Ulteriori casi in cui si rende necessario richiedere una verifica preliminare riguardano l´allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di sette giorni derivante da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell´autorità giudiziaria o di polizia giudiziaria in relazione a un´attività investigativa in corso (v. punto 3.4).
Comunque, anche fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati nel presente provvedimento non sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3.2.2. Esclusione della verifica preliminare

Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza non deve richiedere una verifica preliminare purché siano rispettate tutte le seguenti condizioni:
a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;
b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d´impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;
c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti nel provvedimento di cui alla lett. a) adottato dal Garante.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Resta inteso che **il normale esercizio di un impianto di videosorveglianza, non rientrante nelle ipotesi previste al precedente punto 3.2.1, non deve essere sottoposto all´esame preventivo del Garante, sempreché il trattamento medesimo avvenga con modalità conformi al presente provvedimento.**

Resta altresì inteso che nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza (spesso generici e non valutabili a distanza) cui non segua un esplicito riscontro dell´Autorità, in quanto non si applica il principio del silenzio-assenso.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 53

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3.2.3 Notificazione

E´ regola generale che i trattamenti di dati personali devono essere notificati al Garante solo se rientrano in casi specificamente previsti (art. 37 del Codice). In relazione a quanto stabilito dalla lett. f), del comma 1, dell´art. 37, questa Autorità ha già disposto che **non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente.** Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosorveglianza e che sia riconducibile a quanto disposto dall´art. 37 del Codice, deve essere preventivamente notificato a questa Autorità.

La mancata o incompleta notificazione ai sensi degli artt. 37 e 38 del Codice è punita con la sanzione amministrativa prevista dall´art. 163

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 54

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3.3. Misure di sicurezza da applicare ai dati personali trattati mediante sistemi di videosorveglianza e soggetti preposti

3.3.1. Misure di sicurezza

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 (artt. 31 e ss. del Codice).

Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l´attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

E´ inevitabile che -in considerazione dell´ampio spettro di utilizzazione di sistemi di videosorveglianza, anche in relazione ai soggetti e alle finalità perseguite nonché della varietà dei sistemi tecnologici utilizzati- le misure minime di sicurezza possano variare anche significativamente. E´ tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:

a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini (v. punto 3.3.2). Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi

utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
c) per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto (v. punto 3.4.);
d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all´art. 615-ter del codice penale;
f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie wi-fi, wi-max, Gprs).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3.3.2. Responsabili e incaricati

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 (art. 30 del Codice). Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l´angolo visuale, modificare lo zoom, ecc.) (v. punto 3.3.1.).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Vanno osservate le regole ordinarie anche per ciò che attiene all´eventuale designazione di responsabili del trattamento (art. 29 del Codice).

Il mancato rispetto di quanto previsto nelle lettere da a) ad f) del punto 3.3.1 comporta l´applicazione della sanzione amministrativa stabilita dall´art. 162, comma 2-ter, del Codice.

L´omessa adozione delle misure minime di sicurezza comporta l´applicazione della sanzione amministrativa stabilita dall´art. 162, comma 2-bis, ed integra la fattispecie di reato prevista dall´art. 169 del Codice.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3.4. Durata dell´eventuale conservazione

Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità (v. art. 11, comma 1, lett. e),del Codice), anche l´eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita. La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell´autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell´attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l´esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 61

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Per i comuni e nelle sole ipotesi in cui l´attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle recenti disposizioni normative(12), il termine massimo di durata della conservazione dei dati è limitato "ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l´uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione".

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 62

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante (v. punto 3.2.1), e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va 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. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall´autorità giudiziaria o dalla polizia giudiziaria in relazione ad un´attività investigativa in corso.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l´integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.
In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l´esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.
Il mancato rispetto dei tempi di conservazione delle immagini raccolte e del correlato obbligo di cancellazione di dette immagini oltre il termine previsto comporta l´applicazione della sanzione amministrativa stabilita dall´art. 162, comma 2-ter, del Codice.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

3.5. Diritti degli interessati

Deve essere assicurato agli interessati identificabili l´effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento (art. 7 del Codice).

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all´interessato (art. 10, comma 5, del Codice).

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo (art. 7, comma 3, lett. a), del Codice). Viceversa, l´interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge (art. 7, comma 3, lett. b), del Codice).

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 65

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

4. SETTORI SPECIFICI

4.1. Rapporti di lavoro

Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell´attività lavorativa, pertanto è vietata l´installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l´osservanza dei doveri di diligenza stabiliti per il rispetto dell´orario di lavoro e la correttezza nell´esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge).

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 66

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell´art. 4 della l. n. 300/1970, gli impianti e le apparecchiature, "dai quali può derivare anche la possibilità di controllo a distanza dell´attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l´Ispettorato del lavoro, dettando, ove occorra, le modalità per l´uso di tali impianti" (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lg. n. 165/2001).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Tali garanzie vanno osservate sia all´interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro, come, ad esempio, nei cantieri edili o con riferimento alle telecamere installate su veicoli adibiti al servizio di linea per il trasporto di persone (artt. 82, 85-87, d.lg. 30 aprile 1992, n. 285, "Nuovo codice della strada") o su veicoli addetti al servizio di noleggio con conducente e servizio di piazza (taxi) per trasporto di persone (le quali non devono riprendere in modo stabile la postazione di guida, e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche
indiretti, sull´attività lavorativa degli addetti, v. punto 4.4.).
Il mancato rispetto di quanto sopra prescritto comporta l´applicazione della sanzione amministrativa stabilita dall´art. 162, comma 2-ter, del Codice.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

L´utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori o ad effettuare indagini sulle loro opinioni integra la fattispecie di reato prevista dall´art. 171 del Codice.
Sotto un diverso profilo, eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull´attività giornalistica contenute nel Codice (artt. 136 e ss.), fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l´osservanza del codice deontologico per l´attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi, per motivi legittimi, alla sua diffusione (art. 7, comma 4, lett. a), del Codice).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Settori di particolare interesse

Sicurezza urbana: i Comuni che installano telecamere per fini di sicurezza urbana hanno l´obbligo di mettere cartelli che ne segnalino la presenza, salvo che le attività di videosorveglianza siano riconducibili a quelle di tutela specifica della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. La conservazione dei dati non può superare i 7 giorni, fatte salve speciali esigenze.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Sistemi integrati: per i sistemi che collegano telecamere tra soggetti diversi, sia pubblici che privati, o che consentono la fornitura di servizi di videosorveglianza "in remoto" da parte di società specializzate (es. società di vigilanza, Internet providers) mediante collegamento telematico ad un unico centro, sono obbligatorie specifiche misure di sicurezza (es. contro accessi abusivi alle immagini). Per alcuni sistemi è comunque necessaria la verifica preliminare del Garante.

Sistemi intelligenti: per i sistemi di videosorveglianza "intelligenti" dotati di software che permettono l´associazione di immagini a dati biometrici (es. "riconoscimento facciale") o in grado, ad esempio, di riprendere e registrare automaticamente comportamenti o eventi anomali e segnalarli (es. "motion detection") è obbligatoria la verifica preliminare del Garante.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Violazioni al codice della strada: obbligatori i cartelli che segnalino i sistemi elettronici di rilevamento delle infrazioni. Le telecamere devono riprendere solo la targa del veicolo (non quindi conducente, passeggeri, eventuali pedoni). Le fotografie o i video che attestano l´infrazione non devono essere inviati al domicilio dell´intestatario del veicolo.

Deposito rifiuti: lecito l´utilizzo di telecamere per controllare discariche di sostanze pericolose ed "eco piazzole" per monitorare modalità del loro uso, tipologia dei rifiuti scaricati e orario di deposito.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Settori specifici

Luoghi di lavoro: le telecamere possono essere installate solo nel rispetto dello norme in materia di lavoro. Vietato comunque il controllo a distanza dei lavoratori, sia all´interno degli edifici, sia in altri luoghi di prestazione del lavoro (es. cantieri, veicoli).

Ospedali e luoghi di cura: no alla diffusione di immagini di persone malate mediante monitor quando questi sono collocati in locali accessibili al pubblico. E´ ammesso, nei casi indispensabili, il monitoraggio da parte del personale sanitario dei pazienti ricoverati in particolari reparti (es. rianimazione), ma l´accesso alle immagini deve essere consentito solo al personale autorizzato e ai familiari dei ricoverati.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Istituti scolastici: ammessa l´installazione di sistemi di videosorveglianza per la tutela contro gli atti vandalici, con riprese delimitate alle sole aree interessate e solo negli orari di chiusura.

Taxi: le telecamere non devono riprendere in modo stabile la postazione di guida e la loro presenza deve essere segnalata con appositi contrassegni.

Trasporto pubblico: lecita l´installazione su mezzi di trasporto pubblico e presso le fermate, ma rispettando limiti precisi (es. angolo visuale circoscritto, riprese senza l´uso di zoom).

Webcam a scopo turistico: la ripresa delle immagini deve avvenire con modalità che non rendano identificabili le persone.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Soggetti privati

Tutela delle persone e della proprietà: contro possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, prevenzione incendi, sicurezza del lavoro ecc. si possono installare telecamere senza il consenso dei soggetti ripresi, ma sempre sulla base delle prescrizioni indicate dal Garante.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

5.1. Sicurezza urbana

Recenti **disposizioni legislative in materia di sicurezza hanno attribuito ai sindaci il compito di sovrintendere alla vigilanza ed all´adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidati ad essi dalla legge in materia di sicurezza e di polizia giudiziaria.** Al fine di prevenire e contrastare determinati pericoli che minacciano l´incolumità pubblica e la sicurezza urbana, il sindaco può altresì adottare provvedimenti, anche contingibili e urgenti, nel rispetto dei principi generali dell´ordinamento. Infine, il sindaco, quale ufficiale del Governo, concorre ad assicurare la cooperazione della polizia locale con le forze di polizia statali, nell´ambito delle direttive di coordinamento impartite dal Ministero dell´interno.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

5.1. Sicurezza urbana

…

Da tale quadro emerge che sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana. Non spetta a questa Autorità definire il concetto di sicurezza urbana e delimitarne l´ambito operativo rispetto a quelli di ordine e sicurezza pubblica; purtuttavia, resta inteso che**, nelle ipotesi in cui le attività di videosorveglianza siano assimilabili alla tutela della sicurezza pubblica, nonché alla prevenzione, accertamento o repressione dei reati, trova applicazione l´art. 53 del Codice.**

In ogni caso, si ribadisce l´auspicio che, nelle predette ipotesi, l´informativa, benché non obbligatoria, venga comunque resa, specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l´adozione di misure e accorgimenti, quali l´installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

5.2. Deposito dei rifiuti

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l´utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l´utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose **solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.**

Analogamente, l´utilizzo di sistemi di videosorveglianza è lecito **se risultano inefficaci o inattuabili altre misure** nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, Legge 24 novembre 1981, n. 689).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

5.3. Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada

Gli impianti elettronici di rilevamento automatizzato delle infrazioni, utilizzati per documentare la violazione delle disposizioni in materia di circolazione stradale, analogamente all´utilizzo di sistemi di videosorveglianza, comportano un trattamento di dati personali.

5.3.1. L´utilizzo di tali sistemi è quindi lecito se sono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, delimitando a tal fine la dislocazione e l´angolo visuale delle riprese in modo da non raccogliere immagini non pertinenti o inutilmente dettagliate. In conformità alla prassi ed al quadro normativo di settore riguardante talune violazioni del Codice della strada(18), il Garante prescrive quanto segue:

a) gli impianti elettronici di rilevamento devono circoscrivere la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino non rispettate le disposizioni in materia di circolazione stradale;

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

b) le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (es., ai sensi dell´art. 383 del d.P.R. n. 495/1992, il tipo di veicolo, il giorno, l´ora e il luogo nei quali la violazione è avvenuta); deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell´accertamento amministrativo (es., pedoni, altri utenti della strada);
c) le risultanze fotografiche o le riprese video rilevate devono essere utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale anche in fase di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

d) le immagini devono essere conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione, all´eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore(19), fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell´autorità giudiziaria o di polizia giudiziaria;
e) le fotografie o le immagini che costituiscono fonte di prova per le violazioni contestate non devono essere inviate d´ufficio al domicilio dell´intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità agli aventi diritto;
f) in considerazione del legittimo interesse dell´intestatario del veicolo di verificare l´autore della violazione e, pertanto, di ottenere dalla competente autorità ogni elemento a tal fine utile, la visione della documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale; al momento dell´accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Il mancato rispetto di quanto sopra prescritto nelle lettere da a) ad f) comporta l´applicazione della sanzione amministrativa stabilita dall´art. 162, comma 2-ter, del Codice.

5.3.2. Anche i conducenti dei veicoli e le persone che accedono o transitano in aree dove sono attivi sistemi elettronici di rilevazione automatizzata delle violazioni devono essere previamente informati in ordine al trattamento dei dati personali (art. 13 del Codice).

Particolari disposizioni normative vigenti individuano già talune ipotesi (come, ad es., in caso di rilevamento a distanza dei limiti di velocità) in cui l´amministrazione pubblica è tenuta a informare gli utenti in modo specifico in ordine all´utilizzo di dispositivi elettronici(20).

L´obiettivo da assicurare è quello di un´efficace informativa agli interessati, che può essere fornita dagli enti preposti alla rilevazione delle immagini attraverso più soluzioni.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Un´idonea informativa in materia può essere anzitutto assicurata mediante l´utilizzo di strumenti appropriati che rendano agevolmente conoscibile l´esistenza e la presenza nelle aree interessate degli strumenti di rilevamento di immagini. A tal fine, svolgono un ruolo efficace gli strumenti di comunicazione al pubblico e le iniziative periodiche di diffusa informazione (siti web, comunicati scritti); tali forme di informazione possono essere eventualmente integrate con altre modalità (es., volantini consegnati all´utenza, pannelli a messaggio variabile, annunci televisivi e radiofonici, reti civiche e altra comunicazione istituzionale).

A integrazione di tali strumenti di comunicazione e informazione, va considerato il contributo che possono dare appositi cartelli. A tal fine, il modello semplificato di informativa "minima", riportato nel fac-simile in allegato, può essere utilizzato nei casi in cui la normativa in materia di circolazione stradale non prevede espressamente l´obbligo di informare gli utenti relativamente alla presenza di dispositivi elettronici volti a rilevare automaticamente le infrazioni.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Come si è detto, la normativa di settore prevede espressamente, in alcuni casi (es., rilevamento a distanza dei limiti di velocità, dei sorpassi vietati), l´obbligo di rendere nota agli utenti l´installazione degli impianti elettronici di rilevamento automatizzato delle infrazioni. In questi stessi casi è quindi possibile fare a meno di fornire un´ulteriore, distinta informativa rispetto al trattamento dei dati che riproduca gli elementi che sono già noti agli interessati per effetto degli avvisi di cui alla disciplina di settore in tema di circolazione stradale (art. 13, comma 2, del Codice). L´installazione di questi ultimi appositi avvisi previsti dal Codice della strada permette già agli interessati di percepire vari elementi essenziali in ordine al trattamento dei propri dati personali. Pertanto, gli avvisi che segnalano adeguatamente l´attivazione di dispositivi elettronici di rilevazione automatica delle infrazioni possono essere considerati idonei ad adempiere all´obbligo di fornire l´informativa di cui all´art. 13 del Codice.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Infine, l´obbligo di fornire tale informativa deve ritenersi soddisfatto anche quando il titolare del trattamento, pur mancando una previsione normativa che obblighi specificamente a segnalare la rilevazione automatizzata, la segnali comunque utilizzando avvisi analoghi a quelli previsti dal Codice della strada.

La violazione delle disposizioni riguardanti l´informativa di cui all´art. 13 è punita con la sanzione amministrativa prevista dall´art. 161 del Codice.

5.3.3. Qualora si introducano sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, i comuni dovranno rispettare quanto previsto dal d.P.R. 22 giugno 1999, n. 250. Tale normativa prevede che i dati trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso, ferma restando l´accessibilità agli stessi per fini di polizia giudiziaria o di indagine penale (art. 3 d.P.R. n. 250/1999).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

5.4. Ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e, in particolare, da enti territoriali Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell´espletamento delle più diverse attività istituzionali.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

Questa Autorità ha già individuato al punto 4.6. un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate, in particolare con riferimento all´attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale(21).
In particolare:
a) l´utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell´ente, l´accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell´ente;

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

b) nei casi in cui un "centro" unico gestisca l´attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della
singola pubblica amministrazione.
Il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già il punto 3.2.1 la richiede (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

6. PRIVATI ED ENTI PUBBLICI ECONOMICI
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).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

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.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

6.2. Trattamento di dati personali per fini diversi da quelli esclusivamente personali

6.2.1. Consenso

Nel caso in cui trovi applicazione la disciplina del Codice, il trattamento di dati può essere lecitamente effettuato da privati ed enti pubblici economici solamente se vi sia il consenso preventivo dell´interessato, oppure se ricorra uno dei presupposti di liceità previsti in alternativa al consenso (artt. 23 e 24 del Codice).

Nel caso di impiego di strumenti di videosorveglianza la possibilità di acquisire il consenso risulta in concreto limitata dalle caratteristiche stesse dei sistemi di rilevazione che rendono pertanto necessario individuare un´idonea alternativa nell´ambito dei requisiti equipollenti del consenso di cui all´art. 24, comma 1, del Codice.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

6.2.2. Bilanciamento degli interessi

Tale alternativa può essere ravvisata nell´istituto del bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice). Il presente provvedimento dà attuazione a tale istituto, individuando i casi in cui la rilevazione delle immagini può avvenire senza consenso, qualora, con le modalità stabilite in questo stesso provvedimento, sia effettuata nell´intento di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, o finalità di prevenzione di incendi o di sicurezza del lavoro.

A tal fine, possono essere individuati i seguenti casi, in relazione ai quali, con le precisazioni di seguito previste, il trattamento può lecitamente avvenire pure in assenza del consenso.

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

6.2.2.1. Videosorveglianza (con o senza registrazione delle immagini)

Tali trattamenti sono ammessi in presenza di concrete situazioni che giustificano l´installazione, a protezione delle persone, della proprietà o del patrimonio aziendale.

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.).

Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

6.2.2.2. Riprese nelle aree condominiali comuni

Qualora i trattamenti siano effettuati dal condominio (anche per il tramite della relativa amministrazione), si evidenzia che tale specifica ipotesi è stata recentemente oggetto di una segnalazione da parte del Garante al Governo ed al Parlamento; ciò in relazione all´assenza di una puntuale disciplina che permetta di risolvere alcuni problemi applicativi evidenziati nell´esperienza di questi ultimi anni. Non è infatti chiaro se l´installazione di sistemi di videosorveglianza possa essere effettuata in base alla sola volontà dei comproprietari, o se rilevi anche la qualità di conduttori. Non è parimenti chiaro quale sia il numero di voti necessario per la deliberazione condominiale in materia (se occorra cioè l´unanimità ovvero una determinata maggioranza).

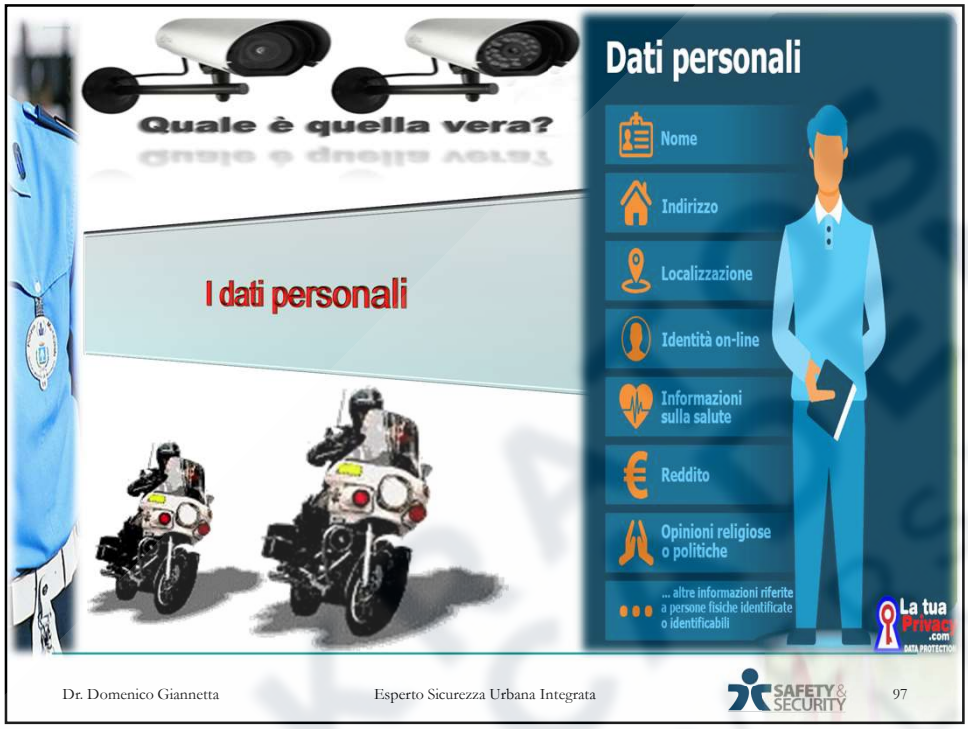
Garante della Privacy Circolare del 27 Aprile 2010 : Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy

7. PRESCRIZIONI E SANZIONI

Il Garante invita tutti i titolari dei trattamenti di dati personali effettuati tramite sistemi di videosorveglianza ad attenersi alle prescrizioni indicate nel presente provvedimento.

Le misure necessarie prescritte con il presente provvedimento devono essere osservate da tutti i titolari di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

- all´inutilizzabilità dei dati personali trattati in violazione della relativa disciplina (art. 11, comma 2, del Codice);
- all´adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante (art. 143, comma 1, lett. c), del Codice), e di analoghe decisioni adottate dall´autorità giudiziaria civile e penale;
- all´applicazione delle pertinenti sanzioni amministrative o penali (artt. 161 e ss. del Codice).



Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

Particolarmente importanti sono:

• i **dati che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

• i **dati rientranti in particolari categorie**: si tratta dei dati c.d. *"sensibili"*, cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i **dati genetici,** i **dati biometrici** e quelli relativi all'**orientamento sessuale**;

Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
98

• i **dati relativi a condanne penali e reati**: si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, **altri dati personali** hanno assunto un ruolo significativo, come **quelli relativi alle comunicazioni elettroniche** (via Internet o telefono) e **quelli che consentono la geolocalizzazione**, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

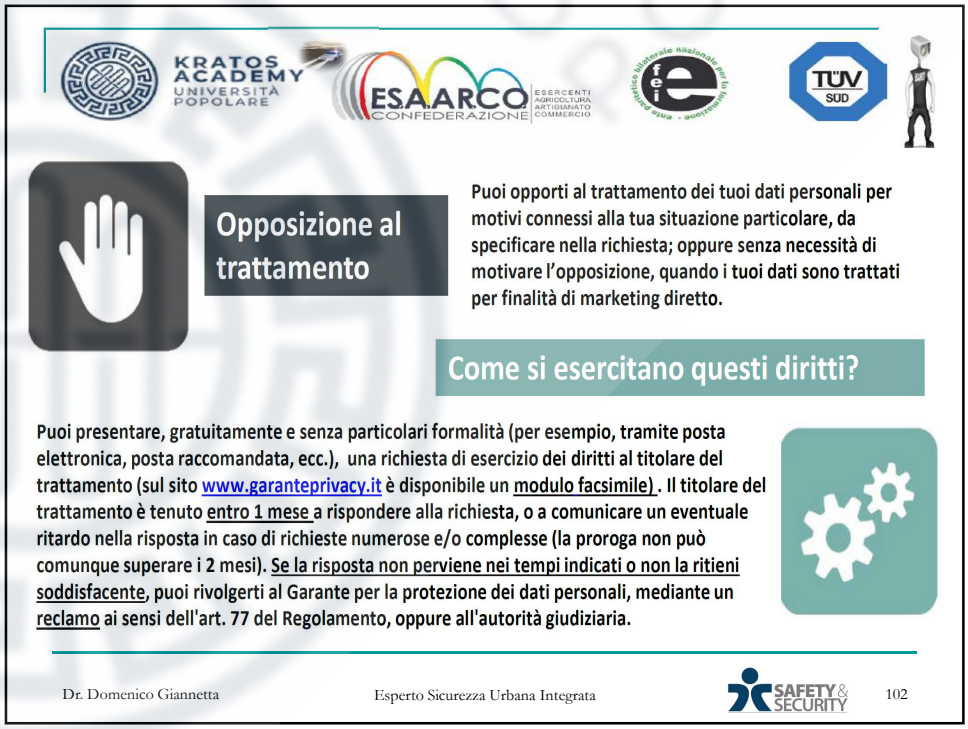
LE PARTI IN GIOCO

Interessato è la persona fisica alla quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale, ecc. di Mario Rossi, questa persona è l"interessato" (articolo 4, paragrafo 1, punto 1), del Regolamento UE 2016/679);

Titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento (articolo 4, paragrafo 1, punto 7), del Regolamento UE 2016/679);

Responsabile è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati (articolo 4, paragrafo 1, punto 8), del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. *"sub-responsabile"* (articolo 28, paragrafo 2).


KRATOS ACADEMY
TÜV
Conosci i principali diritti previsti dal
Regolamento (UE) 2016/679?
Il Regolamento (articoli 15-22) riconosce importanti diritti in materia di protezione dei dati personali, che possono essere esercitati rivolgendosi al titolare del trattamento (soggetto pubblico, impresa, associazione, partito, persona fisica, ecc.).
Accesso ai propri dati personali
Hai il diritto di sapere se è in corso un trattamento di dati personali che ti riguardano e - se confermato - di ottenere una copia di tali dati ed essere informato su: l'origine dei dati; le categorie di dati personali trattate; i destinatari dei dati; le finalità del trattamento; l'esistenza di un processo decisionale automatizzato, compresa la profilazione; il periodo di conservazione dei dati; i diritti previsti dal Regolamento.
Rettifica, cancellazione, limitazione del trattamento, portabilità dei dati personali
Puoi chiedere - nei casi previsti dal Regolamento - che i dati personali a te riferiti siano rettificati o cancellati, o che ne venga limitato il trattamento. Puoi inoltre chiedere che i dati che tu hai fornito al titolare siano trasferiti ad un altro titolare («diritto alla portabilità»), nel caso in cui il trattamento si basi sul tuo consenso o su un contratto con te stipulato e venga effettuato con mezzi automatizzati .
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
101


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
Opposizione al trattamento
Puoi opporti al trattamento dei tuoi dati personali per motivi connessi alla tua situazione particolare, da specificare nella richiesta; oppure senza necessità di motivare l'opposizione, quando i tuoi dati sono trattati per finalità di marketing diretto.
Come si esercitano questi diritti?
Puoi presentare, gratuitamente e senza particolari formalità (per esempio, tramite posta elettronica, posta raccomandata, ecc.), una richiesta di esercizio dei diritti al titolare del trattamento (sul sito www.garanteprivacy.it è disponibile un modulo facsimile). Il titolare del trattamento è tenuto entro 1 mese a rispondere alla richiesta, o a comunicare un eventuale ritardo nella risposta in caso di richieste numerose e/o complesse (la proroga non può comunque superare i 2 mesi). Se la risposta non perviene nei tempi indicati o non la ritieni soddisfacente, puoi rivolgerti al Garante per la protezione dei dati personali, mediante un reclamo ai sensi dell'art. 77 del Regolamento, oppure all'autorità giudiziaria.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
102

Principi generali del trattamento di dati personali

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679, che qui si ricordano brevemente:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 103

Il Regolamento (articolo 5, paragrafo 2) richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è il principio detto di "responsabilizzazione" (o accountability) che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1, del Regolamento, dove si afferma che "il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento."

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 104

Assicurare la liceità del trattamento di dati personali

Il Regolamento, come già previsto dal Codice in materia di protezione dei dati personali, prevede che **ogni trattamento deve trovare fondamento in un'idonea base giuridica.**

I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 del Regolamento:

- consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Per quanto riguarda le **"categorie particolari di dati personali"** (articolo 9 del Regolamento), il loro trattamento è vietato, in prima battuta, a meno che il titolare possa dimostrare di soddisfare almeno una delle condizioni fissate all'articolo 9, paragrafo 2 del Regolamento, che qui ricordiamo:

- l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per uno dei seguenti scopi:
  - per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;

❖ il trattamento è necessario per uno dei seguenti scopi:

- per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
- per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Per alcune di tali finalità sono previste limitazioni o prescrizioni ulteriori, anche nel diritto nazionale

Consenso

Quando il trattamento si fonda sul consenso dell'interessato, il titolare deve sempre essere in grado di dimostrare (articolo 7.1 del Regolamento) che l'interessato ha prestato il proprio consenso), che è valido se:

❖ all'interessato è stata resa l'informazione sul trattamento dei dati personali (articoli 13 o 14 del Regolamento);

❖ è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse. Il consenso deve essere sempre revocabile.

Occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (articolo 7.2), per esempio all'interno della modulistica.

Non è ammesso il consenso tacito o presunto (per esempio, presentando caselle già spuntate su un modulo).

Quando il trattamento riguarda le "categorie particolari di dati personali" (articolo 9 Regolamento) il consenso deve essere "esplicito"; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – articolo 22).

Il consenso non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per le categorie particolari di dati di cui all'articolo 9 Regolamento).

Per approfondimenti: Linee-guida del WP29 sul consenso, qui disponibili: www.garanteprivacy.it/regolamentoue/consenso.

Si segnalano anche le linee-guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251), qui disponibili: www.garanteprivacy/regolamentoue/profilazione.

Interesse vitale di un terzo

Si può invocare tale base giuridica per il trattamento di dati personali solo se nessuna delle altre condizioni di liceità può trovare applicazione (considerando 46).

Interesse legittimo prevalente di un titolare o di un terzo

Il ricorso a questa base giuridica per il trattamento di dati personali presuppone che il titolare stesso effettui un bilanciamento fra il legittimo interesse suo o del terzo e i diritti e libertà dell'interessato. Dal 25 maggio 2018, dunque, tale bilanciamento non spetta più all'Autorità, in linea di principio. Si tratta di una delle principali espressioni del principio di "responsabilizzazione" introdotto dal Regolamento (UE) 2016/679.

L'interesse legittimo del titolare o del terzo deve risultare prevalente sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.

Il Regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

Si ricordi, inoltre, che il legittimo interesse non può essere invocato isolatamente quale base giuridica per il trattamento delle categorie particolari di dati personali (articolo 9, paragrafo 2, del Regolamento).

Trasparenza del trattamento: l'informativa agli interessati

Fatte salve alcune eccezioni, chi intende effettuare un trattamento di dati personali deve fornire all'interessato alcune informazioni anche per metterlo nelle condizioni di esercitare i propri diritti (articoli 15-22 del Regolamento medesimo).

QUANDO

L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del Regolamento) deve essere fornita all'interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati (se raccolti direttamente presso l'interessato: art. 13 del Regolamento). Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del Regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevedeva l'art. 13, comma 4, del Codice).

COSA

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del Regolamento e, in parte, sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.). Se i dati non sono raccolti direttamente presso l'interessato (articolo 14 del Regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.

In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

Il Regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

COME

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: articolo 12, paragrafo 1, e considerando 58). Sono comunque ammessi "altri mezzi", quindi può essere fornita anche in forma orale, ma nel rispetto delle caratteristiche di cui sopra (articolo 12, paragrafo 1).

Il Regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (articolo 12, paragrafo 7); queste icone in futuro dovranno essere uniformate in tutta l'Ue attraverso l'intervento dalla Commissione europea.

In base al Regolamento, si deve porre particolare attenzione alla formulazione dell'informativa, che deve essere soprattutto comprensibile e trasparente per l'interessato, attraverso l'uso di un linguaggio chiaro e semplice. In particolare, bisogna ricordare che per i minori si devono prevedere informative idonee (anche considerando 58). Per maggiori dettagli ed esempi di redazione di informative, il documento del WP29 in materia di "Trasparenza" del trattamento, qui disponibile: www.garanteprivacy.it/regolamentoue/trasparenza

Un approccio responsabile al trattamento: Accountability

Il Regolamento pone l'accento sulla "responsabilizzazione" di titolari e responsabili, ossia, sull' adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento (artt. 23-25, in particolare, e l'intero Capo IV del Regolamento). Dunque, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "data protection by default and by design" (articolo 25), ossia dalla **necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.** Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto previsto dall'articolo 25, paragrafo 1, del Regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel Regolamento rispetto alla gestione degli obblighi dei titolari: ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35- 36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati del Gruppo "Articolo 29", qui disponibili: www.garanteprivacy.it/Regolamentoue/DPIA). (Vedi anche: il tutorial del Garante sul concetto di "rischio")

All'esito di questa valutazione di impatto, il titolare:

- ❖ potrà decidere se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero, se il rischio risulta ciononostante elevato;
- ❖ dovrà consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità avrà quindi il compito di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58 del Regolamento (dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento).

In conseguenza dell'applicazione del principio di accountability, dal 25 maggio 2018 non sono più previste

- la notifica preventiva dei trattamenti all'autorità di controllo;
- una verifica preliminare da parte del Garante per i trattamenti "a rischio" (anche se potranno esservi alcune eccezioni legate a disposizioni nazionali, previste in particolare dall'articolo 36, paragrafo 5 del Regolamento).

Al loro posto, il Regolamento prevede in capo ai titolari l'obbligo (pressoché generalizzato) di tenere un registro dei trattamenti e, appunto, di effettuare valutazioni di impatto in piena autonomia con eventuale successiva consultazione dell'Autorità.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 119

Principio di "responsabilizzazione" dei titolari e responsabili del trattamento: principali elementi

Rapporti contrattuali fra titolare e responsabile del trattamento

Il Regolamento definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento negli stessi termini di cui alla direttiva 95/46/CE e, quindi, al Codice privacy italiano.

Tuttavia, il Regolamento (articolo 28) prevede dettagliatamente le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti. Deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'articolo 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti", quali, in particolare:

- la natura, durata e finalità del trattamento o dei trattamenti assegnati
- le categorie di dati oggetto di trattamento
- le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel Regolamento

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 120

Inoltre, il Regolamento prevede obblighi specifici in capo ai responsabili del trattamento, distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare:

- la tenuta del registro dei trattamenti svolti (articolo 30, paragrafo 2);
- l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (articolo 32);
- la designazione di un RPD-DPO, nei casi previsti dal Regolamento o dal diritto nazionale (articolo 37).

Una novità importante del Regolamento è la possibilità di designare sub-responsabili del trattamento da parte di un responsabile (articolo 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (articolo 82, paragrafo 1 e paragrafo 3).

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti - ma solo se non effettuano trattamenti a rischio (articolo 30, paragrafo 5) - devono tenere un registro delle operazioni di trattamento, i cui contenuti sono indicati all'articolo 30.

Si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. I contenuti del registro sono fissati nell'articolo 30. Tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Misure di sicurezza

Il titolare del trattamento, come pure il responsabile del trattamento, è obbligato ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato).

Fra tali misure, il Regolamento menziona, in particolare, la pseudonimizzazione e la cifratura dei dati; misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; misure atte a garantire il tempestivo ripristino della disponibilità dei dati; procedure per verificare e valutare regolarmente l'efficacia delle misure di sicurezza adottate.

La lista di cui al paragrafo 1 dell'articolo 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Per questi motivi, non possono sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza poiché tale valutazione è rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da articolo 32 del Regolamento.

Vi è, inoltre, la possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate (articolo 32, paragrafo 3).

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 123

Notifica di una violazione dei dati personali

A partire dal 25 maggio 2018, tutti i titolari dovranno notificare al Garante le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (considerando 85). Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34.

I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli articolo 33 e 34 del Regolamento.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 124

Tutti i titolari di trattamento devono in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (articolo 33, paragrafo 5). È bene, dunque, adottare le misure necessarie a documentare eventuali violazioni, anche perché i titolari sono tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.
Si segnalano, al riguardo, le linee-guida in materia di notifica delle violazioni di dati personali del Gruppo "Articolo 29", qui disponibili: www.garanteprivacy/regolamentoue/databreach.

Responsabile della protezione dei dati

La designazione di un "responsabile della protezione dati" (RPD) è finalizzata a facilitare l'attuazione della normativa da parte del titolare/responsabile (articolo 39). Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'articolo 35, oltre alla funzione di punto di contatto per gli interessati e per il Garante rispetto a ogni questione attinente l'applicazione del Regolamento. La sua designazione è obbligatoria in alcuni casi (articolo 37), e il Regolamento delinea le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali: articoli 38 e 39) in termini che il Gruppo di lavoro "Articolo 29" ha ritenuto opportuno chiarire attraverso alcune linee-guida, disponibili anche sul sito del Garante, e alle quali si rinvia per maggiori delucidazioni unitamente alle relative FAQ (www.garanteprivacy.it/Regolamentoue/rpd). Si segnalano anche i materiali disponibili nella sezione "Responsabile della protezione dati" sul sito del Garante, che comprendono ulteriori FAQ sul punto (www.garanteprivacy/regolamentoue/rpd)

I diritti degli interessati

I titolari del trattamento devono rispettare le modalità previste per l'esercizio di tutti i diritti da parte degli interessati, stabilite, in via generale, negli artt. 11 e 12 del Regolamento :

- In primo luogo, il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti, il responsabile del trattamento è tenuto a collaborare con il titolare ai fini dell'esercizio di tali diritti (art. 28, paragrafo 3, lettera e)).
- Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (, in particolare, articolo 11, paragrafo 2 e articolo 12, paragrafo 6).

- Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), pari a 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.
- La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.
- Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive - anche ripetitive (articolo12, paragrafo 5) - ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (articolo 15, paragrafo 3). In quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (articolo 12, paragrafo 1; articolo 15, paragrafo 3).


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
Scheda di sintesi a mero scopo divulgativo. Per un quadro completo della materia, si rimanda alla legislazione in tema di protezione dei dati personali e ai provvedimenti dell'Autorità.
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
Conosci i principali diritti previsti dal
Regolamento (UE) 2016/679?
Il Regolamento (articoli 15-22) riconosce importanti diritti in materia di protezione dei dati personali, che possono essere esercitati rivolgendosi al titolare del trattamento (soggetto pubblico, impresa, associazione, partito, persona fisica, ecc.).
Accesso ai propri dati personali
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
129


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
Hai il diritto di sapere se è in corso un trattamento di dati personali che ti riguardano e - se confermato - di ottenere una copia di tali dati ed essere informato su: l'origine dei dati; le categorie di dati personali trattate; i destinatari dei dati; le finalità del trattamento; l'esistenza di un processo decisionale automatizzato, compresa la profilazione; il periodo di conservazione dei dati; i diritti previsti dal Regolamento.
Rettifica, cancellazione, limitazione del trattamento, portabilità dei dati personali
Puoi chiedere - nei casi previsti dal Regolamento - che i dati personali a te riferiti siano rettificati o cancellati, o che ne venga limitato il trattamento. Puoi inoltre chiedere che i dati che tu hai fornito al titolare siano trasferiti ad un altro titolare («diritto alla portabilità»), nel caso in cui il trattamento si basi sul tuo consenso o su un contratto con te stipulato e venga effettuato con mezzi automatizzati .
Opposizione al trattamento
Puoi opporti al trattamento dei tuoi dati personali per motivi connessi alla tua situazione particolare, da specificare nella richiesta; oppure senza necessità di motivare l'opposizione, quando i tuoi dati sono trattati per finalità di marketing diretto.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
130

Come si esercitano questi diritti?

Puoi presentare, gratuitamente e senza particolari formalità (per esempio, tramite posta elettronica, posta raccomandata, ecc.), una richiesta di esercizio dei diritti al titolare del trattamento (sul sito www.garanteprivacy.it è disponibile un modulo facsimile). Il titolare del trattamento è tenuto entro 1 mese a rispondere alla richiesta, o a comunicare un eventuale ritardo nella risposta in caso di richieste numerose e/o complesse (la proroga non può comunque superare i 2 mesi). Se la risposta non perviene nei tempi indicati o non la ritieni soddisfacente, puoi rivolgerti al Garante per la protezione dei dati personali, mediante un reclamo ai sensi dell'art. 77 del Regolamento, oppure all'autorità giudiziaria.

Scopri di più su: www.garanteprivacy.it/home/diritti

Trasferimento dei dati all'estero

Verso Paesi appartenenti all'Unione europea

Non possono esservi limitazioni né divieti alla libera circolazione dei dati personali nell'Unione europea per motivi attinenti alla protezione dei dati (Articolo 1, paragrafo 3 del Regolamento). Pertanto, non vi sono limiti di alcun genere per quanto riguarda i flussi di dati dall'Italia verso altri Stati membri dell'Ue (e dello Spazio Economico Europeo: Islanda, Norvegia, Liechtenstein).

Verso Paesi non appartenenti all'Unione europea

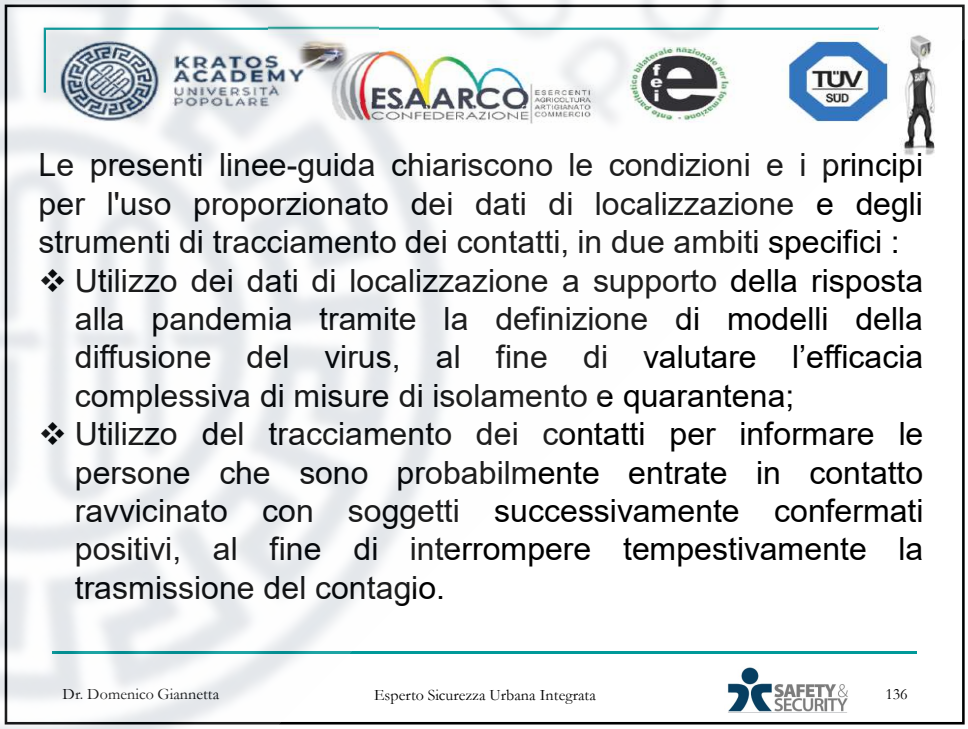
Il trasferimento di dati personali verso Paesi non appartenenti all'Unione europea è vietato, in linea di principio.

Tale divieto può essere superato solo quando intervengano le seguenti specifiche garanzie (articoli da 44 a 49 del Regolamento UE 2016/679):

a) adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;
b) in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali tipo);
c) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (articolo 49 del Regolamento).

Sono altresì vietati trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (articolo 48 del Regolamento UE 2016/679). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all'articolo 49 del Regolamento medesimo. E' lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del titolare o dal diritto dell'Unione europea (articolo 49, paragrafo 4) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.


Quale è quella vera?
Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 elaborate dal Comitato Europeo per la Protezione dei Dati (Edpb)
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
135


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
Le presenti linee-guida chiariscono le condizioni e i principi per l'uso proporzionato dei dati di localizzazione e degli strumenti di tracciamento dei contatti, in due ambiti specifici :
❖ Utilizzo dei dati di localizzazione a supporto della risposta alla pandemia tramite la definizione di modelli della diffusione del virus, al fine di valutare l'efficacia complessiva di misure di isolamento e quarantena;
❖ Utilizzo del tracciamento dei contatti per informare le persone che sono probabilmente entrate in contatto ravvicinato con soggetti successivamente confermati positivi, al fine di interrompere tempestivamente la trasmissione del contagio.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
136

Il concetto di anonimizzazione tende ad essere frainteso e spesso confuso con la pseudonimizzazione. Mentre l'anonimizzazione consente di utilizzare i dati senza restrizioni, i dati pseudonimizzati rientrano nel campo di applicazione del regolamento generale sulla protezione dei dati.

Il mondo si trova ad affrontare una grave crisi sanitaria che richiede risposte forti, il cui impatto si manifesterà anche oltre il termine di questa emergenza. Il trattamento automatizzato dei dati e le tecnologie digitali possono essere elementi chiave nella lotta al COVID-19. Tuttavia, occorre guardarsi dal rischio di effetti irreversibili. Spetta a noi tutti garantire che ogni misura adottata in queste circostanze eccezionali sia necessaria, limitata nel tempo, di portata minima e soggetta a un riesame periodico ed effettivo nonché a una valutazione scientifica.

Il Comitato europeo per la protezione dei dati sottolinea che a nessuno dovrebbe essere chiesto di scegliere tra una risposta efficace all'attuale crisi e la tutela dei diritti fondamentali: entrambi gli obiettivi sono alla nostra portata, e i principi di protezione dei dati possono svolgere un ruolo molto importante nella lotta contro il virus. Il diritto europeo in materia di protezione dei dati consente l'uso responsabile dei dati personali per la gestione della salute, garantendo al contempo che non siano erosi i diritti e le libertà individuali.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 139

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 140

Le Linee Guida 5-2020 dell'European Board sul consenso sono solo un aggiornamento di quelle già adottate e successivamente emendate dal Gruppo articolo 29 – Sotto la lente del Board sono finite, in particolare, le pratiche dei «cookie walls» e dello «scrolling», di cui si precisano in modo più esplicito gli elementi di contrasto con i requisiti del consenso.

In informatica, file di informazioni che i siti web memorizzano sul computer dell'utente di Internet durante la navigazione, specialmente allo scopo di identificare chi ha già visitato il sito in precedenza.
I cookie walls sono dei cookie come tanti altri, ma usati per fare qualcosa che il GDPR non accetta.
L'idea alla base e' che si comportino come un Firewall: se non dai il consenso, il sito non si consulta.
Inutile dire che le autorità hanno già vietato tali comportamenti che obbligano ad accetterli, ma ci sono anche decisioni contrarie a determinate condizioni.
Sta di fatto che le decisioni dei giudici sono diverse da quelle delle Autorità, non di rado, e non di rado perche' non hanno approfondito i temi complicatissimi del GDPR.

Quindi il cookie wall e' un cookie di fatto profilante (anche se potrebbe essere tecnico) che impedisce di usare un servizio finche' non lo si accetta.
Per le autorità questo e' un consenso che, se dato, non e' libero, quindi come non dato, con le relative mostruose sanzioni che non distinguerebbero il contesto, pur essendo questo richiesto dal GDPR.
Il problema di fondo rimande: si vuole profilare a tutti i costi gli utenti visitatori. Questo e' inaccettabile e comporta la reazione del GDPR di bloccare ogni contatto con terze parti, riportando il web al millennio scorso.
A dicembre 2019 la CNIL dichiara che i cookie wall dovrebbero essere considerati una violazione del GDPR. Il Garante olandese lo ha indicato in una propria guida nel marzo 2019.

Le Linee Guida dell'EDPB (European Data Protection Board) n. 5-2020 sul consenso non sono altro che una versione leggermente aggiornata di quelle già adottate dal Gruppo di lavoro articolo 29.
In particolare il Comitato europeo si è reso conto che era necessario fornire dei chiarimenti su due argomenti specifici:

1. la validità del consenso prestato dall'interessato nell'interazione con i c.d. «cookie walls»;
2. la possibilità di associare al c.d. «scrolling» (scorrimento) delle pagine di un sito web il consenso dell'utente/interessato.

Più che di inedite prese di posizione, si tratta di inserti necessari a inquadrare in modo più esplicito prassi che, alla luce delle disposizioni sul consenso, già erano e risultavano non corrette.

Dunque sono solo i paragrafi concernenti questi due argomenti ad essere stati revisionati, mentre la residua parte del documento è rimasta – salvo che per le modifiche editoriali - invariata.

La revisione riguarda, quindi, in particolare:

- la Sezione sulle "Condizionalità" (3.1.2, ai periodi 38-41, con introduzione dei nn. 39, 40 e 41);
- la Sezione sulla "Manifestazione di volontà inequivocabile" (3.4, periodo 86).

Cookie walls e consenso

Sono chiamati «cookie walls» quei cookie che permettono l'accesso e/o la fruizione di una pagina web a condizione che essi siano stati assentiti dall'utente. Sono appunto dei muri, vere e proprie barriere digitali: prestandovi il consenso, l'interessato apre la strada al tracciamento dei dati e alla quasi inevitabile profilazione solo per poter proseguire la navigazione e/o accedere alle funzionalità del sito.

Evidentemente, questo genere di condizionalità non può essere conforme al Gdpr e, a fronte di possibili diversità di approccio allo stesso, il Comitato ha inteso – con la propria autorevolezza – esprimersi in modo netto.

Così, al paragrafo 39, le Linee Guida stabiliscono che “al fine di garantire la libertà del consenso, l'accesso ai servizi e alle funzionalità non deve essere condizionato al rilascio del consenso, da parte di un utente, alla memorizzazione delle informazioni o all'accesso ad informazioni già memorizzate nel suo terminale” . Questa affermazione è meglio còlta nel suo significato se calata nel contesto dell'intera sezione dedicata alle condizionalità, all'inizio della quale si legge che “per valutare se il consenso sia stato prestato liberamente è di rilievo l’articolo 7, paragrafo 4, del regolamento”, tale disposizione indicando, tra l’altro, “che è altamente inopportuno 'accorpare' il consenso all’accettazione delle condizioni generali di contratto/servizio o 'subordinare' la fornitura di un contratto o servizio a una richiesta di consenso al trattamento di dati personali che non sono necessari per l’esecuzione del contratto o servizio”. In poche parole, “l’articolo 7, paragrafo 4, mira a garantire che la finalità del trattamento dei dati personali non sia mascherata né accorpata all’esecuzione di un contratto o alla prestazione di un servizio per il quale i dati personali non sono necessari”.

Al paragrafo 40 è quindi proposto un nuovo esempio, il n. 6a: quello del provider di un sito web che colloca uno 'script' di blocco della visibilità di un contenuto a meno che sia prestato il consenso ai cookie e al trattamento dei dati per i quali i cookie vengono installati. Dunque, in tale eventualità, per accedere ai contenuti della pagina, è necessario che l'utente accetti questo tipo di cookie. Non può dunque dirsi prospettata all'interessato una reale, genuina possibilità di scelta.

Le Linee Guida concludono, in sostanza, che trattasi di una prassi non corretta, non conforme al Gdpr - in essa essendo in gioco un consenso non valido, non rispondente ai requisiti canonici.

Sulla stessa linea appaiono anche i successivi chiarimenti pubblicati dal Garante Privacy, nei quali viene testualmente indicato che le modalità di acquisizione del consenso basate su uno "scroll", ovvero sulla prosecuzione della navigazione all'interno della medesima pagina web, siano considerate in linea con i requisiti di legge qualora, tuttavia, queste azioni siano chiaramente indicate nell'informativa e siano in grado di generare un evento, registrabile e documentabile presso il server del gestore del sito, che possa essere qualificato come azione positiva dell'utente.

'Scrolling' e consenso

Per l'esempio n. 16 riportato nelle Linee Guida del Gruppo di lavoro articolo 29, rev. 01 del 2018, "scorrere un sito verso il basso o sfogliarne le pagine non sono azioni chiare e positive, poiché l'avviso che continuare a scorrere il sito costituirà un'espressione di consenso può essere difficile da distinguere e/o può essere trascurato inavvertitamente quando l'interessato scorre rapidamente grandi quantità di testo; inoltre tali azioni non sono sufficientemente inequivocabili".
Anche qui l'intervento del Comitato è nel senso di meglio esplicitare l'inquadramento della prassi del c.d. 'scrolling' e precisarne l'inettitudine a presumersi/costituire valida manifestazione di consenso.

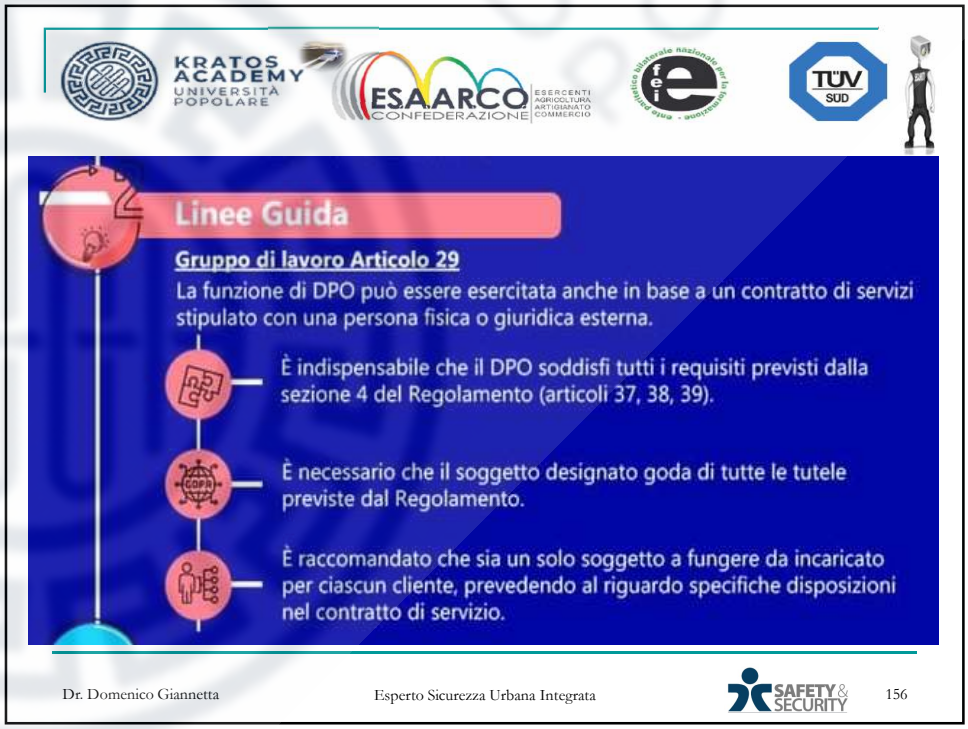
E così, di poco modificato, l'esempio 16 revisionato è più perentorio: “azioni come scorrere o sfogliare una pagina web o come altra attività analoga dell'utente, non potranno in qualsivoglia modo soddisfare il requisito della azione chiara e positiva: dette azioni si distinguono ben difficilmente da altre attività o interazioni dell'utente e perciò con esse non sarà possibile stabilire che sia stato ottenuto un consenso privo di ambiguità. Per di più, in un caso come questo, sarebbe difficile offrire all'utente la possibilità di revocare il consenso in un modo che fosse altrettanto semplice come averlo prestato”.

I due fattori della migliore esplicitazione paiono all'osservatore i seguenti: quell'”under any circumstances”, qui tradotto come “in qualsivoglia modo”, esclude che lo 'scrolling' possa mai essere accettato come “azione chiara e positiva”, possibilità che la precedente formulazione non chiudeva del tutto. Si aggiunge a ciò, del tutto appropriatamente, l'osservazione circa la difficoltà della revoca del consenso, come contrapposta alla 'leggerezza' del suo rilascio.


Quale è quella vera?
Obblighi dei Comuni
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
153


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
Le amministrazioni Comunali, in qualità di titolari del trattamento, sono gravate da numerosi obblighi da rispettare a pena di sanzioni, anche abbastanza pesanti.
Tra i principali adempimenti rientra l'individuazione del responsabile del trattamento dei dati personali (di regola coincidente con il Comandante della Polizia Municipale responsabile del servizio), nonché la designazione del responsabile della protezione dei dati (DPO) in base al Regolamento (Ue) 2016/679.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
154


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
L'AFFIDAMENTO DEL SERVIZO DI DPO AD UN SOGGETTO ESTERNO ALLA PA
Normativa
Regolamento UE 679/2016 - Articolo 37
PARAGRAFO 5
Il DPO è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
PARAGRAFO 6
Il DPO può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
155


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
Linee Guida
Gruppo di lavoro Articolo 29
La funzione di DPO può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna.
È indispensabile che il DPO soddisfi tutti i requisiti previsti dalla sezione 4 del Regolamento (articoli 37, 38, 39).
È necessario che il soggetto designato goda di tutte le tutele previste dal Regolamento.
È raccomandato che sia un solo soggetto a fungere da incaricato per ciascun cliente, prevedendo al riguardo specifiche disposizioni nel contratto di servizio.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
156


Giurisprudenza italiana
Sentenza TAR Friuli Venezia Giulia 287/2018
La certificazione ISO/IEC/27001 non costituisce un titolo abilitante ai fini dell'assunzione e dello svolgimento delle funzioni di DPO, dovendosi valutare unicamente le competenze.
Sentenza TAR Lecce 1468/2019
Se la funzione di DPO viene attribuita ad una persona giuridica, il soggetto designato come DPO deve essere membro o appartenere all'organico della persona giuridica.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
157


L'Amministrazione comunale deve pubblicare una informativa sul proprio sito contenente:
modalità e finalità di attivazione degli impianti di videosorveglianza;
modalità di raccolta e conservazione dei dati;
modalità di esercizio del diritto di accesso degli interessati secondo quanto previsto dal Regolamento UE 2016/679 e dal D.Lgs. n. 51/2018;
indicazione della esatta collocazione di tutti gli impianti di videosorveglianza comunale con indicazione della natura e finalità degli stessi.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
158

Occorre inoltre disciplinare le modalità di nomina degli incaricati e dei preposti alla gestione dell'impianto di videosorveglianza nonché i casi di diretta visione delle immagini

Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

Particolarmente importanti sono:

- i **dati che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);
- i **dati rientranti in particolari categorie**: si tratta dei dati c.d. *"sensibili"*, cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i **dati genetici,** i **dati biometrici** e quelli relativi all'**orientamento sessuale**;

- i **dati relativi a condanne penali e reati**: si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, **altri dati personali** hanno assunto un ruolo significativo, come **quelli relativi alle comunicazioni elettroniche** (via Internet o telefono) e **quelli che consentono la geolocalizzazione**, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

LE PARTI IN GIOCO

Interessato è la persona fisica alla quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale, ecc. di Mario Rossi, questa persona è l'interessato (articolo 4, paragrafo 1, punto 1), del Regolamento UE 2016/679);

Titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento (articolo 4, paragrafo 1, punto 7), del Regolamento UE 2016/679);

Responsabile è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati (articolo 4, paragrafo 1, punto 8), del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. *"sub-responsabile"* (articolo 28, paragrafo 2).

Cosa è il diritto alla protezione dei dati personali?*

Il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8). Oggi è tutelato, in particolare, dal 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), oltre che da vari altri atti normativi italiani e internazionali e dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101.

In particolare, il Regolamento (UE) 2016/679 disciplina il trattamento dei dati personali indipendentemente dal fatto che questo sia effettuato o meno nell'Unione europea, sia quando svolto da titolari o responsabili stabiliti in Ue o in un luogo soggetto al diritto di uno Stato membro dell'Ue in virtù del diritto internazionale pubblico (per esempio l'ambasciata o la rappresentanza consolare di uno Stato membro), sia quando il titolare o il responsabile non è stabilito nell'Unione europea ma le attività di trattamento riguardano:

- l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione europea, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
- il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione europea.

Il Regolamento (UE) 2016/679 ha ampliato i diritti riconosciuti all'interessato con riferimento ai dati che lo riguardano, rendendoli maggiormente incisivi in una realtà permeata sempre più dal ricorso alle nuove tecnologie e all'utilizzo della rete.

Diritto di accedere ai propri dati personali

L'interessato ha il diritto di chiedere al titolare del trattamento (soggetto pubblico, impresa, associazione, partito, persona fisica, ecc.) se è in corso o meno un trattamento di dati personali che lo riguardano e, qualora il trattamento sia confermato:

- di ottenere una copia di tali dati;
- di essere informato su:
  a) le finalità del trattamento;
  b) le categorie di dati personali trattate;
  c) i destinatari dei dati;
  d) il periodo di conservazione dei dati personali;
  e) quale sia l'origine dei dati personali trattati;
  f) gli estremi identificativi di chi tratta i dati (titolare, responsabile, rappresentante designato nel territorio dello Stato italiano, destinatari);
  g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione;
  h) i diritti previsti dal Regolamento.

Ogni persona può tutelare i propri dati personali, in primo luogo, esercitando i diritti previsti dagli articoli da 15 a 22 del Regolamento (UE) 2016/679.

Come?

L'interessato può presentare un'istanza al titolare, senza particolari formalità (ad esempio, mediante lettera raccomandata, telefax, posta elettronica, ecc.). Su questo sito è disponibile un modulo che si può utilizzare per esercitare i predetti diritti.

L'istanza può essere riferita, a seconda delle esigenze dell'interessato, a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali che lo riguardano, comunque trattati.
All'istanza il titolare, deve fornire idoneo riscontro, ossia:

- senza ingiustificato ritardo, al più tardi entro 1 mese dal suo ricevimento;
- tale termine può essere prorogato di 2 mesi, qualora si renda necessario tenuto conto della complessità e del numero di richieste. In tal caso, il titolare deve comunque darne comunicazione all'interessato entro 1 mese dal ricevimento della richiesta.

Cosa fare se ritengo che il trattamento dei dati che mi riguardano non sia corretto o se la risposta ad un'istanza per l'esercizio dei diritti previsti dagli articoli 15-22 del Regolamento (UE) 2016/679 non perviene nei tempi indicati o non è soddisfacente?

Se ritiene che il trattamento dei dati che lo riguardano non è conforme alla disposizioni vigenti ovvero se la risposta ad un'istanza con cui esercita uno o più dei diritti previsti dagli articoli 15-22 del Regolamento (UE) 2016/679 non perviene nei tempi indicati o non è soddisfacente, l'interessato può rivolgersi all'autorità giudiziaria o al Garante per la protezione dei dati personali, in quest'ulimo caso mediante un reclamo ai sensi dell'articolo art. 77 del Regolamento (UE) 2016/679.

Il Regolamento europeo non prevede più l'istituto del ricorso per fare valere i diritti di accesso ai dati personali (che pertanto non è più esperibile davanti al Garante a partire dal 25 maggio 2018).

Strumenti di tutela

IL RECLAMO

Il reclamo al Garante è un atto circostanziato con il quale si rappresenta una violazione della disciplina rilevante in materia di protezione dei dati personali (articolo 77 del Regolamento UE 679/1996) e artt. da 140-bis a 143 del Codice. Al reclamo segue un'istruttoria preliminare e un eventuale successivo procedimento amministrativo formale che può portare all'adozione dei provvedimenti di cui all'articolo 58 del Regolamento.
Avverso la decisione del Garante è ammesso il ricorso giurisdizionale ai sensi degli articoli 143 e 152 del Codice e dell'articolo 78 del Regolamento.
La presentazione del un reclamo è gratuita.

SEGNALAZIONE

Chiunque può rivolgere, ai sensi dell'art. 144 del Codice, una segnalazione che il Garante può valutare anche ai fini dell'emanazione dei provvedimenti di cui all'art. 58 del Regolamento (indirizzo).

CHE COS'E' IL RECLAMO E COME SI PRESENTA AL GARANTE

Il reclamo è lo strumento che consente all'interessato di rivolgersi al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia di protezione dei dati personali (art. 77 del Regolamento (Ue) 2016/679 e artt. da 140-bis a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento) e di richiedere una verifica dell'Autorità.
Il reclamo può essere sottoscritto direttamente dall'interessato oppure, per suo conto, da un avvocato, un procuratore, un organismo, un'organizzazione o un'associazione senza scopo di lucro. In tali casi, è necessario conferire una procura da depositarsi presso il Garante assieme a tutta la documentazione utile ai fini della valutazione del reclamo presentato.
Il reclamante potrà far pervenire l'atto utilizzando la modalità ritenuta più opportuna, **consegnandolo a mano presso gli uffici del Garante** (all'indirizzo di seguito indicato) o mediante l'inoltro di:
a) **raccomandata A/R indirizzata a: Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 Roma**
b) **messaggio di posta elettronica certificata indirizzata a: protocollo@pec.gpdp.it**
In sede di prima applicazione, il reclamo e l'eventuale procura dovranno essere sottoscritti con firma autenticata, ovvero con firma digitale, ovvero con firma autografa (in tale ultimo caso, al reclamo dovrà essere allegata copia di un documento di riconoscimento dell'interessato/a in corso di validità).

AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
P.ZZA VENEZIA 11
00187 ROMA

Reclamo ex art. 77 del Regolamento (Ue) 2016/679 e artt. da 140-bis a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento

Diritto alla rettifica, alla cancellazione, alla limitazione del trattamento, alla portabilità dei dati personali

Il Regolamento (UE) 2016/679 (articoli da 15 a 22), ha ampliato i diritti riconosciuti all'interessato con riferimento ai dati che lo riguardano, rendendoli maggiormente incisivi nella nostra realtà permeata sempre più dal ricorso alle nuove tecnologie e all'utilizzo della rete. L'interessato può richiedere a chi sta trattando i suoi dati personali che questi siano:

a) rettificati (perché inesatti o non aggiornati), eventualmente integrando informazioni incomplete;

b) cancellati, se:

- i dati non sono più necessari ai fini del perseguimento delle finalità per le quali sono stati raccolti o trattati;
- l'interessato revoca il consenso o si oppone al trattamento; oppure
- i dati sono trattati illecitamente o devono essere cancellati per adempiere a un obbligo legale;

e se non vi sono altri trattamenti per i quali i dati sono considerati necessari (libertà di espressione e informazione, svolgimento di compiti nel pubblico interesse, trattamenti connessi alla sanità pubblica, ecc.).

c) limitati nel relativo trattamento, se:
- i dati non sono esatti o sono trattati illecitamente e l'interessato si oppone alla loro cancellazione;
- nonostante il titolare non ne abbia più bisogno ai fini del trattamento, i dati sono necessari all'interessato per fare valere un diritto in sede giudiziaria;

d) trasferiti ad un altro titolare (c.d. diritto alla portabilità), se il trattamento si basa sul consenso o su un contratto stipulato con l'interessato e viene effettuato con mezzi automatizzati.

Nota: Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Diritto di opposizione

E' possibile opporsi al trattamento dei propri dati personali:
a) per motivi connessi alla situazione particolare dell'interessato, da specificare nella richiesta;
b) (senza necessità di motivare l'opposizione) quando i dati sono trattati per finalità di marketing diretto.

Principi generali del trattamento di dati personali

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679, che qui si ricordano brevemente:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Il Regolamento (articolo 5, paragrafo 2) richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è il principio detto di "responsabilizzazione" (o accountability) che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1, del Regolamento, dove si afferma che "il titolare mette in atto misure tecniche e organizzative adeguate **per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento."**

Assicurare la liceità del trattamento di dati personali

Il Regolamento, come già previsto dal Codice in materia di protezione dei dati personali, prevede che ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 del Regolamento:
- consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Per quanto riguarda le **"categorie particolari di dati personali"** (articolo 9 del Regolamento), il loro trattamento è vietato, in prima battuta, a meno che il titolare possa dimostrare di soddisfare almeno una delle condizioni fissate all'articolo 9, paragrafo 2 del Regolamento, che qui ricordiamo:

- ❖ l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;

- il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per uno dei seguenti scopi:
  - per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
  - per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
  - per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
  - per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
  - per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
  - per motivi di interesse pubblico nel settore della sanità pubblica;
  - per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Per alcune di tali finalità sono previste limitazioni o prescrizioni ulteriori, anche nel diritto nazionale.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 181

Consenso

Quando il trattamento si fonda sul consenso dell'interessato, il titolare deve sempre essere in grado di dimostrare (articolo 7.1 del Regolamento) che l'interessato ha prestato il proprio consenso), che è valido se:

all'interessato è stata resa l'informazione sul trattamento dei dati personali (articoli 13 o 14 del Regolamento);

è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse. Il consenso deve essere sempre revocabile.

Occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (articolo 7.2), per esempio all'interno della modulistica.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 182

Non è ammesso il consenso tacito o presunto (per esempio, presentando caselle già spuntate su un modulo).
Quando il trattamento riguarda le "categorie particolari di dati personali" (articolo 9 Regolamento) il consenso deve essere "esplicito"; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – articolo 22).
Il consenso non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per le categorie particolari di dati di cui all'articolo 9 Regolamento).

Interesse vitale di un terzo
Si può invocare tale base giuridica per il trattamento di dati personali solo se nessuna delle altre condizioni di liceità può trovare applicazione (considerando 46).
Interesse legittimo prevalente di un titolare o di un terzo
Il ricorso a questa base giuridica per il trattamento di dati personali presuppone che il titolare stesso effettui un bilanciamento fra il legittimo interesse suo o del terzo e i diritti e libertà dell'interessato. Dal 25 maggio 2018, dunque, tale bilanciamento non spetta più all'Autorità, in linea di principio. Si tratta di una delle principali espressioni del principio di "responsabilizzazione" introdotto dal Regolamento (UE) 2016/679.
L'interesse legittimo del titolare o del terzo deve risultare prevalente sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.
Il Regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.
Si ricordi, inoltre, che il legittimo interesse non può essere invocato isolatamente quale base giuridica per il trattamento delle categorie particolari di dati personali (articolo 9, paragrafo 2, del Regolamento).

Trasparenza del trattamento: l'informativa agli interessati

Fatte salve alcune eccezioni, chi intende effettuare un trattamento di dati personali deve fornire all'interessato alcune informazioni anche per metterlo nelle condizioni di esercitare i propri diritti (articoli 15-22 del Regolamento medesimo).

QUANDO

L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del Regolamento) deve essere fornita all'interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati (se raccolti direttamente presso l'interessato: articolo 13 del Regolamento).
Nel caso di dati personali non raccolti direttamente presso l'interessato (articolo 14 del Regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevedeva l'articolo 13, comma 4, del Codice).

COSA

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del Regolamento e, in parte, sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.). Se i dati non sono raccolti direttamente presso l'interessato (articolo 14 del Regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.
In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.
Il Regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.
Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

COME

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: articolo 12, paragrafo 1, e considerando 58). Sono comunque ammessi "altri mezzi", quindi può essere fornita anche in forma orale, ma nel rispetto delle caratteristiche di cui sopra (articolo 12, paragrafo 1).

Il Regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (articolo 12, paragrafo 7); queste icone in futuro dovranno essere uniformate in tutta l'Ue attraverso l'intervento dalla Commissione europea.

In base al Regolamento, si deve porre particolare attenzione alla formulazione dell'informativa, che deve essere soprattutto comprensibile e trasparente per l'interessato, attraverso l'uso di un linguaggio chiaro e semplice. In particolare, bisogna ricordare che per i minori si devono prevedere informative idonee (anche considerando 58).

Un approccio responsabile al trattamento: Accountability

Il Regolamento pone l'accento sulla "responsabilizzazione" di titolari e responsabili, ossia, sull' adozione di comportamenti proattivi e tali da **dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento** (artt. 23-25, in particolare, e l'intero Capo IV del Regolamento). Dunque, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "data protection by default and by design" (articolo 25), ossia dalla necessità di configurare il trattamento **prevedendo fin dall'inizio le garanzie indispensabili** "al fine di soddisfare i requisiti" del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto previsto dall'articolo 25, paragrafo 1, del Regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel Regolamento rispetto alla gestione degli obblighi dei titolari: ossia il **rischio inerente al trattamento**. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35- 36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All'esito di questa valutazione di impatto, il titolare:

- potrà decidere se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero, se il rischio risulta ciononostante elevato;
- dovrà consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità avrà quindi il compito di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58 del Regolamento (dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento).

In conseguenza dell'applicazione del principio di accountability, dal 25 maggio 2018 non sono più previste :

- la notifica preventiva dei trattamenti all'autorità di controllo;
- una verifica preliminare da parte del Garante per i trattamenti "a rischio" (anche se potranno esservi alcune eccezioni legate a disposizioni nazionali, previste in particolare dall'articolo 36, paragrafo 5 del Regolamento).

Al loro posto, il Regolamento prevede in capo ai titolari l'obbligo (pressoché generalizzato) di tenere un registro dei trattamenti e, appunto, di effettuare valutazioni di impatto in piena autonomia con eventuale successiva consultazione dell'Autorità.

Principio di "responsabilizzazione" dei titolari e responsabili del trattamento: principali elementi

Rapporti contrattuali fra titolare e responsabile del trattamento

Il Regolamento **definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE e, quindi, al Codice privacy italiano.

Tuttavia, il Regolamento (articolo 28) prevede dettagliatamente le caratteristiche **dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti. Deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'articolo 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti", quali, in particolare:

- la natura, durata e finalità del trattamento o dei trattamenti assegnati
- le categorie di dati oggetto di trattamento
- le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel Regolamento

Inoltre, il Regolamento prevede **obblighi specifici in capo ai responsabili del trattamento, distinti da quelli pertinenti ai rispettivi titolari**. Ciò riguarda, in particolare:

- la tenuta del registro dei trattamenti svolti (articolo 30, paragrafo 2);
- l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (articolo 32);
- la designazione di un RPD-DPO, nei casi previsti dal Regolamento o dal diritto nazionale (articolo 37).

Una novità importante del Regolamento è la possibilità di designare sub-responsabili del trattamento da parte di un responsabile (articolo 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (articolo 82, paragrafo 1 e paragrafo 3).

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti - ma solo se non effettuano trattamenti a rischio (articolo 30, paragrafo 5) - **devono tenere un** registro delle operazioni di trattamento, i cui contenuti sono indicati all'articolo 30.

Si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. I contenuti del registro sono fissati nell'articolo 30. Tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Il registro deve avere **forma scritta**, anche elettronica, e deve essere esibito su richiesta al Garante.

Misure di sicurezza

Il titolare del trattamento, come pure il responsabile del trattamento, è obbligato ad adottare misure tecniche e organizzative **idonee a garantire un livello di sicurezza adeguato al rischio del trattamento** (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato).

Fra tali misure, il Regolamento menziona, in particolare, la pseudonimizzazione e la cifratura dei dati; misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; misure atte a garantire il tempestivo ripristino della disponibilità dei dati; procedure per verificare e valutare regolarmente l'efficacia delle misure di sicurezza adottate.

La lista di cui al paragrafo 1 dell'articolo 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Per questi motivi, non possono sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza poiché tale valutazione è rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da articolo 32 del Regolamento.

Vi è, inoltre, la possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate (articolo 32, paragrafo 3).

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 195

Notifica di una violazione dei dati personali

A partire dal 25 maggio 2018, tutti i titolari dovranno notificare al Garante le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (considerando 85). Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34.

I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli articolo 33 e 34 del Regolamento.

Tutti i titolari di trattamento devono in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provmenti adottati (articolo 33, paragrafo 5). È bene, dunque, adottare le misure necessarie a documentare eventuali violazioni, anche perché i titolari sono tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 196

Responsabile della protezione dei dati

La designazione di un "responsabile della protezione dati" (RPD) è finalizzata a facilitare l'attuazione della normativa da parte del titolare/responsabile (articolo 39). Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'articolo 35, oltre alla funzione di punto di contatto per gli interessati e per il Garante rispetto a ogni questione attinente l'applicazione del Regolamento.

La sua designazione è obbligatoria in alcuni casi (articolo 37), e il Regolamento delinea le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali.

I diritti degli interessati

I titolari del trattamento devono rispettare le modalità previste per l'esercizio di tutti i diritti da parte degli interessati, stabilite, in via generale, negli artt. 11 e 12 del Regolamento

- In primo luogo, il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti, il responsabile del trattamento è tenuto a collaborare con il titolare ai fini dell'esercizio di tali diritti (articolo 28, paragrafo 3, lettera e)).
- Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (, in particolare, articolo 11, paragrafo 2 e articolo 12, paragrafo 6).
- Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), pari a 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

- La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.
- Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive - anche ripetitive (articolo12, paragrafo 5) - ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (articolo 15, paragrafo 3). In quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (articolo 12, paragrafo 1; articolo 15, paragrafo 3).

Trasferimento dei dati all'estero

Verso Paesi appartenenti all'Unione europea

Non possono esservi limitazioni né divieti alla libera circolazione dei dati personali nell'Unione europea per motivi attinenti alla protezione dei dati (Articolo 1, paragrafo 3 del Regolamento). Pertanto, non vi sono limiti di alcun genere per quanto riguarda i flussi di dati dall'Italia verso altri Stati membri dell'Ue (e dello Spazio Economico Europeo: Islanda, Norvegia, Liechtenstein).

Verso Paesi non appartenenti all'Unione europea

Il trasferimento di dati personali verso Paesi non appartenenti all'Unione europea è vietato, in linea di principio.

Tale divieto può essere superato solo quando intervengano le seguenti specifiche garanzie (articoli da 44 a 49 del Regolamento UE 2016/679):

a) adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;

b) in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali tipo);
c) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (articolo 49 del Regolamento).
Sono altresì vietati trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (articolo 48 del Regolamento UE 2016/679). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all'articolo 49 del Regolamento medesimo. E' lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del titolare o dal diritto dell'Unione europea (articolo 49, paragrafo 4) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 201

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 202

FONDAMENTI DI LICEITA´ DEL TRATTAMENTO

Il regolamento conferma che ogni trattamento deve trovare fondamento in un´idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all´art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 196/2003 (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

In particolare: CONSENSO

Cosa cambia?
- Per i dati "sensibili" (si veda art. 9 regolamento) il consenso DEVE essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22). Si segnalano, al riguardo, le linee-guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251), qui disponibili: www.garanteprivacy.it/regolamentoue/profilazione.
- NON deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l´inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) DEVE essere in grado di dimostrare che l´interessato ha prestato il consenso a uno specifico trattamento.
- Il consenso dei minori è valido a partire dai 16 anni (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

In particolare: CONSENSO

Cosa non cambia?

- DEVE essere, in tutti i casi, libero, specifico, informato e inequivocabile e NON è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).

- DEVE essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

RACCOMANDAZIONI

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.

In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all´interessato (art. 7.2), per esempio all´interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20).

INTERESSE VITALE DI UN TERZO
Cosa cambia?
Si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione (si veda considerando 46)

INTERESSE LEGITTIMO PREVALENTE DI UN TITOLARE O DI UN TERZO
Cosa cambia?
Il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell´interessato NON SPETTA all´Autorità ma è compito dello stesso titolare; si tratta di una delle principali espressioni del principio di «responsabilizzazione» introdotto dal nuovo pacchetto protezione dati.
Cosa non cambia?
L´interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell´interessato per costituire un valido fondamento di liceità.
Il regolamento chiarisce espressamente che l´interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

RACCOMANDAZIONI

Il Regolamento offre alcuni criteri per il bilanciamento in questione *(si veda considerando 47)* e soprattutto appare utile fare riferimento al documento pubblicato dal Gruppo "Articolo 29" sul punto *(WP217)*.

Si confermano, inoltre, nella sostanza, i **requisiti indicati dall´Autorità nei propri provvedimenti in materia di bilanciamento di interessi** [si veda, per esempio, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680 con riguardo all´utilizzo della videosorveglianza; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6068256 in merito all´utilizzo di sistemi di rilevazione informatica anti-frode; ecc.] con particolare riferimento agli esiti delle verifiche preliminari condotte dall´Autorità, con eccezione ovviamente delle disposizioni che il Regolamento ha espressamente abrogato (per es.: obbligo di notifica dei trattamenti).I titolari dovrebbero condurre la propria valutazione alla luce di tutti questi principi.

Contenuti dell´informativa

I contenuti dell´informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare **DEVE SEMPRE** specificare i **dati di contatto del RPD-DPO (Responsabile della protezione dei dati-Data Protection Officer)**, ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest´ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti** (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all´autorità di controllo. Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l´informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l´interessato.

Tempi dell´informativa

Nel caso di dati personali non raccolti direttamente presso l´interessato *(art. 14 del regolamento)*, l´informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**NON** della registrazione) dei dati (a terzi o all´interessato) (diversamente da quanto prevede attualmente l´art. 13, comma 4, del Codice).

Modalità dell´informativa

Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell´informativa, che deve avere forma **concisa, trasparente, intelligibile per l´interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee *(si veda anche considerando 58)*.

L´informativa è data, **in linea di principio, per iscritto** e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: *si vedano art. 12, paragrafo 1, e considerando 58*), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra *(art. 12, paragrafo 1)*. Il regolamento ammette, soprattutto, l´utilizzo di **icone** per presentare i contenuti dell´informativa in forma sintetica, **ma solo "in combinazione" con l´informativa estesa** *(art. 12, paragrafo 7)*; queste icone dovranno essere identiche in tutta l´Ue e saranno definite prossimamente dalla Commissione europea.

Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l´esonero dall´informativa** *(si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall´articolo 23, paragrafo 1, di quest´ultimo)*, anche se occorre sottolineare che **spetta al titolare**, in caso di dati personali raccolti da fonti diverse dall´interessato, **valutare se la prestazione dell´informativa agli interessati comporti uno sforzo sproporzionato** *(si veda art. 14, paragrafo 5, lettera b))* – a differenza di quanto prevede l´art. 13, comma 5, lettera c) del Codice.

L´informativa *(disciplinata nello specifico dagli artt. 13 e 14 del regolamento)* deve essere fornita all´interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l´interessato – art. 13 del regolamento). Se i dati non sono raccolti direttamente presso l´interessato *(art. 14 del regolamento)*, l´informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare **la propria identità e quella dell´eventuale rappresentante nel territorio italiano**, le **finalità del trattamento**, i **diritti degli interessati** (compreso il diritto alla portabilità dei dati), se esiste un **responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati**.

RACCOMANDAZIONI

E´ opportuno che i titolari di trattamento **verifichino la rispondenza delle informative** attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione**, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del regolamento.

Il regolamento supporta chiaramente il concetto di **informativa "stratificata"**, più volte esplicitato dal Garante nei suoi provvedimenti [si veda http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680 relativo all´utilizzo di un´icona specifica per i sistemi di videosorveglianza con o senza operatore; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1246675 contenente prescrizioni analoghe rispetto all´utilizzo associato di sistemi biometrici e di videosorveglianza in istituti bancari], in particolare attraverso l´impiego di icone associate (in vario modo) a contenuti più estesi, che devono essere facilmente accessibili, e promuove **l´utilizzo di strumenti elettronici** per garantire la massima diffusione e semplificare la prestazione delle informative.

I titolari potranno, dunque, una volta adeguata l´informativa nei termini sopra indicati, **continuare o iniziare a utilizzare queste modalità** per la prestazione dell´informativa, comprese le icone che l´Autorità ha in questi anni suggerito nei suoi provvedimenti (videosorveglianza, banche, ecc.) – in attesa della definizione di icone standardizzate da parte della Commissione.

Dovranno essere adottate anche le **misure organizzative interne** idonee a garantire il rispetto della tempistica: il termine di 1 mese per l´informativa all´interessato è chiaramente un termine massimo, e occorre ricordare che l´art. 14, paragrafo 3, lettera a), del regolamento menziona in primo luogo che il **termine deve essere "ragionevole"**.

Poiché spetterà al titolare valutare lo **sforzo sproporzionato** richiesto dall´informare una pluralità di interessati, qualora i dati non siano stati raccolti presso questi ultimi, e salva l´esistenza di specifiche disposizioni normative nei termini di cui all´art. 23, paragrafo 1, del regolamento, sarà utile fare riferimento ai **criteri evidenziati nei provvedimenti** con cui il Garante ha riconosciuto negli anni l´esistenza di tale sproporzione (si veda, in particolare, il provvedimento del 26 novembre 1998 – http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39624; più di recente, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3864423 in tema di esonero dagli obblighi di informativa).

Il termine per la risposta all´interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; **il titolare deve comunque dare un riscontro all´interessato entro 1 mese dalla richiesta, anche in caso di diniego.**

Spetta al titolare valutare la complessità del riscontro all´interessato e **stabilire l´ammontare dell´eventuale contributo** da chiedere all´interessato, ma soltanto se si tratta di richieste **manifestamente infondate o eccessive** (anche ripetitive) *(art. 12.5)*, a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste **più "copie" dei dati personali** nel caso del diritto di accesso *(art. 15, paragrafo 3)*; in quest´ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il **riscontro all´interessato** di regola deve avvenire in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l´accessibilità; può essere dato **oralmente solo se così richiede l´interessato** stesso *(art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3)*.

La risposta fornita all´interessato non deve essere solo "intelligibile", ma anche **concisa, trasparente e facilmente accessibile**, oltre a utilizzare un **linguaggio semplice e chiaro**.

Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
218

Modalità per l´esercizio dei diritti

Le modalità per l´esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del regolamento.

Il titolare del trattamento deve agevolare l´esercizio dei diritti da parte dell´interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. **Benché sia il solo titolare a dover dare riscontro** in caso di esercizio dei diritti *(artt. 15-22)*, il responsabile è tenuto a collaborare con il titolare ai fini dell´esercizio dei diritti degli interessati *(art. 28, paragrafo 3, lettera e))*.

L´esercizio dei diritti è, in linea di principio, gratuito per l´interessato, ma possono esservi eccezioni *(si veda il paragrafo "Cosa cambia")*. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l´interessato, e quest´ultimo ha il dovere di fornirle, secondo modalità idonee *(si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6)*.

Sono ammesse **deroghe ai diritti** riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell´articolo 23 nonché di altri articoli relativi ad ambiti specifici *(si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica)*.

RACCOMANDAZIONI

E´ opportuno che i titolari di trattamento adottino le misure tecniche e organizzative eventualmente necessarie per favorire l´esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che – a differenza di quanto attualmente previsto – dovrà avere per impostazione predefinita forma scritta (anche elettronica). Potranno risultare utili le indicazioni fornite dal Garante nel corso degli anni con riguardo all´intelligibilità del riscontro fornito agli interessati e alla completezza del riscontro stesso [si vedano varie decisioni relative a ricorsi contenute nel Bollettino dell´Autorità pubblicato qui: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/766652, e più recentemente, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1449401 in materia di dati sanitari, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1290018 in materia di dati telematici].

Quanto alla definizione eventuale di un contributo spese da parte degli interessati, che il regolamento rimette al titolare del trattamento, l´Autorità intende valutare l´opportunità di definire linee-guida specifiche (anche sul fondamento delle determinazioni assunte sul punto nel corso degli anni: si veda in particolare la Deliberazione n. 14 del 23 dicembre 2004), di concerto con le altre autorità Ue, alla luce di quanto prevede l´Art. 70 del regolamento con riguardo ai compiti del Board.

Diritto di accesso (art. 15)

Cosa cambia?

Il diritto di accesso prevede **in ogni caso** il diritto di ricevere **una copia dei dati** personali oggetto di trattamento.

Fra le informazioni che il titolare deve fornire **non rientrano le "modalità" del trattamento**, mentre **occorre indicare il periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le **garanzie** applicate **in caso di trasferimento dei dati verso Paesi terzi**.

RACCOMANDAZIONI

Oltre al rispetto delle prescrizioni relative alla modalità di esercizio di questo e degli altri diritti *(si veda "Modalità per l´esercizio dei diritti")*, i titolari possono c**onsentire agli interessati di consultare direttamente, da remoto** e in modo sicuro, i propri dati personali (*si veda considerando 68)*.

Diritto di cancellazione (diritto all´oblio) (art.17)
Cosa cambia?
Il diritto cosiddetto "all´oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l´obbligo per i titolari (se hanno "reso pubblici" i dati personali dell´interessato: ad esempio, pubblicandoli su un sito web) **di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati,** compresi "qualsiasi link, copia o riproduzione" *(si veda art. 17, paragrafo 2)*.

Ha **un campo di applicazione più esteso** di quello di cui all´art. 7, comma 3, lettera b), del Codice, poiché l´interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento *(si veda art. 17, paragrafo 1)*.

Diritto di limitazione del trattamento (art. 18)
Cosa cambia?
Si tratta di un diritto **diverso e più esteso rispetto al "blocco" del trattamento** di cui all´art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile **non solo in caso di violazione** dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche **se l´interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare)** o **si oppone al loro trattamento** ai sensi dell´art. 21 del regolamento (in attesa della valutazione da parte del titolare).
Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell´interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

RACCOMANDAZIONI
Il diritto alla limitazione prevede che **il dato personale sia "contrassegnato"** in attesa di determinazioni ulteriori; pertanto, è opportuno che i titolari prevedano nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

Diritto alla portabilità dei dati (art. 20)
Cosa cambia?

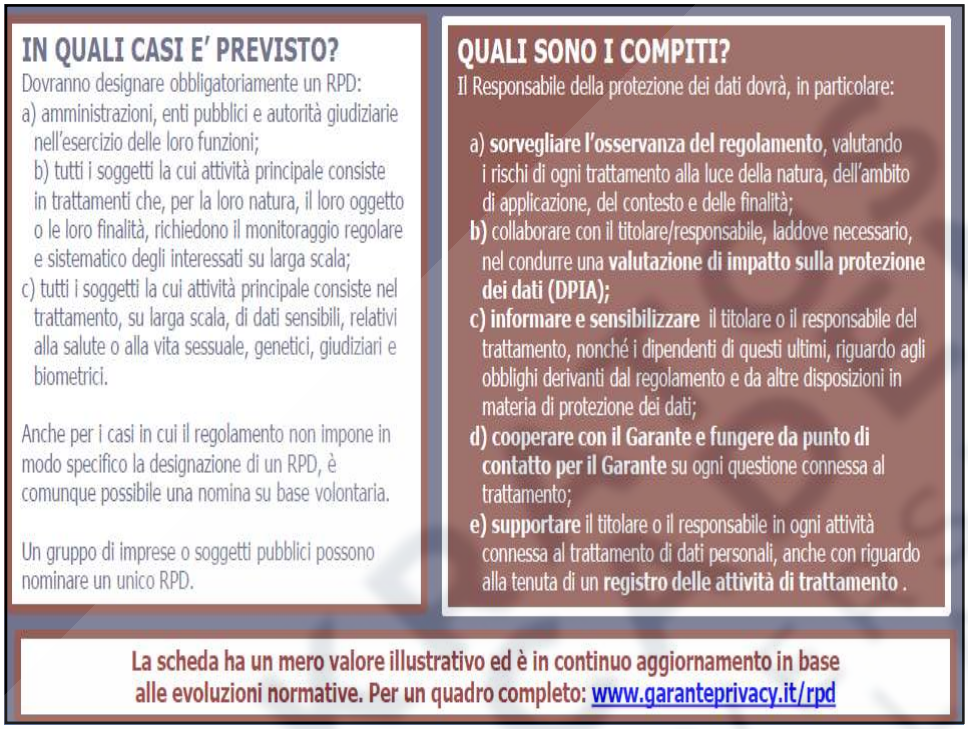
Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).
Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell´interessato o sulla base di un contratto stipulato con l´interessato** (quindi non si applica ai dati il cui trattamento si fonda sull´interesse pubblico o sull´interesse legittimo del titolare, per esempio), e solo i dati che siano stati **"forniti" dall´interessato** al titolare *(si veda il considerando 68 per maggiori dettagli)*.
Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall´interessato, se tecnicamente possibile.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 225

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 226


GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI
Il Responsabile della protezione dei dati (RPD)
La scheda presenta la figura del Responsabile della protezione dei dati (RPD)
in base a quanto previsto dal Regolamento (UE) 2016/679, dalle Linee-guida dell'EDPB
e dal Codice in materia di protezione dei dati personali (d.lgs. 196/2003)


KRATOS ACADEMY
UNIVERSITÀ POPOLARE
ESAARCO
CONFEDERAZIONE
TÜV SÜD
QUALI SONO I REQUISITI?
Il Responsabile della protezione dei dati, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:
1. possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;
2. adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;
3. operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (RPD/DPO esterno).
Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
228



IN QUALI CASI E' PREVISTO?

Dovranno designare obbligatoriamente un RPD:

a) amministrazioni, enti pubblici e autorità giudiziarie nell'esercizio delle loro funzioni;

b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria.

Un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.

QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati dovrà, in particolare:

a) **sorvegliare l'osservanza del regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;

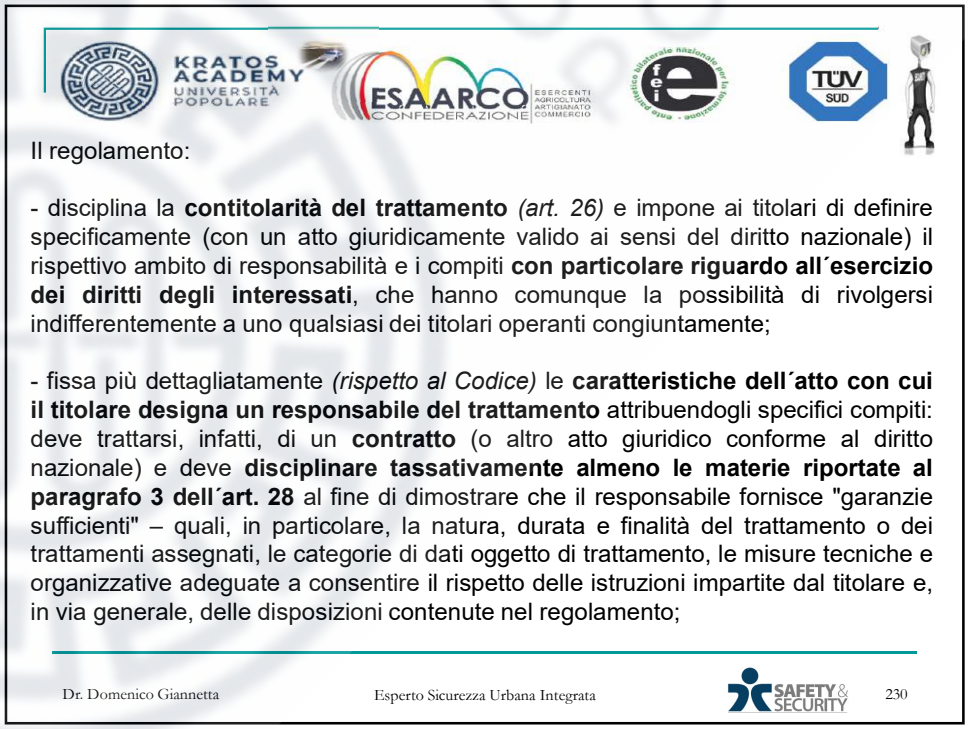
b) collaborare con il titolare/responsabile, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA);**

c) **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;

d) **cooperare con il Garante e fungere da punto di contatto per il Garante** su ogni questione connessa al trattamento;

e) **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento** .

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base alle evoluzioni normative. Per un quadro completo: www.garanteprivacy.it/rpd



Il regolamento:

- disciplina la **contitolarità del trattamento** *(art. 26)* e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all´esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

- fissa più dettagliatamente *(rispetto al Codice)* le **caratteristiche dell´atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell´art. 28** al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 230

- consente la **nomina di sub-responsabili del trattamento** da parte di un responsabile *(si veda art. 28, paragrafo 4)*, per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest´ultimo **risponde dinanzi al titolare dell´inadempimento dell´eventuale sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l´evento dannoso "non gli è in alcun modo imputabile" *(si veda art. 82, paragrafo 1 e paragrafo 3)*;

- prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti** svolti *(ex art. 30, paragrafo 2)*; l´adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti *(ex art. 32 regolamento)*; la **designazione di un RPD-DPO** (si segnalano, al riguardo, le linee-guida in materia di responsabili della protezione dei dati adottate dal Gruppo "Articolo 29", disponibili qui anche nella versione in italiano: www.garanteprivacy.it/regolamentoue/rpd), nei casi previsti dal regolamento o dal diritto nazionale *(si veda art. 37 del regolamento)*. Si ricorda, inoltre, che **anche il responsabile** non stabilito nell´Ue dovrà **designare un rappresentante** in Italia quando ricorrono le condizioni di cui all´art. 27, paragrafo 3, del regolamento – diversamente da quanto prevedeva l´art. 5, comma 2, del Codice.

Il regolamento definisce **caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice italiano). Pur non prevedendo espressamente la **figura dell´"incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l´autorità diretta del titolare o del responsabile" *(si veda, in particolare, art. 4, n. 10, del regolamento)*.

DESIGNATI

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 233

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 234

Il regolamento pone con forza l´accento sulla "responsabilizzazione" (accountability nell´accezione inglese) di titolari e responsabili – ossia, sull´**adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l´applicazione del regolamento** *(si vedano artt. 23-25, in particolare, e l´intero Capo IV del regolamento)*. Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Il primo fra tali criteri è sintetizzato dall´espressione inglese **"data protection by default and by design"** *(si veda art. 25)*, ossia dalla necessità di configurare il trattamento prevedendo fin dall´inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all´atto del trattamento stesso", secondo quanto afferma l´art. 25(1) del regolamento) e richiede, pertanto, un´analisi preventiva e un impegno applicativo da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento**. Quest´ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati *(si vedano considerando 75-77)*; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione *(si vedano artt. 35-36)* tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati adottate dal Gruppo "Articolo 29", qui disponibili: www.garanteprivacy.it/regolamentoue/DPIA). All´esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l´autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l´autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell´art. 58: dall´ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Dunque, l´intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà 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, appunto, di effettuazione di valutazioni di impatto in piena autonomia, con eventuale successiva consultazione dell´Autorità, tranne alcune specifiche situazioni di trattamento (vedi art. 36, paragrafo 5 del regolamento). Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l´erede dell´attuale Gruppo "Articolo 29") spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

Nei paragrafi seguenti si richiamano **alcune delle principali novità** in termini di adempimenti da parte di titolari e responsabili del trattamento.

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio *(si veda art. 30, paragrafo 5)*, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all´art. 30. Si tratta di uno **strumento fondamentale** non soltanto ai fini dell´eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all´interno di un´azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

RACCOMANDAZIONI

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell´organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un´accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell´art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell´ottica della complessiva valutazione di impatto dei trattamenti svolti.


GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI
Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017
Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679
COSA È?
È una procedura prevista dall'articolo 35 del Regolamento UE/2016/679 (RGDP) che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
PERCHÉ?
La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
242

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari**.

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT**.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248)

Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati. I titolari sono infatti tenuti non soltanto a garantire l´osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

Le linee-guida del WP29 offrono alcuni chiarimenti sul punto; in particolare, precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all´art. 35), chi debba condurla (il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di interpretarla come un processo soggetto a revisione continua piuttosto che come un adempimento una tantum.

Le linee-guida chiariscono, peraltro, anche quando una valutazione di impatto non sia richiesta: ciò vale, in particolare, per i trattamenti in corso che siano già stati autorizzati dalle autorità competenti e non presentino modifiche significative prima del 25 maggio 2018, data di piena applicazione del regolamento.

Il messaggio finale delle linee-guida (già sottoposte a consultazione pubblica) è che la valutazione di impatto costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri. In questo senso, la valutazione di impatto permette di realizzare concretamente l´altro fondamentale principio fissato nel regolamento 2016/679, ossia la protezione dei dati fin dalla fase di progettazione (data protection by design) di qualsiasi trattamento.

Misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, **la lista di cui al paragrafo 1 dell´art. 32 è una lista aperta e non esaustiva** ("tra le altre, se del caso"). Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza** *(ex art. 33 Codice)* poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l´attenzione anche sulla possibilità di utilizzare l´adesione a specifici codici di condotta o a schemi di certificazione per attestare l´adeguatezza delle misure di sicurezza adottate. Tuttavia, l´Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all´art. 6, paragrafo 1), lettere c) ed e) del regolamento) potranno restare in vigore (in base all´art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Notifica delle violazioni di dati personali

A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all´autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, **la notifica all´autorità** dell´avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell´art. 34, che coincidono solo in parte con quelle attualmente menzionate nell´art. 32-bis del Codice. **I contenuti della notifica** all´autorità e della comunicazione agli interessati sono indicati, **in via non esclusiva, agli artt. 33 e 34 del regolamento**. Si segnalano, al riguardo, le linee-guida in materia di notifica delle violazioni di dati personali del Gruppo "Articolo 29", qui disponibili www.garanteprivacy.it/regolamentoue/databreach.

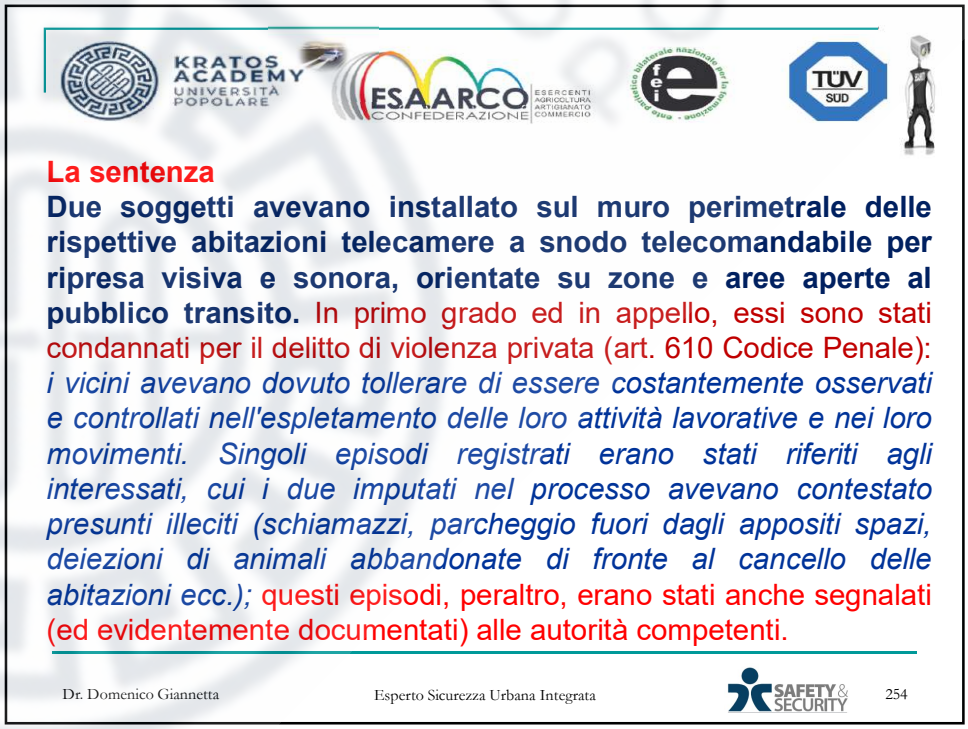
RACCOMANDAZIONI

Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all´autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati *(si veda art. 33, paragrafo 5)*; tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall´art. 32-bis, comma 7, del Codice. Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Responsabile della protezione dei dati

Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l´approccio responsabilizzante che è proprio del regolamento *(si veda art. 39)*, essendo finalizzata a facilitare l´attuazione del regolamento da parte del titolare/del responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all´art. 35. La sua designazione è obbligatoria in alcuni casi *(si veda art. 37)*, e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali: *si vedano artt. 38 e 39*) in termini che il WP29 ha ritenuto opportuno chiarire attraverso alcune linee-guida di recente pubblicazione, disponibili anche sul sito del Garante, e alle quali si rinvia per maggiori delucidazioni unitamente alle relative FAQ (si veda: http://www.garanteprivacy.it/regolamentoue/rpd).


Quale è quella vera?
Corte di Cassazione Sentenza n. 20527 del 07/03/2019
Videosorveglianza: non è violenza privata riprendere i vicini in zona di pubblico transito
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
253


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
La sentenza
Due soggetti avevano installato sul muro perimetrale delle rispettive abitazioni telecamere a snodo telecomandabile per ripresa visiva e sonora, orientate su zone e aree aperte al pubblico transito. In primo grado ed in appello, essi sono stati condannati per il delitto di violenza privata (art. 610 Codice Penale): i vicini avevano dovuto tollerare di essere costantemente osservati e controllati nell'espletamento delle loro attività lavorative e nei loro movimenti. Singoli episodi registrati erano stati riferiti agli interessati, cui i due imputati nel processo avevano contestato presunti illeciti (schiamazzi, parcheggio fuori dagli appositi spazi, deiezioni di animali abbandonate di fronte al cancello delle abitazioni ecc.); questi episodi, peraltro, erano stati anche segnalati (ed evidentemente documentati) alle autorità competenti.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
254

Art. 610 Codice penale - Fonti→ Codice penale→ LIBRO SECONDO - Dei delitti in particolare→ Titolo XII - Dei delitti contro la persona→ Capo III - Dei delitti contro la libertà individuale→ Sezione III - Dei delitti contro la libertà morale

Chiunque, con violenza [581] o minaccia (1), costringe altri a fare, tollerare od omettere qualche cosa (2) è punito con la reclusione fino a quattro anni (3).
La pena è aumentata [64] se concorrono le condizioni prevedute dall'articolo 339.

(1) La violenza è qui un concetto ampio, comprensivo anche della violenza diretta alle cose o a soggetti diversi dalla vittima. Ugualmente anche la minaccia comprende un ventaglio applicativo molto ampio, che prescinde quindi dal tipo di mezzi utilizzati o dal grado della minacci stessa.
(2) L'azione o omissione limitate dalla condotta violenta o minacciosa devono a loro volta essere determinate ovvero devono riguardare "qualche cosa", diversamente si applicano i reati di minaccia, percosse o lesioni.
(3) Alcuni autori riconoscono la necessità di ulteriore presupposto per la condotta di coartazione ovvero che questa dovrebbe essere illegittima, quindi non giustificata da alcun diritto (si pensi alle scriminanti degli artt. 51-54). Un caso discusso è quello del diritto di sciopero, garantito se non lede le altrui libertà, come nel caso delle cosiddette azioni di picchettaggio che consistono in atti diretti a costringere altri lavoratori ad astenersi dalla prestazione lavorativa, considerate penalmente rilevanti secondo la disposizione in esame.

L'uso di telecamere puntate sulla pubblica via non è di per sé illegittimo, se utilizzato per difendere beni primari, come la sicurezza o la proprietà privata, e purché le telecamere siano regolarmente segnalate.
La sentenza n. 20527/2019 della Cassazione fa luce sulla rilevanza penale dell'uso di sistemi di videosorveglianza, utilizzati nell'ambito di rapporti di vicinato non proprio idilliaci.
Nel caso oggetto della pronuncia, gli imputati erano stati condannati tanto in primo grado quanto (con pena ridotta) in sede di appello per il reato di violenza privata ex art. 610 del c.p.
Nella fattispecie, essi avevano installato, sul muro perimetrale delle rispettive abitazioni, telecamere a snodo telecomandabile per ripresa visiva e sonora, orientate su zone e aree aperte al pubblico transito, "costringendo" gli abitanti della zona, e in particolare le costituite parti civili, a tollerare di essere costantemente osservati e controllati nell'espletamento delle loro attività lavorative e nei loro movimenti.

Tali controlli venivano, poi, puntualmente riferiti e utilizzati per rimarcare la commissione di presunti illeciti (schiamazzi, parcheggio delle auto fuori dalle aree di sosta consentite, deiezioni animali abbandonante dinanzi al cancello delle abitazioni, e così via) che sarebbero stati perseguiti mediante esposti e denunce effettivamente poi inoltrati alle competenti autorità.
Gli imputati proponevano ricorso per cassazione, accolto dalla Suprema Corte.
Secondo i giudici di legittimità, il sistema di videosorveglianza che riprende il pubblico transito non può ritenersi di per sé illegittimo, se utilizzato per difendere beni primari, come la sicurezza o la proprietà privata, e sempre che le telecamere siano regolarmente segnalate.

In merito al reato di cui all'art. 610 c.p., la Cassazione ha ricordato il proprio consolidato orientamento secondo cui tale norma tutela la libertà psichica della persona; il requisito della violenza si identifica in qualsiasi atto o fatto, posto in essere dall'agente, che si risolva comunque nella coartazione della libertà fisica o psichica del soggetto passivo, il quale viene così indotto, contro la sua volontà, a fare, tollerare od omettere qualche cosa, indipendentemente dall'esercizio su di lui di un vero e proprio costringimento fisico.
Nel caso oggetto della pronuncia, il fatto contestato consisteva non nell'acquisizione di immagini relative alla condotta tenuta da cittadini sulla pubblica via, ma nel condizionamento esercitato su alcune persone (in particolare sulle costituite parti civili) dagli imputati, mediante la installazione di telecamere e l'utilizzo di immagini tratte dai filmati registrati dalle stesse.

Secondo la Corte, in tale fatto non sarebbero ravvisabili gli estremi della violenza privata: in primo luogo, l'installazione di sistemi di videosorveglianza con riprese del pubblico transito è un'attività di per sé tutt'altro che illecita; inoltre, non vi sarebbe stata nel caso concreto alcuna significativa costrizione della libertà di autodeterminazione.
Peraltro, la pronuncia in commento sottolinea come il valore fondamentale della libertà individuale possa essere bilanciato con altri, come quello della sicurezza. In materia di riprese tramite strumenti di videosorveglianza, inoltre, è previsto che chiunque installi tale sistema debba provvedere a segnalarne la presenza tramite appositi cartelli, così che chiunque si avvicini all'area interessata dalle riprese sia avvisato della presenza di telecamere già prima di entrare nel loro raggio di azione.
La Corte ha dunque annullato senza rinvio la sentenza impugnata perché il fatto non sussiste.

Nell'accogliere il ricorso degli imputati (assolvendoli dalle accuse addebitate nei precedenti gradi di giudizio), la Corte di Cassazione non ha assolutamente liberalizzato l'attività di videoripresa di aree pubbliche da parte di privati. Anzi, i supremi giudici hanno ricordato che esiste un nucleo di norme che regolano la materia della protezione dei dati personali (che deve essere rispettato) e, segnatamente, i presupposti e le modalità di installazione di impianti di videosorveglianza. Nulla di innovativo insomma: sono principi che la Corte ripete, con costanza, da un ventennio.

Alla base del ragionamento c'è il bilanciamento tra la libertà individuale e di autodeterminazione e la sicurezza e tutela del patrimonio; entrambi, secondo la Corte, sono interessi tutelati dal nostro ordinamento. In certi casi, è però possibile comprimere la libertà altrui per finalità di sicurezza, a patto che si rimanga nei confini della legalità.

Rispettando queste prescrizioni di legge, la condotta del privato di riprendere aree pubbliche non costituisce certamente reato. Al di là della materia penale, questo argomento si scontra anche con il diritto alla riservatezza, in cui il potere sanzionatorio del Garante della Privacy, soprattutto dopo la piena vigenza del GDPR, è molto rilevante. Insomma, **per evitare di commettere un reato basterà anche affiggere cartelli con cui si informano i terzi dell'operatività dell'impianto, ma ciò solo non è sufficiente per evitare altre sanzioni.**

Come essere in regola?

Le principali regole operative sono contenute nel Provvedimento in materia di videosorveglianza - 8 aprile 2010 emanato dall'Autorità Garante per la protezione dei dati personali. Il vademecum è pienamente applicabile, pur essendo ormai datato, laddove non incompatibile con i principi disciplinati dalla normativa in materia di protezione dei dati personali (in particolare, dal GDPR).

I principali (ma non gli unici) obblighi che ricaviamo sono:

- **il dovere di informativa:** chi installa un sistema di videosorveglianza deve informare tutti coloro che potrebbero ritentare nel campo di ripresa. Come? Con apposita cartellonistica, di cui è fornito anche un modello, e con cui si informano i terzi su chi sia il titolare del trattamento (cioè colui che ha installato l'impianto) e per quale finalità lo sta facendo (es. sicurezza, tutela del patrimonio);
- **misure di sicurezza:** devono essere messe in campo adeguate misure di sicurezza a protezione dei dati per prevenire perdite di dati, accessi di persone non autorizzate ai dati ecc. Le misure possono essere fisiche (nomina di soggetti che possono accedere, chiusura dei locali dove sono conservate le immagini, impianti anti intrusione ecc.) o informatiche (firewall, log eventi, accessi limitati, accesso con credenziali ecc.);
- **periodo limitato di conservazione delle immagini:** le immagini non possono essere conservate per più di 24 ore, salvo comprovate esigenze (es. furto per cui conservo le immagini da dare all'autorità giudiziaria).

Ai sensi dell'art. 35 GDPR il titolare del trattamento (chi ha installato l'impianto) deve effettuare valutazione d'impatto sulla protezione dati (c.d. DPIA, Data protection impact assessment).

Tale documento, che sostituisce la verifica preliminare di cui al provvedimento del Garante del 2010, è una valutazione di rischi legati al trattamento dei dati rispetto ai fini per cui il trattamento è effettuato. Si tratta di una analisi strutturata e piuttosto complessa, obbligatoria perché la videosorveglianza è un monitoraggio sistematico su larga scala. La DPIA va effettuata nella fase di progettazione dell'impianto o, quantomeno, prima di metterlo in funzione.

Non serve il consenso dei terzi (anche perché una sua raccolta sarebbe davvero cervellotica nonché un non senso), perché le riprese sono effettuate per un legittimo interesse di chi sorveglia gli spazi pubblici a tutela di un suo interesse.
Questo punto è anche ripreso dalla Corte di Cassazione nella sentenza citata, che si ispira alla giurisprudenza della Corte di Giustizia Europea. Il legittimo interesse, però, va verificato caso per caso: non è sempre detto che, per esempio, alcune deiezioni canine depositate di fronte a casa nostra possano giustificare un impianto di videosorveglianza, dipende dal contesto concreto. Non è semplice stabilire a priori se un interesse sia legittimo o meno; una delle poche certezze è costituita dagli istituti di credito: visto che una banca maneggia denaro contante (anche se sempre meno) e custodisce altri beni preziosi, è nel suo legittimo interesse tutelare il patrimonio proprio e dei clienti e la videosorveglianza è uno strumento importante a ciò dedicato.

Il Tribunale Amministrativo Regionale per il Lazio, Sezione Seconda Bis, ha chiarito che **qualsivoglia sistema di videosorveglianza installato presso una via "aperta" al pubblico (seppur privata) bisogna di espressa autorizzazione dell'Amministrazione Comunale,** in mancanza della quale può essere immediatamente sospeso il trattamento dei dati e ordinata la rimozione dell'apparato di videosorveglianza.

Presupposto per tale regola è che la rete stradale sia aperta al pubblico transito facendo sorgere in capo al Comune il diritto di gestirla poiché assoggettata a servitù di uso pubblico ("*dicatio ad patriam*").
Ne discende che le aree sottoposte a "pubblico" passaggio possano essere video sorvegliate solo tramite impianti gestiti dal Comune.

Infatti, solo alla Pubblica Amministrazione territoriale è demandato il fine della prevenzione dei reati e del controllo del territorio per la tutela della sicurezza urbana secondo quanto stabilito dalle regole in materia di protezione dei dati personali dettate dalla direttiva 2016/680 (direttiva Polizia).

Pertanto, a tale tipo di trattamento non si applicano le regole del Regolamento europeo 2016/679 (GDPR) anche laddove siano i privati ad installare telecamere rivolte verso aree pubbliche, posto che in tal caso occorre sempre un accordo formale con il Comune con cui questi sia indicato quale unico ed esclusivo gestore dell'impianto di videosorveglianza e che provveda al trattamento dei dati nei richiamati fini di polizia e consentendo così alle forze di Polizia locali di avere l'accesso esclusivo alle telecamere installate per motivi di sicurezza.

Invero, l'installazione di impianti di videosorveglianza da parte di privati è consentita solo in rapporto all'area di stretta pertinenza della proprietà privata, on esclusione di aree pubbliche o soggette al pubblico transito, per le quali, invece, l'installazione di impianti del genere compete al Comune per le finalità di prevenzione e tutela della pubblica incolumità.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 271

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 272

Molti condomini si avvalgono di sistemi di videosorveglianza per tutelare la sicurezza degli inquilini e delle parti comuni. È dunque frequente che l'amministratore faccia installare apposite videocamere nei punti nevralgici dell'edificio: cortile, androne, pianerottoli delle scale, ecc..

Le riprese vanno effettuate nel rispetto della privacy, nel senso che non si può puntare l'occhio della telecamera nella proprietà esclusiva dei condòmini: ad esempio, sarà lecita la telecamera che filma ciò che accade nel cortile, in quanto area comune, mentre non lo sarà quella che, posta sul pianerottolo, riesce a riprendere ciò che accade all'interno dell'abitazione appena si apre la porta.

Al di là di ciò, occorre sapere che **le riprese delle videocamere condominiali sono utilizzabili in sede penale non solo contro eventuali malviventi e topi di appartamento, ma anche contro i condòmini stessi che dovessero macchiarsi di qualche crimine.**

Tanto è stato ribadito dalla **Corte di Cassazione** (Sentenza del 15 luglio 2020, n. 21027), secondo cui sono utilizzabili nel processo penale non solo le riprese provenienti dalle videocamere condominiali ma anche le immagini estrapolate da un **sistema di videosorveglianza privato** installato nel rispetto della normativa vigente e senza violazione dei luoghi di privata dimora.

Videosorveglianza in condominio: come funziona?

Prima di analizzare il caso affrontato dalla Suprema Corte che ha condotto quest'ultima a ribadire il principio secondo cui sono utilizzabili in sede penale le riprese delle videocamere condominiali, **è bene fare brevemente chiarezza su come funziona la videosorveglianza in condominio.**

Innanzitutto, va detto che **ogni singolo condomino può installare un proprio sistema di videosorveglianza senza chiedere il consenso dell'assemblea o dell'amministratore, se è per la propria sicurezza.**

È dunque possibile che le proprie telecamere riprendano una **zona comune** (cioè, condominiale) come il cortile o il **pianerottolo**, purché non catturino immagini della proprietà privata altrui.

È legale perciò installare una videocamera di sicurezza davanti alla propria porta se l'occhio della telecamera, pur inquadrando il pianerottolo, non riprenda la soglia di casa del vicino.

Secondo la Corte di Cassazione (Cass., sent. n. 34151 del 12 luglio 2017), ai fini della integrazione del **reato di interferenze illecite nella vita privata** (art. 615-bis c.p.), deve escludersi che le scale condominiali ed i relativi pianerottoli siano luoghi di privata dimora cui estendere la tutela penalistica alle immagini riprese, trattandosi di zone che non assolvono alla funzione di consentire l'esplicazione della vita privata al riparo di sguardi indiscreti, essendo destinati all'uso di un numero indeterminato di soggetti.

Quanto detto, però, va meditato alla luce di un'altra considerazione: **non è possibile riprendere una zona condominiale quando questa non sia strettamente collegata con il proprio diritto alla sicurezza.**
In altre parole, **mentre è più che legittimo installare una videocamera privata sul proprio pianerottolo (purché riprenda solo l'area comune e il proprio ingresso), potrebbe non esserlo acquistare, a proprie spese, un'ulteriore telecamera, questa volta però installandola direttamente nell'androne comune, così da poter tenere sotto controllo tutti coloro che entrano in condominio.**
Nel caso appena prospettato, sebbene la videosorveglianza sia realizzata a tutela della sicurezza, c'è senza dubbio una **violazione della privacy**, visto che il singolo condomino può disporre di un impianto di videocamere limitatamente alla propria abitazione e a tutto ciò che è davvero indispensabile a difenderla.

E così, se è ammesso, entro stretti limiti, la possibilità di riprendere parte del pianerottolo antistante al proprio uscio di casa, non sarà lecito installare una telecamera in una zona condominiale che non è direttamente collegabile alla sicurezza della propria abitazione.
Questo discorso non vale, ovviamente, se l'impianto di videosorveglianza è **deliberato dall'assemblea**: in tale evenienza, l'amministratore potrà senza dubbio far installare l'impianto in tutte le parti comuni, avendo cura di non violare la riservatezza delle aree di proprietà esclusiva.

Utilizzabilità in sede penale delle riprese in condominio: il caso

Ricorreva in Corte di Cassazione un imputato condannato per molteplici reati (minacce, violenze, danneggiamenti, ecc.) commessi in ambito condominiale.

Secondo la difesa, le prove utilizzate per dimostrare la responsabilità penale del predetto sarebbero inutilizzabili perché acquisite in violazione di legge.

Per la precisione, la pubblica accusa si era avvalsa di immagini provenienti da telecamere che riprendevano costantemente il lastrico solare e il giardino, parti integranti della dimora dell'imputato e, pertanto, luoghi di esclusiva pertinenza.

Per corroborare la propria tesi la difesa dell'imputato richiama l'orientamento della **Corte di Cassazione (Sez. Un., n. 26795 del 2006) che escludono l'utilizzabilità di registrazioni svolte con modalità illegittime in quanto relative a persone o cose che si captano in contrasto con norme di legge.**

Utilizzabilità in sede penale delle riprese condominiali: la decisione

La Corte di Cassazione, con la sentenza in commento (15 luglio 2020, n. 21027), rigetta il ricorso proposto dall'imputato.

Secondo la Suprema Corte, **le riprese prodotte in giudizio, seppur provenienti da un sistema di videosorveglianza privato, riguardano parti di proprietà comune dell'edificio e, pertanto, sono pienamente utilizzabili in giudizio.**

Per la precisione, le videoriprese sono state effettuate in luogo anche di **pertinenza condominiale**, ove oggetto di registrazione sono parti comuni della proprietà della parte civile.

Secondo la Suprema Corte, **sono legittime le immagini registrate che derivano, come nel caso al vaglio, da videoregistrazioni provenienti da privati, installate a fronte di esigenze di sicurezza delle parti comuni, poi acquisite come prove documentali ex art. 234 c.p.p. Sicché, i fotogrammi estrapolati da detti filmati non possono essere considerati prove illegittimamente acquisite e non ricadono nella sanzione processuale di inutilizzabilità.**

Videoriprese per dimostrare i reati condominiali

La sentenza in commento si pone nel solco di granitico insegnamento del giudice di legittimità. Ad esempio, **secondo la Corte di Cassazione (sent. n. 32544 del 19 novembre 2020), per dimostrare la commissione di reati in condominio le registrazioni delle aree comuni possono essere utilizzate nel processo.**

Secondo i giudici, le registrazioni video e audio effettuate tramite telecamere poste per esigenze di sicurezza delle parti comuni di edifici condominiali, pur non essendo registrazioni effettuate dalla polizia giudiziaria e non potendo essere assimilate alle **intercettazioni**, possono comunque essere utilizzate come elemento probatorio nel processo penale.

Non ci sono dubbi che siano utilizzabili in sede penale le riprese delle videocamere condominiali, purché ovviamente siano rispettose dell'inviolabilità della proprietà privata.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 285

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 286

Sempre più frequentemente nella quotidiana attività dei comandi di Polizia Locale il personale si trova a dover affrontare **esposti, segnalazioni o denunce relative ad effettivi o presunti utilizzi illeciti di telecamere di videosorveglianza private installate dai cittadini a difesa della loro proprietà, abitazioni o attività commerciali** in alcuni casi anche interfacciate e connesse con possibili altri interlocutori quali per esempio le società di vigilanza privata che di fatto gestiscono e controllano per conto loro gli impianti.

In altri casi, secondo quanto previsto già dai **Decreti Sicurezza del 2017** tali impianti sono realizzati e manotenuti dai privati che ne cedono il totale controllo alla Polizia Locale ed eventualmente condivisi mediante la sottoscrizione di patti per la sicurezza anche con le altre forze di polizia, andando così ad implementare le aree poste sotto videosorveglianza all'interno delle aree cittadine.

Ma come comportarsi?
Quale è la disciplina in vigore?
Quali le sanzioni previste e le competenze in ambito di accertamento?
Quali sono i limiti operativi e i doveri istituzionali della Polizia Locale.

Da un punto di visto normativo occorre ricordare come anche **gli impianti di videosorveglianza privata rientrano, molto spesso anche se non sempre nell'attività di trattamento dati e conseguentemente gli interessati devono muoversi secondo i dettami del GDPR adottando tutte le misure richieste dal caso.**

Trattandosi poi di attività di natura esclusivamente privata tale attività non troverà applicazione la **Direttiva 2016/680 del Parlamento europeo e del Consiglio d'Europa**, 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.

Tale direttiva che in Italia è stata recepita con l'emanazione del **Decreto Legislativo 18 marzo 2018 n. 51** che introduce la regolamentazione delle protezione delle persone fisiche con riferimento al trattamento dei dati da parte delle autorità a fini di **prevenzione, investigazione e repressione di reati** e appunto non tocca direttamente i privati se non nella misura in cui gli impianti siano collegati e ceduti alle forze di polizia o allorquando i filmati siano acquisiti per indagini dai corpi di polizia giudiziaria.

L'installazione di impianti di videosorveglianza da parte di privati.

Per prima cosa occorre ricordare che l'installazione di sistemi di videosorveglianza di un portone di ingresso di una civile abitazione o di un esercizio commerciale non trova attuazione la disciplina generale del Codice della Privacy, ma è opportuno sottolineare che al fine di evitare di incorrere nel reato di interferenza illecite nella vita privata (art.615 bis c.p.), l'angolo della 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) o ad ambiti antistanti l'abitazione di altri condomini o edifici.

Specie poi per gli **esercizi commerciali andrà operata particolare attenzione ad evitare di riprendere porzioni di strada pubblica** in quanto tale attività risulterebbe illecita, non potendo il privato video controllare la pubblica via in quanto privo delle necessarie qualifiche finalità di legge che riserva tale compito alle sole forze di Polizia.

Infatti **per quanto concerne i privati la finalità unica è sempre solo quella della tutela della proprietà privata non potendo invece mai integrare per natura stessa del titolare del trattamento quelle di polizia e di sicurezza pubblica.**

Inoltre è opportuno ricordare che nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, la conservazione temporanea dei dati deve essere commisurata al tempo necessario e predeterminato a raggiungere la finalità perseguita **(massimo 72 ore).**

In questi casi **il sistema di videosorveglianza impiegato dovrà essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.**

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata. A tal fine, si può utilizzare **il modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, individuato dall'apposito cartello previsto dalla legge che deve essere collocato prima del raggio di azione della telecamera,** anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti.

L'impianto normativo nazionale in materia trova riscontro anche in quanto stabilito dalla Corte di giustizia europea, con la sentenza dell'11 dicembre 2014, resa nella causa C-212/13, secondo la quale la legge sulla privacy si applica anche agli impianti installati per proteggere la propria abitazione se riprendono la via pubblica.

In questi casi deve essere bilanciato, però, l'interesse alla riservatezza con l'interesse alla tutela dei propri beni e della propria incolumità.
Con la **sentenza la Corte Ue**, in primo luogo, **ha chiarito che le riprese con la telecamera di famiglia rappresentano un trattamento di dati personali:** questo perché l'immagine di una persona registrata da una telecamera consente di identificare la persona interessata e costituisce un trattamento automatizzato.
In secondo luogo non è possibile considerare questo trattamento di dati come un trattamento effettuato da persone fisiche per scopi esclusivamente personali: una qualifica di questo tipo implicherebbe esclusione dell'applicazione della normativa sulla privacy.

Pertanto l'esenzione prevista dalla Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 (relativa alla tutela delle persone fisiche riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati) rispetto al trattamento di dati effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico deve essere interpretata in modo restrittivo nel senso che una videosorveglianza che si estende allo spazio pubblico e che, di conseguenza, è diretta al di fuori della sfera privata della persona che tratta i dati non può essere considerata un'attività esclusivamente personale o domestica.
Fatta questa doverosa premessa proviamo quindi a esaminare le singole situazioni e ad indicare quali procedure di accertamento e eventuale sanzionamento i Comandi possono mettere in atto alla luce delle competenze riservate dalla legge e del sistema sanzionatorio profondamente mutato con l'introduzione del GDPR.

Esercizio commerciale o residenza privata le cui telecamere riprendono anche parte di pubblica via.

Questa è una delle possibili situazioni di irregolarità più facilmente riscontrabili.

La ripresa della pubblica via da parte di un privato è ovviamente vietata in quanto non supportata dalle necessarie e finalità di legge.

Certamente gli esercizi commerciali possono installare impianti di videosorveglianza avendo cura di fornire ai cittadini mediante l'apposizione dei consueti cartelli la necessaria informativa in formato minimo ma dovranno avere particolare cura affinchè le telecamere stesse non riprendano porzioni di strada o pubblica via.

Infatti non bisogna però dimenticare che secondo quanto stabilito dalla sentenza della Corte di Giustizia Europea quarta sezione, C-212/13, 11 dicembre 2014 **l'utilizzo di un sistema di videosorveglianza, installato da un privato sulla sua abitazione per proteggere i beni, la salute e la vita dei proprietari dell'abitazione, se in grado di riprendere anche lo spazio pubblico, non costituisce più un trattamento dei dati effettuati per l'esercizio di attività a carattere esclusivamente personale, e pertanto, deve avvenire nel rispetto della normativa in materia di dati personali.**

La ripresa infatti di luoghi pubblici diversi dall'ingresso delle attività commerciale o dell'abitazione privata può costituire un illecito trattamento di dati sanzionato secondo le previsioni normative degli artt. 83 e 84 GDPR con sanzioni amministrative pecuniarie piuttosto gravose.

In particolare, l'art. 83 del GDPR distingue due gruppi di sanzioni amministrative.

Nel primo gruppo rientrano le violazioni cosiddette di minore gravità, per le quali sono previste le sanzioni amministrative pecuniarie di importi fino a 10 milioni di euro o, per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, che riguardano in particolare le violazioni degli obblighi imposti tra gli altri al titolare ed al responsabile del trattamento (artt. 8, 11, da 25 a 39, 42 e 43 GDPR).

Nel secondo gruppo di sanzioni, rientrano le sanzioni più pesanti in considerazione della maggiore gravità delle fattispecie a cui sono ricondotte, che ammontano fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore che riguardano tra gli altri le violazioni dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9; e dei diritti degli interessati a norma degli articoli da 12 a 22.

In materia però, secondo il nuovo impianto sanzionatorio e di accertamento la Polizia Locale non ha competenza specifica che rimane invece in capo al Garante della Privacy ai suoi uffici e a specifici uffici delle forze di polizia all'uopo individuati formati e strutturati e con i quali sono stati sottoscritti specifici protocolli in materia.

Infatti il GDPR individua nell'autorità nazionale di controllo l'organo competente ad irrogare le sanzioni che in Italia ai sensi dell'art. 15, co. 3 del d.lgs. 101/2018 **è il Garante per la protezione dei dati personali.**

Alla luce di questo nuovo e complesso impianto sanzionatorio nel nostro ordinamento, l'organo preposto ai controlli ed all'irrogazione di sanzioni amministrative è l'Autorità Garante per la protezione di dati personali, detto anche **Garante per la Privacy**, che è un'autorità indipendente, in forma collegiale, già prevista dalla Direttiva 95/46/CE.

Ma il Garante non è l'unico organo preposto ai controlli.

I procedimenti sanzionatori, infatti, possono essere iniziati anche a seguito di accertamenti svolti dai **Corpi di Polizia dello Stato specializzati (Polizia Postale)** e in particolare dalla **Guardia di Finanza** (Nucleo Speciale Privacy), con cui è siglato protocollo operativo con l'Autorità Garante, non avendo quest'ultima personale di fatto sufficiente a gestire efficacemente tutte le violazioni segnalate.

In ogni caso al termine dell'attività istruttoria sarà lo stesso Garante **ad emanare un'ordinanza ingiunzione** con la quale verrà comminata la sanzione amministrativa.

Ma allora cosa può fare la Polizia Locale e come deve comportarsi?

- Intervenire sul posto e verificare l'effettiva situazione.
- **Verificare** la presenza dei cartelli di area sottoposta a videosorveglianza costituenti informativa minima sul trattamento dati.
- **Prendere visione** dell'orientamento delle telecamere e se effettivamente le stesse dovessero inquadrare zone più o meno ampie della pubblica via con particolare riguardo ad esempio alla carreggiata stradale con eventuale possibilità pe le stesse di riprendere in modo chiaro le targhe dei veicoli intransito.

- **Constatato** il fatto la soluzione più veloce e consigliabile di fronte soprattutto a interventi tecnici immediatamente eseguibili volti al riorientamento delle telecamere è quello di diffidare l'interessato anche solo verbalmente e di invitarlo ad un immediato adeguamento dell'impianto.
- **Di fronte a interventi tecnici** non immediatamente eseguibili la diffida con l'invito a sanare la situazione potenzialmente illecita potrebbe essere fatta anche in forma scritta.

- **Nel caso in cui invece l'irregolarità** fosse in modo evidentemente macroscopica o che a seguito delle diffide scritte o verbale l'interessato non dovesse provvedere la Polizia Locale dovrebbe procedere con la redazione di specifico e apposito verbale di accertamento ex art. 13 Legge 689/81 con il quale andranno specificate la località interessata, gli eventuali esposti o segnalazioni che hanno dato il via al controllo, eventuali inviti o diffide alla regolarizzazione le generalità del proprietario dell'esercizio commerciale o dell'abitazione privata e se diverso del titolare del trattamento, l'indicazione se l'impianto di videosorveglianza è auto gestito o affidato a società di vigilanza privata e quale sa il campo di inquadratura delle telecamere specificando qual parti di pubblica via siano riprese.
- **Gli esiti degli accertamenti** con l'esposizione dei fatti andranno trasmessi via pec direttamente al Garante per la Privacy o in alternativa previo preventivi accordi con il Nucleo Speciale Privacy della Guardia di Finanza che ha sede a Roma o con i Comandi territorialmente competenti della Polizia Postale.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 309

Per quanto riguarda ulteriori eventuali profili di natura penale occorre ricordare che la **Corte di Cassazione, sez. V Penale, con la sentenza del 13 maggio 2019, n. 20527 ha stabilito che nel caso di telecamere installate dal privato finalizzate a proteggere la propria sicurezza che dovessero puntare sulla pubblica via nel caso in cui la loro presenza sia correttamente segnalata a norma di legge con i relativi cartelli tale fatto non costituisce però il reato di violenza privata di cui all'art 610 c.p.**

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 310

Infine si rammenta che **l'utilizzo di telecamere all'interno di locali commerciali va segnalato mediante l'apposizione dei relativi avvisi anche all'esterno del negozio come ribadito dalla Corte di Cassazione che con la sentenza della sezione II civile n 13633 del 5 luglio 2016** che ha confermato che non è sufficiente l'affissione dei cartelli all'interno dei locali commerciali.

L'interferenza illecita nella vita privata mediante telecamere di videosorveglianza.

Diverso è il caso in cui la Polizia Locale dovesse essere chiamata in causa per presunte violazioni rientranti nella fattispecie di reato di interferenza illecita nella vita privata.

Tale fattispecie si può configurare nelle situazioni in cui le telecamere di un privato orientate in modo da riprendere anche od esclusivamente la proprietà privata altrui.

Il dispositivo dell'art. 615 bis c.p. così recita:

Chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni.

Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo.

I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato.

In proposito occorre chiarire che **il richiamo esplicito all'art. 614 individua per la sussistenza del reato stesso solo l'abitazione o il luogo di privata dimora, o nelle appartenenze di essi.**

Pertanto l'ipotesi di reato sarà valida anche per i pianerottoli, cortili, i giardini o i garage mentre dovranno essere escluse proprietà private diverse dalle abitazioni o dimore quali negozi uffici o luoghi di lavoro.

La seconda precisazione porta ad osservare che **il reato in questione è un delitto e pertanto richiede come elemento soggettivo il dolo ovvero l'intenzionalità della condotta.** Non è pertanto sufficiente constatare l'errato orientamento dell'inquadratura di una telecamera privata che dovesse anche inquadrare l'abitazione o il cortile altrui, ma andrà ricercato il dolo ravvisabile meglio in casi ove le telecamere fossero intenzionalmente dirette sulla proprietà altrui in modo esclusivo, la mancata e voluta regolazione delle inquadrature anche a seguito di lamentela della parte offesa o diffida da parte dell'interessato, del suo legale o delle forze di polizia.

Non risultano quindi perseguibili sotto il profilo penale in questione situazioni in cui un privato installa delle telecamere che inquadrano legittimamente la propria proprietà e in modo parziale non voluto ed accidentale quella altrui, salvo i casi in cui lo stesso avvisato e richiesto di porre rimedio alla questione non dovesse attivarsi in tal senso.

Infine condizione necessaria per la procedibilità del reato è la presentazione nei termini di legge, ricorrenti da quando la parte offesa è venuta a conoscenza della interferenza illecita, della prevista denuncia querela.

La competenza in merito al reato in questione è del Tribunale monocratico.

Da un punto di vista operativo la Polizia Locale dovrà:

- Raccogliere la denuncia querela;
- Eseguire sopralluogo per accertare la situazione e lo stato dei luoghi redigendo eventuale verbale di sopraluogo;
- Identificare il presunto autore del reato;
- Esperire eventuale tentativo di conciliazione tra le parti, o prima della presentazione della querela da parte delle perdona offesa o in seguito raccogliendo così l'eventuale remissione ed accettazione della querela;
- Redigere verbale di identificazione, elezione di domicilio e nomina del difensore a carico dell'indagato;
- Raccogliere sue eventuali spontanee dichiarazioni
- Redigere annotazione di p.g. sull'attività di indagine svolta;
- Trasmettere la relativa CNR alla competente Procura della Repubblica

Le liti tra vicini per inquadrature che vanno oltre la proprietà dell'interessato.

Non di rado giungono ai Comandi di Polizia Locale anche segnalazioni, esposti o richieste di intervento relative a diatribe tra vicini o condomini relativo alla collocazione di telecamere che oltre a riprendere la proprietà dell'interessato entrano nella presunta sfera della proprietà altrui.

Si fa rifermento a situazioni di minore gravità quali ad esempio le telecamere che poste nel cortile condominiale a controllo di un'auto privata riprendono anche l'auto del vicino, telecamere poste all'ingresso di un'abitazione privata che inquadrano anche la tromba delle scale condominiali o situazioni analoghe.

In questi casi se la videosorveglianza non interessa la pubblica via l'interessato non deve adempiere a particolari adempimenti in materia di trattamento dati e quindi non vi sono profili sanzionatori amministrativi per violazione del GDPR.
Infatti nei casi in cui l'installazione viene effettuata da persone fisiche per fini esclusivamente personali non si applicherà la disciplina del Codice a patto che i dati e quindi le immagini non vengano comunicati in modo sistematico a terzi o diffusi.
Parimenti **quando l'angolatura delle telecamere non invade gli spazi della privata dimora come sopra specificato, e in mancanza dell'elemento soggettivo del dolo non vi sono gli estremi neanche per perseguire la condotta sotto il profilo penale.**

La situazione riveste unicamente questioni di carattere civilistico e di rapporti di vicinato e pertanto, fatta salva l'istituzionale compito della bonaria ricomposizione delle liti tra privati di cui all'art. 1 TULPS, si suggerisce di rimandare i cittadini ai propri legali per la gestione di un eventuale contenzioso unicamente di natura privata.
In materia di possibili contrasti tra vicini si ricorda che in materia di videosorveglianza caso particolare è rappresentato dai **videocitofoni** per i quali il garante ha precisato che questi sistemi sono ammessi per finalità identificative dei visitatori che si accingono ad entrare in luoghi privati. Queste apparecchiature che rilevano immagini e suoni senza registrazioni normalmente sono collocate sugli ingressi degli immobili normalmente in corrispondenza dei campanelli-citofoni per finalità di controllo delle persone che accedono all'edificio.

Tuttavia la loro esistenza deve essere conosciuta e quindi comunicata attraverso un'informativa rilevabile in modo agevole (cartello nei casi in cui non sono utilizzabili per usi esclusivamente personali).

Per quanto riguarda la videosorveglianza invece interna ai condomini la norma di riferimento è **l'art. 7, Legge 11 dicembre 2012, n. 220** - Modifiche alla disciplina del condominio negli edifici, in vigore dal 17 giugno 2013 che ha introdotto nel Codice Civile **l'art. 1122-ter Impianti di videosorveglianza sulle parti comuni** secondo il quale le deliberazioni concernenti l'installazione sulle parti comuni dell'edificio di impianti volti a consentire la videosorveglianza su di esse sono approvate dall'assemblea con la maggioranza di cui al secondo comma dell'articolo 1136.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 321

Tale articolo è dedicato agli impianti di videosorveglianza sulle parti comuni: le deliberazioni concernenti l´installazione sulle parti comuni dell´edificio di impianti volti a consentire la videosorveglianza su di esse sono approvate dall´assemblea con la maggioranza di cui al secondo comma dell´articolo 1136 c.c, quindi sono valide le deliberazioni approvate con un numero di voti che rappresenti la maggioranza degli intervenuti e almeno la metà **del valore dell'edificio**.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 322

Una volta ottenuta la maggioranza richiesta si dovranno comunque seguire gli adempimenti richiesti, mutuati dalle indicazioni del Garante nel Provvedimento generale in materia di videosorveglianza dell'8 aprile 2010:

- Cartello informativo
- Tempi minimi stabiliti di conservazione delle riprese (al massimo 72 ore)
- Individuazione del personale che visiona le immagini tramite la nomina di responsabile ed incaricato(i) del trattamento.
- Verifica preliminare del Garante nei casi previsti dal Codice Privacy (ad es. a sistemi di video sorveglianza dotati di software che permetta il riconoscimento tramite incrocio o confronto delle immagini, con altri specifici dati personali).

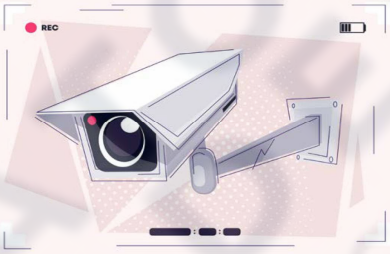
Verbale di sopralluogo e accertamento amministrativo da utilizzare per i controlli in materia e da inoltrare al Garante Privacy a titolo di segnalazione di possibili situazioni di irregolarità.

www.gpdp.it/videosorveglianza

gennaio 2022

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Sistemi di VIDEOSORVEGLIANZA installati da PERSONE FISICHE



Le REGOLE da seguire

Le persone fisiche possono, nell'ambito di attività di carattere personale o domestico, attivare sistemi di videosorveglianza a tutela della sicurezza di persone o beni senza alcuna autorizzazione e formalità, purché:

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 325

- le telecamere siano idonee a riprendere SOLO aree di PROPRIA ESCLUSIVA PERTINENZA;
- vengano attivate MISURE TECNICHE PER OSCURARE PORZIONI DI IMMAGINI in tutti i casi in cui, per tutelare adeguatamente la sicurezza propria o dei propri beni, sia inevitabile riprendere parzialmente anche AREE di TERZI;
- nei casi in cui sulle aree riprese insista una SERVITÙ DI PASSAGGIO in capo a terzi, sia acquisito formalmente (una tantum) il CONSENSO del soggetto titolare di tale diritto;

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 326


KRATOS ACADEMY
UNIVERSITÀ POPOLARE
ESA.ARCO
CONFEDERAZIONE
TÜV SÜD
NON siano oggetto di ripresa AREE CONDOMINIALI COMUNI o di TERZI;
NON siano oggetto di ripresa AREE APERTE AL PUBBLICO (strade pubbliche o aree di pubblico passaggio);
NON siano oggetto di COMUNICAZIONE A TERZI o di DIFFUSIONE le immagini riprese.
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
327


Gli adempimenti privacy di cui al d.l. n. 127/2021 in ambito lavorativo privato
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
328

Il 21 settembre 2021 è stato pubblicato il d.l. n. 127, in vigore dal 22 settembre, con cui, tra le altre cose, si rende obbligatorio il possesso della certificazione verde COVID-19 (c.d. "green pass") per tutti gli ambienti di lavoro, privati e pubblici, dal 15 ottobre 2021 (e fino al 31 dicembre 2021, termine di cessazione dello stato di emergenza).

Ciò significa che i lavoratori che vorranno accedere ai luoghi in cui svolgano la propria attività lavorativa, **dovranno essere in possesso di green pass in corso di validità in quel momento, altrimenti sarà loro impedito l'ingresso.**

Ad essi si aggiungono i collaboratori a partita IVA (qualora accedano al luogo di lavoro), volontari, stagisti e altri soggetti che svolgano la propria attività a qualsiasi titolo (anche in base a contratti esterni) nei locali di un'impresa privata.

Quest'ultima (nonché il datore di lavoro del dipendente che si rechi a lavorare a qualsiasi titolo nei locali di un'azienda altrui) dovrà quindi verificare tale circostanza, negando l'accesso a chi non abbia i requisiti di legge.

Il datore di lavoro non potrà chiedere ai dipendenti se siano vaccinati, o di fornire altre informazioni sul proprio stato vaccinale o copia di documenti che comprovino l'avvenuta vaccinazione anti Covid-19, ma il controllo sarà istantaneo, in presenza e non comporterà la conservazione del certificato.

Tecnicamente, "*la verifica delle certificazioni verdi COVID-19 è effettuata mediante la lettura del codice a barre bidimensionale, utilizzando esclusivamente l'applicazione mobile descritta nell'allegato B (VerificaC19) che consente unicamente di controllare l'autenticità, la validità e l'integrità della certificazione, e di conoscere le generalità dell'intestatario, senza rendere visibili le informazioni che ne hanno determinato l'emissione*" (art. 13, DPCM 17 giugno 2021)

E' chiaro che questa verifica rappresenti un trattamento di dati personali, per cui è opportuno esaminare quali siano le implicazioni, gli obblighi e i principali incombenti privacy, per le aziende che si trovano ad essere Titolari di questa (nuova) attività di trattamento.

Come principio generale, **i Titolari del trattamento che effettuino i controlli debbono osservare strettamente le norme di legge, per rispettare i diritti e le libertà delle persone sottoposte al trattamento.**

Stelle polari sono quindi i precetti di cui agli articoli 5,24,25 e 32 del GDPR.

Per quanto riguarda gli adempimenti concreti, il primo è da effettuare entro il 15 ottobre 2021 (cioè prima ancora dell'inizio del trattamento).
In base all'art. 3 del Decreto Legge n. 127 (che introduce un nuovo art. 9-septies nel DL 22 aprile 2021, n. 52), i datori di lavoro debbono infatti, entro tale data, "*definire le modalità operative per l'organizzazione delle verifiche, anche a campione*": è quindi necessario redigere, prima del prossimo 15 ottobre, un documento che definisca i criteri e le regole dei controlli.
Questo incombente è apparentemente nuovo e ulteriore rispetto a quanto previsto dal GDPR: ma è appunto una novità solo apparente, in quanto tale obbligo è già previsto dagli artt. 24,25 e 32 GDPR, che impongono al Titolare del trattamento di mettere in atto, tra l'altro, misure anche organizzative adeguate, per garantire che il trattamento sia effettuato conformemente al GDPR stesso e un livello di sicurezza adeguato al rischio.

Il secondo adempimento del Titolare, sempre stabilito dal nuovo art. 9-septies, DL 52/2021, è l'individuazione, con un atto formale, dei soggetti incaricati dell'accertamento delle violazioni degli obblighi.
Si tratta, sostanzialmente, di scegliere le persone da incaricare ad effettuare i suddetti controlli e la formalizzazione della loro autorizzazione, in ossequio anche all'art. 29 GDPR e all'art. 13, c. 2, del DPCM citato.
Deve quindi essere redatto un formale atto di autorizzazione al trattamento, contenente le necessarie istruzioni sull'esercizio dell'attività di verifica.
E' comunque consigliabile effettuare anche una formazione specifica degli incaricati/autorizzati.

Un ulteriore obbligo è poi quello di informare l'interessato sul trattamento dei suoi dati personali, che verrà effettuato tramite la verifica del Green Pass (art. 13 GDPR).

Tale informativa dovrà essere esposta nel luogo e nel momento in cui verrà effettuata la verifica, in modo che le persone possano comprendere come verranno trattati i loro dati personali; ma ben potrà essere pubblicata anche sul sito internet dell'azienda, o consegnata al lavoratore controllato (anche via mail), prima del trattamento.

E' però consigliabile informare chiaramente sin d'ora i dipendenti, sia dei futuri controlli (che avverranno dal 15 ottobre in poi), sia delle conseguenze del mancato possesso del green pass.

Da ultimo, è senz'altro necessario integrare il registro dei trattamenti aziendale, con le informazioni per la suddetta, nuova, attività di trattamento.

Si potrà integrare il registro semplicemente allegando una stampa (se cartaceo), ovvero lo stesso documento PDF (oppure, se si utilizza un software per il registro, inserendo i relativi dati).

Quanto indicato dovrà corrispondere realmente alle caratteristiche e modalità del trattamento effettuato.

Si ricorda, infine, che **l'omissione dei suddetti adempimenti può comportare l'applicazione di sanzioni amministrative, alcune delle quali previste dallo stesso Decreto Legge n. 127, mentre le altre dall'art. 83 GDPR.**

Ma cosa accade se il datore di lavoro omette di adempiere a tali incombenti?
Quali rischi corre?

Il d.l. in oggetto prevede sanzioni amministrative specifiche per alcuni di tali inadempimenti, mentre, per gli altri, "soccorre" il GDPR.

Anzi, a ben vedere, il Regolamento Europeo 679/2016 prevederebbe già sanzioni per il datore di lavoro (che è Titolare di questo trattamento) anche per le omissioni ora specificamente punite dal d.l. n. 127/2021.

Quali sono quindi tali sanzioni? Come e quando si applicano?

Il primo adempimento richiesto dal nuovo art. 9-*septies*, d.l. 22 aprile 2021, n. 52 (introdotto appunto dal d.l. n. 127) è la definizione, entro il 15 ottobre 2021, delle modalità operative per l'organizzazione delle verifiche, anche a campione: si tratta, sostanzialmente, della redazione di una policy procedurale e organizzativa per i controlli, da realizzare prima ancora dell'inizio del trattamento.

La sua omissione è punita dal c. 9 di detto nuovo articolo (che rimanda a sua volta all'art. 4, comma 1, d.l. 25 marzo 2020 n. 19), con la sanzione amministrativa da € 400,00 ad € 1.000,00.

Come anticipato, tale incombente sarebbe comunque già imposto dagli artt. 25 e 32 (oltre che 24) GDPR, che prevedono l'obbligo del Titolare di mettere in atto misure anche organizzative adeguate, per garantire che il trattamento sia effettuato conformemente al GDPR stesso e un livello di sicurezza adeguato al rischio.

La violazione di tale obbligo è punita dal successivo art. 83, par. 4, con la sanzione amministrativa pecuniaria fino a € 10.000.000,00, o, per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

L'art. 9 della l. n. 689/81 prevede però il principio di specialità, secondo cui "quando uno stesso fatto è punito… da una pluralità di disposizioni che prevedono sanzioni amministrative, si applica la disposizione speciale".

E poiché la norma di cui al nuovo art. 9-*septies* del d.l. 22 aprile 2021, n. 52 (introdotto dal citato art. 3, d.l. 127/2021), è speciale rispetto a quella generale del GDPR, dovrà applicarsi la sanzione prevista dalla stessa norma speciale, decisamente meno gravosa per il trasgressore.

Il secondo adempimento del Titolare, sempre stabilito dal nuovo art. 9-*septies*, d.l. n. 52/2021, è l'individuazione (con un atto formale, contenente le necessarie istruzioni sull'esercizio dell'attività di verifica) dei soggetti incaricati dell'accertamento delle violazioni degli obblighi.

Poiché è legittimo ritenere pure tale adempimento una "misura organizzativa di cui al comma 5" (unitamente alla redazione della suddetta policy), la sua omissione deve considerarsi punita con la sanzione amministrativa da € 400,00 ad € 1.000,00, sempre ai sensi del c. 9.

Anche in questo caso si tratterebbe comunque della violazione di un obbligo GDPR (stabilito dall'art. 29), punito con la sanzione di cui al già visto art. 83, par. 4: ma per il principio di specialità, varranno le medesime conclusioni.

Ulteriore obbligo privacy è quello di informare il lavoratore interessato sul trattamento dei suoi dati personali, che verrà effettuato tramite la verifica del Green Pass (art. 13 GDPR).

L'omessa (o inadeguata) informativa è sanzionata "soltanto" dall'art. 83 GDPR. Ma non dal par. 4, bensì dal par. 5, che prevede pene doppie (sanzione amministrativa pecuniaria fino a € 20.000.000,00, o, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).

L'ultimo adempimento richiesto dalla normativa sulla protezione dei dati personali è l'integrazione del registro dei trattamenti aziendale, con le informazioni relative alla suddetta, nuova, attività di trattamento.

La sua mancanza potrebbe sottoporre il Titolare alla sanzione amministrativa prevista dall'art. 83, par. 4, GDPR.

È quindi necessario tenere ben presente che l'omissione delle misure privacy dovute per adempiere ai nuovi obblighi di controllo introdotti dal d.l. n. 127/2021 comporterebbe il rischio, per il datore di lavoro, di subire non soltanto le sanzioni previste dal c. 9, art. 9-*septies*, d.l. n. 52/2021, ma anche quelle già vigenti in base al GDPR.

VIOLAZIONE	SANZIONE DL 127/2021	SANZIONE GDPR	QUALE SI APPLICA
Omessa redazione di policy procedurale e organizzativa per i controlli, entro il 15 ottobre 2015	Sanzione amministrativa da € 400,00 ad € 1.000,00 (art. 9-septies, c. 9, D.L. 22 aprile 2021, n. 52)	Sanzione amministrativa pecuniaria fino a € 10.000.000,00, o fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4, GDPR)	Sanzione amministrativa da € 400,00 ad € 1.000,00
Omessa redazione di atto formale di incarico/autorizzazione dei soggetti incaricati dell'accertamento delle violazioni degli obblighi, contenente le necessarie istruzioni sull'esercizio dell'attività di verifica	Sanzione amministrativa da € 400,00 ad € 1.000,00 (art. 9-septies, c. 9, D.L. 22 aprile 2021, n. 52)	Sanzione amministrativa pecuniaria fino a € 10.000.000,00, o fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4, GDPR)	Sanzione amministrativa da € 400,00 ad € 1.000,00

VIOLAZIONE	SANZIONE DL 127/2021	SANZIONE GDPR	QUALE SI APPLICA
Omessa o inadeguata informativa al lavoratore interessato sul trattamento dei suoi dati personali, che verrà effettuato tramite la verifica del Green Pass		Sanzione amministrativa pecuniaria fino a € 20.000.000,00, o fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, GDPR)	Sanzione amministrativa pecuniaria fino a € 20.000.000,00, o fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore
Omessa integrazione del registro dei trattamenti aziendale, con le informazioni relative alla nuova attività di trattamento		Sanzione amministrativa pecuniaria fino a € 10.000.000,00, o fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4, GDPR)	Sanzione amministrativa pecuniaria fino a € 10.000.000,00, o fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 343

Anche se è frequente vedere telecamere private rivolte verso le strade solo i Comuni e le forze di polizia possono, infatti, legittimamente posizionare sistemi di videosorveglianza negli spazi aperti al pubblico, ma anche in questo caso andranno sempre osservati tutti i principi previsti dal regolamento europeo in materia di corretto trattamento dei dati personali. E segnalare adeguatamente gli impianti mettendo a disposizione degli interessati informative di primo e secondo livello. Lo ha *evidenziato il Garante per la protezione dei dati personali con l'ordinanza ingiunzione n. 20 del 27 gennaio 2022.*

Un circolo privato ha posizionato dispositivi di ripresa sia all'interno che all'esterno della struttura **senza installare alcun cartello informativo**.

La Polizia Locale ha segnalato all'Autorità una serie di irregolarità commesse dal circolo **tra cui l'errato puntamento delle telecamere verso le strade ed in particolare il posizionamento di un dispositivo di ripresa verso la caserma dei Carabinieri, prossima alla sede del circolo.**

Il Garante ha quindi adottato un **provvedimento sanzionatorio per l'errato angolo di visuale delle telecamere e per la mancanza di una idonea informativa.** La necessità di utilizzare la videosorveglianza a protezione degli interessi legittimi di un soggetto privato, specifica l'interessante provvedimento, **«si arresta ai confini delle aree di propria pertinenza. Anche nei casi in cui si renda necessario estendere la videosorveglianza alle immediate vicinanze dell'area di pertinenza, il titolare del trattamento deve comunque mettere in atto misure idonee a evitare che il sistema di videosorveglianza raccolga dati anche oltre le aree di pertinenza, eventualmente oscurando tali aree».**

Nel caso sottoposto all'esame del collegio, prosegue l'Autorità centrale, «risulta accertato che il circolo ha effettuato un trattamento di dati personali, per mezzo di un impianto di videosorveglianza **in violazione dei principi generali in materia di protezione dei dati personali di cui all'art. 5, par. 1, lett. a) e c) e in assenza di idonea informativa in spregio a quanto stabilito dall'art. 13 del Regolamento.**

Spetta al titolare del trattamento, **nel caso di specie da individuarsi nel circolo,** valutare la liceità dello stesso posto in essere mediante le videocamere e informare gli interessati della presenza delle stesse, mediante l'apposizione di idonei cartelli recanti l'informativa, da cui risulti l'indicazione del titolare e delle finalità del trattamento. Il trattamento deve inoltre 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 per la tutela dell'interesse legittimo del titolare del trattamento (spazi pubblici, altri esercizi commerciali o edifici pubblici estranei rispetto alle attività del titolare, ecc.)».**

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 349

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 350

La Corte di Cassazione con la Sentenza nr. 8911/2021 prende in esame il caso di un pubblico ufficiale a cui viene attribuita una responsabilità penale per avere effettuato un accesso al sistema informativo, a cui era autorizzato ad accedere, ma per ricavare informazioni estranee ai compiti d'ufficio.

I Magistrati della Suprema Corte, rigettando il ricorso dell'interessato **affermano che integra il reato di "accesso abusivo a un sistema informatico" (art. 615-ter codice penale) la condotta di colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema.**

Lo stesso reato è integrato laddove la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso, **acceda o si mantenga nel sistema per ragioni ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso gli è attribuita.**

Inoltre, aggiungono i magistrati, **è penalmente rilevante anche la condotta del soggetto che, pur essendo abilitato ad accedere al sistema informatico o telematico, vi si introduca con la password di servizio per raccogliere dati protetti per finalità estranee alle ragioni di istituto ed agli scopi sottostanti alla protezione dell'archivio informatico, utilizzando sostanzialmente il sistema per finalità diverse da quelle consentite.**

Viene precisato inoltre che **la fattispecie in esame punisce non soltanto l'abusiva introduzione nel sistema (da escludersi nel caso di possesso del titolo di legittimazione), ma anche l'abusiva permanenza in esso contro la volontà del titolare dello ius excludendi** e che, nel caso in cui il titolo di legittimazione all'accesso venga utilizzato dall'agente per finalità diverse da quelle consentite, deve ritenersi che la permanenza nel sistema informatico avvenga contro la volontà del titolare del diritto di esclusione, in tal modo venendosi a precisare quanto già evincibile da Sezioni Unite Casani in riferimento alla (ir)rilevanza della violazione di specifiche disposizioni che disciplinano l'accesso al sistema.

Si prefigura il reato contestato anche se l'informazione fornita sia quella della non rinvenibilità di iscrizione a carico del richiedente, in relazione ad uno specifico procedimento, secondo quanto emerge dalla visione degli atti e delle annotazioni accessibili all'ufficio di cui fa parte il funzionario propalante, in quanto ciò che assume rilievo è la rivelazione di quanto è desumibile dai registri consultabili, mentre «Non appare neutra la notizia che non risultano iscrizioni, perché a norma di legge – art. 110-bis disp. att. cod. proc. pen. – l'addetto può rispondere alla richiesta dell'interessato, avanzata secondo le procedure prescritte dalla legge, soltanto con la formula "Non risultano iscrizioni suscettibili di comunicazione", formula quest'ultima che lascia impregiudicato il potere del pubblico ministero di secretazione».

Deve essere, inoltre, affermato il principio per cui **la rivelazione di notizie acquisite dalle banche dati SDI e comunicate, in assenza delle prescritte formalità, integra il reato di cui all'art. 326 cod. pen.(rilevazione del segreto d'ufficio) anche quando consistano nella propalazione dell'assenza di annotazioni.**

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 357


KRATOS ACADEMY
UNIVERSITÀ POPOLARE
ESAARCO
CONFEDERAZIONE
TÜV SÜD
VIDEO & AUDIO
AXON
POLIZIA LOCALE
PADOVAOGGI
Dr. Domenico Giannetta
Esperto Diritto Amministrativo
SAFETY & SECURITY
359


KRATOS ACADEMY
UNIVERSITÀ POPOLARE
ESAARCO
CONFEDERAZIONE
TÜV SÜD
Dash cam
Uno strumento che grazie alle funzioni del software e ad appositi sensori è in grado di registrare immagini di alta qualità in movimento, anche ad alta velocità. I modelli più evoluti si possono integrare al sistema GPS e ottenere le coordinate del veicolo.
Dr. Domenico Giannetta
Esperto Diritto Amministrativo
SAFETY & SECURITY
360

La Dash Cam è un dispositivo di ripresa video che può essere installato in auto per registrare cosa accade dentro e fuori la vettura

La Dash Cam è quella che possiamo altrimenti chiamare "telecamera da cruscotto", **dispositivo elettronico che serve per l'acquisizione di immagini** e che si può applicare sul parabrezza per registrare gli eventi che accadono all'esterno dell'auto o per riprendere la cabina interna. Si tratta di un accessorio molto diffuso negli ultimi anni, che videoregistra interno e esterno del veicolo, **tutelando l'automobilista in caso di tentativi di truffa e/o sinistri.**

È una telecamera che, una volta installata, **non deve essere azionata manualmente** ma continua la sua registrazione. Si tratta di una tecnologia legale, i file possono essere mostrati alle autorità.

Si tratta di una fotocamera digitale piccola, a doppia lente e un angolo visuale ampio. Riesce a effettuare riprese di **alta qualità,** fino a 30 fotogrammi al secondo, anche in situazioni di scarsa luminosità. È facile installarla in auto e permette di registrare quello che succede dentro e fuori dall'abitacolo, sia mentre si è in viaggio, che durante la sosta in un parcheggio. Registra immagini di alta qualità in movimento, anche ad alta velocità.
In genere la Dash Cam si fissa con la **ventosa sul parabrezza** e si ricarica con la presa accendisigari. **La scheda memoria interna può avere capienza differente a seconda del modello, il requisito minimo è di 64 GB.** Chi usa una Dash Cam deve effettuare un download periodico dei video, salvando quelli eventualmente utili. Alcune telecamere sovrascrivono in automatico i nuovi filmati sui file più vecchi, non interrompendo mai la ripresa.

Si tratta di un dispositivo utile in caso di **sinistro stradale, tentativi di truffa e contenziosi,** grazie al video che mostra quanto accaduto con immagini non alterate; si tratta di un rilevamento in tempo reale, una sorta di testimonianza diretta, che può essere mostrata sia alle Forze di Polizia che alla compagnia assicuratrice, per ricostruire la dinamica dei fatti.
La presenza della Dash Cam può essere molto **utile anche in caso di atti di vandalismo, quando il veicolo è in sosta, oppure per casi di collisione e tamponamento.** Si tratta di un dispositivo che può registrare anche ciò che accade all'interno dell'abitacolo, utile soprattutto per i tassisti notturni. C'è da considerare anche la variante "piacevole" della Dash Cam, che può registrare viaggi con amici e familiari.

I filmati registrati dalla Dash Cam hanno **efficacia di prova** solo se non contestati da parte avversa. Secondo una sentenza della Corte di Cassazione "l'eventuale disconoscimento della parte avversa deve essere **chiaro, circostanziato ed esplicito**, dovendo concretizzarsi nell'allegazione di elementi attestanti la non corrispondenza tra realtà fattuale e realtà riprodotta" (Cassazione Civile, Sez. Lav., 21/09/2016, n. 18507). Questo significa che **i video si possono utilizzare come prova se non sono contestati dalle parti.** In ogni caso **la contestazione non può essere meramente generica, ma basarsi su fatti convincenti. In ogni caso, se necessario, il Giudice deve valutare se il video può essere usato per risolvere il contenzioso.**

Il Garante per la **tutela dei dati personali** ha emanato il Provvedimento sulla videosorveglianza per stabilire quando è necessario avere il consenso per la rivelazione delle immagini e la diffusione di dati privati a enti pubblici. La Dash Cam può essere usata solo da una persona fisica per attività personali.

Il **Bodycam** è un dispositivo di registrazione audio, video o fotografico indossabile.
Ha una gamma di usi e design, di cui l'uso più noto è come parte dell'attrezzatura di polizia.
Altri usi includono uso sportivo per scopi sociali e ricreativi, nel commercio, nell'assistenza sanitaria, nell'uso militare, nel giornalismo, nella sorveglianza dei cittadini e nella sorveglianza segreta.

Le body cam sono una delle forme di videosorveglianza espressamente prevista dalla vigente normativa sulla privacy e quindi, al di fuori dei casi di esclusione come nel caso di reparti specializzati che svolgano esclusivamente attività di controllo dell'ordine e della sicurezza pubblica, sono illegali se adottate senza svolgere preventivamente all'acquisto e adozione valutazione d'impatto – DPIA (Data Privacy Impact Assessment) che dimostri la sussistenza dei requisiti di legge e in particolare del principio di proporzionalità e ottenga l'approvazione del Garante.

Per i corpi di Polizia Locale che abbiano superficialmente adottato questi strumenti si espongono al rischio di sequestro e di sanzioni sino a 10 milioni di euro, importi in grado di determinare il dissesto finanziario per qualsiasi ente.

Dr. Domenico Giannetta Esperto Diritto Amministrativo 369

Molti credendo immotivatamente che le body cam siano escluse dalla disciplina della videosorveglianza, che è un'attività espressamente e minuziosamente disciplinata dalle norme [art. 35 GDPR], senza eseguire preventivamente la valutazione d'impatto sulla protezione dei dati - DPIA, senza dimostrare l'attuazione del principio di proporzionalità tra l'adozione di uno strumento così invasivo e le reali esigenze della polizia, espone l'amministrazione pubblica che ha adottato illegittimamente le body cam al sequestro degli strumenti e alla sanzione sino a dieci milioni di euro [art. 35 comma 1 e art. 83 comma 4 GDPR], una somma che, anche se applicata in misura ridotta, determina conseguenze devastanti per l'ente, per la parte politica e per i dirigenti.

Dr. Domenico Giannetta Esperto Diritto Amministrativo 370

Regolamento (UE) n. 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).

Reg. UE/2016/679 GDPR, art. 83 (Condizioni generali per infliggere sanzioni amministrative pecuniarie) comma 4 "*In conformità del paragrafo 2 la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR o per le imprese fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente se superiore:*
a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8 11 da 25 a 39 42 e 43…omissis…".

Dr. Domenico Giannetta Esperto Diritto Amministrativo SAFETY & SECURITY 371

Le body cam sono oggettivamente strumenti di registrazione audiovisiva e quindi, sul piano funzionale e strutturale, in nulla si distinguono da tutti gli altri sistemi usati per la videosorveglianza ossia la sorveglianza sistematica su larga scala di una zona accessibile al pubblico che è uno dei casi espressamente sottoposto agli obblighi di valutazione d'impatto sul trattamento dei dati personali - DPIA [art. 35 comma 3 del GDPR].

Reg. UE/2016/679 GDPR, art.35 comma 3 "*La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*"

Dr. Domenico Giannetta Esperto Diritto Amministrativo SAFETY & SECURITY 372

Inoltre, come se non bastasse, **è una delle nuove tecnologie che sin dalla valutazione dell'implementazione deve essere attentamente valutato per i rischi sui diritti e le libertà delle persone fisiche [art. 35 comma 1 del GDPR].**

Reg. UE/2016/679 GDPR, art. 35 comma 1 "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, …*".

L'obbligo della Valutazione d'impatto - DPIA nei casi di videosorveglianza, comunque siano eseguiti, è stato ribadito anche dal Garante per la Protezione dei Dati Personali che con la delibera 11 ottobre 2018, n. 467 "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati, ai sensi dell'articolo 35, comma 4, del regolamento (UE) n. 2016/679*", che ha attuato le indicazioni del WP29 del 2017 fatte proprie dal Comitato europeo per la protezione dei dati (*European Data Protection Board – EDPB*) **nelle Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del 29 gennaio 2020.**

La valutazione d'impatto sulla protezione dei dati è una procedura, nota anche con l'acronimo DPIA (*Data Protection Impact Assessment*) o PIA (*Privacy Impact Assessment*), come si indicherà nel seguito, è prevista dall'articolo 35 del Regolamento UE/2016/679 (GDPR) e ha lo scopo di descrivere un trattamento di dati per valutarne la necessità e la proporzionalità così come tutti gli altri principi fondamentali del GDPR.
Il processo di DPIA può riguardare un singolo trattamento anche più trattamenti che presentino analogie per natura, ambito, finalità e rischi.

Reg. UE/2016/679 GDPR, art.35 (Valutazione d'impatto sulla protezione dei dati) c.1 "*…Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi…*".

Dalla descrizione del trattamento ne consegue la valutazione e quindi la predisposizione di idonee misure per affrontarlo.

La DPIA è uno strumento importante in termini di responsabilizzazione (*accountability*) in quanto aiuta il titolare a rispettare le prescrizioni normative ma attesta anche di aver adottato idonee misure per garantirne il rispetto.

A quali condizioni solo legali le body cam

Preliminarmente all'acquisto delle body cam, anzi ancor prima che l'amministrazione bandisca le **procedure di gara** anche sotto mentite spoglie, come spesso vengono **artatamente definite le c.d. "sperimentazioni" sussiste l'obbligo di eseguire la Valutazione d'impatto-DPIA, in ossequio al principio della *privacy by design* (art. 25 comma 5 GDPR).**

Reg. UE/2016/679 GDPR, art.25 (Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita) comma 1 "*Tenendo conto dello stato dell'arte e dei costi di attuazione nonché della natura dell'ambito di applicazione del contesto e delle finalità del trattamento come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate…omissis…".*

La valutazione deve essere preventiva e solo a margine di un favorevole processo di analisi che **escluda qualsiasi rischio per le libertà fondamentali dei cittadini e l'utilizzo improprio degli impianti di videosorveglianza** si può procedere con la decisione di procedere all'acquisto, all'installazione e all'impiego di qualsiasi sistema di videosorveglianza.

Nella valutazione d'impatto sul trattamento dei dati - DPIA si deve attentamente considerare innanzitutto il rispetto dei principi fondamentali del trattamento dei dati personali e in particolare [art. 5 GDPR]:

- **Principio di trasparenza**, quindi tutti devono sapere, tra le altre cose, in che modo e per quanto tempo, con quali sistemi di sicurezza le immagini video saranno detenute dall'amministrazione e l'informativa deve essere completa, disponibile e ben visibile almeno sul sito dell'ente [art. 5 comma 1 del GDPR];

Reg. UE/2016/679 GDPR, art. 5 (Principi applicabili al trattamento di dati personali) c.1 a "*I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»)*".

- Limitazione delle finalità, quindi si deve esplicitare perché, a che scopo sono registrate le immagini della body cam e per quale motivo si è scelto quel metodo invasivo, indicando tassativamente le finalità e le necessità, ad esempio per scopo di ordine pubblico [art. 5 comma 1 del GDPR];

Reg. UE/2016/679 GDPR, art.5 (Principi applicabili al trattamento di dati personali) c.1 b *"I dati personali sono: … omissis… b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);"*.

- **Minimizzazione dei dati**, si deve accertare che la ripresa sia minima e limitata alle immagini e quindi alle informazioni che effettivamente servono [art. 5 comma 1 del GDPR];

Reg. UE/2016/679 GDPR, art.5 (Principi applicabili al trattamento di dati personali) c.1 c "*I dati personali sono: … omissis… c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);*".

- **Limitazione della conservazione**, che le immagini registrate siano mantenute per il tempo strettamente necessario alle finalità e che questo tempo sia adeguatamente [art. 5 comma 1 del GDPR];

Reg. UE/2016/679 GDPR, art.5 (Principi applicabili al trattamento di dati personali) c.1 c "*I dati personali sono: … omissis… e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»)*"

- **Sicurezza e riservatezza**, che le riprese audiovisive siano conservate garantendo la massima sicurezza mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali [art. 5 comma 1 del GDPR].

Reg. UE/2016/679 GDPR, art. 5 (Principi applicabili al trattamento di dati personali) c.1 c "*I dati personali sono: … omissis… f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).*".

Dr. Domenico Giannetta Esperto Diritto Amministrativo 383

La valutazione d'impatto-DPIA, dato il rischio che comunque sussiste devono essere inviate al garante che giudicherà, tra le altre cose, la sussistenza e la dimostrazione dei principi di:

- **Liceità**, accertando che le riprese siano necessarie per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, quindi si dovrà dimostrare, ad esempio, perché un pubblico ufficiale, la cui parola fa pubblica fede, abbia bisogno di documentare la propria attività con un mezzo così invasivo [art. 6 comma 1 del GDPR];

Reg. UE/2016/679 GDPR, art.6 (Liceità del trattamento) "1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;".

Dr. Domenico Giannetta Esperto Diritto Amministrativo 384

- **proporzionalità**, questo principio è stato ribadito dalle nuove Linee Guida del Garante europeo della protezione dei dati (GEPD), essendo già previsto dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea e dall'art. 16 del Trattato sul funzionamento dell'Unione europea (TFUE), quindi si deve dimostrare che l'adozione delle body cam sia una scelta proporzionale alle necessità, tenendo conto non solo degli obiettivi della misura stessa, ma anche della necessità di proteggere i diritti e le libertà in generale e che quella finalità, a sua volta, non sia raggiungibile con altri mezzi, ragionevolmente applicabili nel contesto di riferimento.

L'analisi contenuta nella valutazione d'impatto - DPIA deve essere attenta e approfondita, poiché non si deve credere che gli enti pubblici siano, in qualche modo, legibus solutibus e, quindi, data la finalità istituzionale dell'azione degli organismi pubblici, il fine giustifichi i mezzi e anche le azioni.

Legibus solutus è una locuzione latina, traducibile con la frase: "sciolto dalle leggi", attribuita al giurista romano Ulpiano. Si dice specialmente di soggetti che in regimi di tipo imperiale o monarchico non erano tenuti al vincolo di rispettare le leggi esistenti.

Ci si deve ricordare infatti che il Regolamento UE 2016/679 sulla privacy ha completamente sostituito il precedente quadro normativo sul trattamento dei dati personali e, come Regolamento europeo, **non solo non ha bisogno di alcuna conversione in legge da parte degli Stati membri** ma è addirittura sovraordinato rispetto le norme nazionali le quali non possono né variarlo né derogarlo.

Dr. Domenico Giannetta Esperto Diritto Amministrativo 387

La disciplina europea della privacy **non fa alcuna differenza negli obblighi e nelle sanzioni tra aziende private ed enti pubblici,** se non nel fatto che le prime sono sanzionate in maniera proporzionale al fatturato, e non consente alcuna deroga o giustificazione derivante da esigenze di bilancio o urgenze.

Dr. Domenico Giannetta Esperto Diritto Amministrativo 388

Quindi l'omissione delle valutazioni preliminari e delle procedure di gestione del trattamento dei dati in generale per le riprese effettuate con le body cam determina, a carico degli enti pubblici così come dei soggetti privati, tra le altre cose, una sanzione sino a dieci milioni di euro (art. 35 comma 1 e art. 83 comma 4 GDPR), una somma che, anche se applicata in misura ridotta, determina conseguenze devastanti.

Quando le body cam sono lecite in via generale

Quanto detto sinora non si applica in tutti i casi in cui non si applica la normativa sulla privacy di cui al GDPR, in questi casi quindi l'adozione delle body cam è legittimo a prescindere:

- Attività di polizia giudiziaria [art. 2 comma 5 GDPR], che tuttavia non può essere preventiva ma solo repressiva e conseguente alla notizia di reato, quindi non è legittima la giustificazione che le body cam siano utilizzate per documentare eventuali reati;

Reg. UE/2016/679 GDPR, art.2 (Ambito di applicazione materiale) c.2 "*Il presente regolamento non si applica ai trattamenti di dati personali: …omissis… d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.*".

❖Attività di controllo dell'ordine della sicurezza pubblica [art. 2 comma 5 GDPR], in questi casi l'attività può essere anche preventiva ma deve essere limitata al contesto territoriale e al momento in cui sussistano rischi, ad esempio nel caso di tumulti in occasione di manifestazioni sportive, politiche, sindacali.

Dette finalità devono essere predefinite sin dall'inizio e conformi alle norme, non si possono quindi considerare come eventuali.

Le Body Cam nell'ambito delle forze di polizia

Con l'espressione **Body Cam** si fa riferimento ad una telecamera indossata dalle forze dell'ordine durante operazioni di tutela dell'ordine pubblico. Telecamere che potrebbero essere eccessivamente invasive. Questo è motivo per cui il Ministero degli Interni ha sviluppato un apposito progetto, che è stato sottoposto all'esame **al Garante della Privacy**.

L'Autorità ha avanzato una serie di osservazioni.

Esaminiamo innanzitutto **l'architettura informatica** a cui queste telecamere si appoggiano e gli elementi afferenti alla **protezione dei dati**, che il parere dell'Autorità Garante ha messo in evidenza.

Occorre analizzare il funzionamento del sistema di telecamere.

Body Cam delle forze dell'ordine: come funzionano

La soluzione tecnologica è basata sui seguenti elementi:

- le **video telecamere indossabili**,
- un **server centrale**, ubicato presso il centro informatico della polizia di Stato,
- i **totem multimediali** dislocati presso i reparti mobili e che contengono:
  - ✓ un personal computer,
  - ✓ software di gestione,
  - ✓ punti di ricarica delle telecamere e di scarico dei dati, con possibilità di archiviazione locale delle registrazioni,
- **postazioni di lavoro** presso i gabinetti di polizia scientifica.

La valutazione d'impatto sulla protezione dei dati

Un aspetto importante è legato al fatto che, data la criticità dell'applicazione, è indispensabile sviluppare la **valutazione di impatto (Data Protection Impact Assessment)** prevista dall'articolo 35 del **Regolamento Generale Europeo sulla protezione dei Dati**.

Ricordiamo che:

- lo sviluppo di un documento conforme all'articolo 25 del Regolamento Europeo è **obbligatorio** per qualsiasi tipo di trattamento;
- lo sviluppo della valutazione di impatto è **necessario** solo per trattamenti che possono, anche potenzialmente, avere riflessi significativi sulla protezione e gestione dei dati.

Le Body Cam e il parere Garante della Privacy

L'Autorità Garante ha dedicato ampio spazio alle modalità con cui vengono scaricate le registrazioni, a bordo delle telecamere; registrazioni che successivamente possono essere messe a disposizione della polizia scientifica per gli appropriati approfondimenti. (**Newsletter n. 481 – Garante Privacy**)

La conservazione dei dati

A questo punto si pone immediatamente in evidenza il tema legato alla **durata di archiviazione dei dati** e viene individuato **un termine di sei mesi di conservazione dei dati**; ciò salvo un'adeguata proroga dei termini, quando i dati personali sono inseriti in un procedimento per l'applicazione di una misura di prevenzione o in un procedimento penale in genere.

2.7. Durata della conservazione dei dati.
In relazione alle specifiche finalità perseguite con i trattamenti in esame, tenendo conto della composizione tra le esigenze di polizia e quelle contrapposte di tutela dei dati personali, **la DPIA individua in sei mesi il termine di conservazione dei dati personali acquisiti.** Detto termine si applica ai dati memorizzati nei NAS dei Reparti mobili e al suo spirare le registrazioni sono irreversibilmente cancellate con modalità automatica.

Un fenomeno, che l'esperienza ha messo in evidenza, è la **accidentale attivazione della telecamera:**

- ❖ in mancanza dei requisiti di necessità di registrazione

oppure

- ❖ in previsione di eventi critici, che poi non si sono verificati.

Soggetti designati come amministratori di sistemi, a fronte di richiesta avanzata dall'ufficiale di pubblica sicurezza responsabile del servizio, cancellano tempestivamente queste registrazioni.

A questo proposito, gli ufficiali responsabili del servizio di ordine pubblico devono essere adeguatamente informati, mediante pubblicazione di apposite linee guida.

La protezione delle registrazioni

Un elemento fondamentale per garantire la protezione delle video registrazioni riguarda **l'adozione di appropriate garanzie in fase di accesso.** Questo può avvenire sia in tempo quasi reale, quando le circostanze sul campo lo richiedano, oppure successivamente, per ricostruire gli eventi video registrati.

Ricordiamo inoltre che **gli operatori sul campo devono interrompere al più presto la registrazione, ove non vi siano più ragioni per mantenere attivata la telecamera.** Questo principio risponde alla più generale prescrizione di minimizzazione dei dati raccolti, in relazione alle esigenze per cui i dati stessi vengono catturati.

Body Cam e utilizzo dei totem

Il Garante si raccomanda di modo particolare di fare **attenzione all'utilizzo dei totem, distaccati sul campo, per garantire che l'accesso a questi dati venga tutelato in maniera garantistica.**

Occorre quindi allestire un **log di sistema, che registri tutti gli accessi e le operazioni effettuate sui dati.**

Copie di filmati e fotografie

L'autorità Garante ha inoltre raccomandato di **prestare massima attenzione all'effettuazione di copie dei filmati e di eventuali fotografie, adottando misure garantistiche; tali copie devono essere inviate solo a soggetti debitamente autorizzati e conservate con le stesse garanzie previste per le copie originali.**

In conclusione, **il Garante ha dato parere favorevole alla valutazione di impatto ed all'architettura generale proposta, precisando comunque tutt'una serie di elementi migliorativi, che il ministero si è impegnato ad adottare al più presto possibile.**

Body cam: ok dal Garante Privacy, ma no al riconoscimento facciale dal Garante per la Privacy

Con due distinti pareri [doc. web 9690691 e n. 9690902] il Garante per la privacy ha dato via libera al Ministero dell'interno - Dipartimento della pubblica sicurezza e al Comando generale dell'Arma dei Carabinieri all'uso delle body cam **per documentare situazioni critiche di ordine pubblico in occasione di eventi o manifestazioni.** Le due Forze di Polizia dovranno comunque recepire alcune indicazioni dell'Autorità relative all'implementazione delle **misure di sicurezza e al tracciamento degli accessi ai dati per rendere i trattamenti pienamente conformi alla normativa sulla protezione dei dati personali trattati a fini di prevenzione e accertamento dei reati (Decreto legislativo n. 51/2018).**

L'Autorità ha chiesto, in particolare, al Ministero di specificare che **il sistema che intende utilizzare non consente l'identificazione univoca o il riconoscimento facciale della persona (facial recognition), come già precisato nella documentazione trasmessa dall'Arma.** I due sistemi, sottoposti al Garante autonomamente, presentano notevoli analogie, non solo per quanto riguarda le finalità perseguite, ma anche dal punto di vista strutturale, ad eccezione delle differenze imputabili alle specifiche strutture organizzative delle due Forze di Polizia. Le videocamere indossabili in uso al personale dei reparti mobili incaricato potranno essere attivate solo in presenza di concrete e reali situazioni di pericolo di turbamento dell'ordine pubblico o di fatti di reato.

Non è ammessa la registrazione continua delle immagini e tantomeno quella di episodi non critici.
I dati raccolti riguardano audio, video e foto delle persone riprese, data, ora della registrazione e coordinate Gps, che una volta scaricati dalle videocamere sono disponibili, con diversi livelli di accessibilità e sicurezza, per le successive attività di accertamento.
I due pareri resi dal Garante sulle due valutazioni di impatto presentate dal Ministero e dall'Arma tengono conto degli approfondimenti effettuati dagli uffici dell'Autorità.

A differenza di quanto sostenuto dal Ministero e dall'Arma, **che pur avendo presentato la DPIA non ritenevano necessaria la consultazione preventiva dell'Autorità, il Garante ha affermato che in base al Decreto tale consultazione è dovuta, in quanto i rischi per le persone riprese possono essere anche molto elevati, spaziando dalla discriminazione alla sostituzione d'identità, al pregiudizio per la reputazione, all'ingiusta privazione di diritti e libertà.**

L'utilizzo delle body cam nel corso di manifestazioni pubbliche rende estremamente probabile il trattamento di dati che rivelino le opinioni politiche, sindacali, religiose o l'orientamento sessuale dei partecipanti.

Il Garante ha ritenuto tra l'altro **ragionevole il periodo di sei mesi di conservazione dei dati e rispettato il principio di privacy by default, essendo prevista la loro cancellazione automatica trascorso tale termine.**

L'Autorità infine ha raccomandato alle Amministrazioni di valutare la possibilità di condividere i documenti originali con tutti i soggetti autorizzati da remoto, senza il ricorso alla produzione di copie.

KRATOS ACADEMY UNIVERSITÀ POPOLARE — ESA.ARCO CONFEDERAZIONE — TÜV SÜD

Per l'utilizzo delle body cam e delle dash cam è necessario

- ✓ Predisporre un progetto evidenziando la necessità concreta per la sicurezza degli agenti bilanciandola con la compressione dei diritti dei soggetti ripresi – Reg UE 679/2016 – GDPR
- ✓ Approvare un disciplinare / regolamento di utilizzo
- ✓ Far validare il progetto e il disciplinare / regolamento dal DPO
- ✓ Formulare un accordo con le RSU ai sensi dell'art. 4 dello Statuto dei Lavoratori
- ✓ Effettuare la formazione degli agenti (aspetti di privacy – aspetti operativi – aspetti tecnologici)
- ✓ Predisporre dei protocolli operativi con body cam
- ✓ Curare gli aspetti di cybersecurity
- ✓ Formulare e condividere le regole di accesso / visione / estrazione

Dr. Domenico Giannetta — Esperto Sicurezza Urbana Integrata — SAFETY & SECURITY — 410

Progettazione e previsione di utilizzo

Chi li utilizzerà

- Personale esterno / interno
- Personale specializzato
- Particolari servizi / contesti

Dr. Domenico Giannetta — Esperto Sicurezza Urbana Integrata — 411

Con quali regole ?

- ✓ Rispetto del Reg UE 679/2016 – GDPR – D.Lgs. 196/2003
- ✓ Disciplinare / Regolamento di utilizzo (si attivano solo in casi specifici)
- ✓ Formazione del personale ai sensi dell'art. 37 del d.lgs. n. 81/2008
- ✓ Nessun agente o ufficiale potrà accedere ai files ma solo il responsabile appositamente individuato potrà accedere per estrarre le fonti di prova per la competente Autorità Giudiziaria e le operazioni saranno tracciate e non modificabili
- ✓ Uso per motivi di Polizia Giudiziaria
- ✓ Divieto di utilizzo per sanzionare
- ✓ Uso in operazioni di privazione della libertà previste dalla legge
- ✓ L'attivazione sarà comunicata a voce e sarà visibile il led di registrazione
- ✓ Dati protetti e conservati per sette giorni a disposizione dell'Autorità Giudiziaria

Dr. Domenico Giannetta — Esperto Sicurezza Urbana Integrata — 412

Quali sono gli obiettivi ?

- Ridurre l'aggressività
- Deflazionare i comportamenti violenti
- Garantire gli agenti e i cittadini

Dr. Domenico Giannetta — Esperto Sicurezza Urbana Integrata — 413

Esempi di disciplinare / regolamento

1. L'attivazione delle registrazioni avviene esclusivamente nelle circostanze operative specificate nei punti successivi, senza ulteriori margini di discrezionalità.

2. La videocamera operativa a bordo uomo/Body Cam è attivata su ordine del capo pattuglia/assegnatario qualora emergano elementi e/o indicatori circa "l'insorgere di una criticità per la sicurezza operativa degli operanti e/o per la sicurezza delle persone presenti nella scena dell'intervento":

Dr. Domenico Giannetta — Esperto Sicurezza Urbana Integrata — 414

2.1 - In luoghi pubblici o aperti al pubblico sul presupposto di cui al punto 2), al compimento delle "attività di controllo di polizia amministrativa/pubblica sicurezza/sicurezza urbana" (es. controllo e contestazione di violazioni amministrative al codice stradale, ispezioni di attività commerciali su suolo pubblico, accessi in esercizi pubblici o cantieri edilizi), senza alcuna possibilità di utilizzare il sistema per l'acquisizione e utilizzo delle registrazioni in funzione probatoria dell'accertamento di illeciti amministrativi;

2.2) in luoghi pubblici o aperti al pubblico nonché in luoghi privati, nell'ambito di attività di polizia giudiziaria, in relazione al compimento delle "attività di polizia giudiziaria" e/o di attività di privazione della libertà previsti dalla normativa es. accompagnamento per identificazione (od altre misure es. arresto d'iniziativa in flagranza di reato, resistenza e fuga del sospettato di reato, perquisizioni e sequestri d'iniziativa o delegati, esecuzione di misura cautelare delegata dall'A.G., altre circostanze legittimanti l'uso di mezzi di coazione fisica), per l'utilizzo e acquisizione delle registrazioni quale indizio o fonte di prova dell'eventuale reato tentato o consumato come previsto dal codice di procedura penale (rif. artt. 187, 189, 234, 354 c.p.p.).

3 - La videocamera operativa a bordo veicolo/Dash Cam è sempre attivata nel corso delle operazioni di "pattugliamento di controllo del territorio" per le finalità di sicurezza stradale; la visione di tale camera è quella esterna al parabrezza in relazione alla carreggiata con focus sui veicoli e targhe presenti nella circolazione, a tal fine potranno anche essere installati algoritmi di comparazione delle targhe visualizzate dalla videocamera con la banca dati dei veicoli oggetto di furto e/o sprovvisti di assicurazione obbligatoria, che mediante alert all'equipaggio consentiranno agli operanti di fermare il veicolo e procedere alle misure cautelari di legge sui veicoli in circolazione che costituiscono un potenziale pericolo;

4 - Per le Body Cam, il capo pattuglia dà verbalmente all'interlocutore informativa sintetica dell'avvio della registrazione, mentre una luce led di colore rosso avvisa che il sistema sta registrando. Per le Dash Cam, sulla carrozzeria delle auto ove sono installate è apposta segnaletica recante la scritta "Veicolo dotato di sistema di videosorveglianza" e/o il simbolo grafico della VDS;

5 - Al termine delle circostanze che hanno legittimato l'attivazione, il capo pattuglia assegnatario, dispone la cessazione della registrazione delle Body Cam, salvo eventuale riattivazione nel caso di ulteriori condizioni legittimanti;

C.P.P. - Art. 354. Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro

1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.
2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. **In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.** Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.
3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di PG compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 419

C.P.P. - Art. 189. Prove non disciplinate dalla legge

1. Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 420

C.P.P. - Art. 234. Prova documentale

1. E' consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo.

2. Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia.

3. E' vietata l'acquisizione di documenti che contengono informazioni sulle voci correnti nel pubblico intorno ai fatti di cui si tratta nel processo o sulla moralità in generale delle parti, dei testimoni, dei consulenti tecnici e dei periti.

Cosa si deve intendere per documento informatico?

L'art. 234, comma 1, C.P.P. indica che: «È consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo».

Pertanto:

il documento informatico rientra tra il novero delle prove digitali, in qualsiasi forma si presenti e in relazione a qualsiasi contenuto;

nonché:

i dati di carattere informatico contenuti nel computer, in quanto rappresentativi, alla stregua della previsione normativa, di cose, rientranti tra le prove documentali

(Cass., Sez. III, n.37419, 5/7/2012, CED 253573–01)

La digital forensics (conosciuta anche come scienza digitale forense) è un ramo della scienza forense che comprende il recupero e l'indagine del materiale trovato nei dispositivi digitali, spesso in relazione a eventi di criminalità informatica.

Modalità di acquisizione

- Verbalizzare la richiesta ed acquisizione della fonte di prova video
- Verbalizzare le operazioni «ripetibili» ovvero su di una copia effettuate presso il Comando e verbalizzare la creazione della copia
- Verbalizzare le operazioni di consegna del verbale operazioni compiute del file acquisito e della «copia» su cui sono state effettuate le operazioni di analisi

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 423

Come rendere «non modificabili» i files acquisiti ?
ART. 354 C.P.P.

- ✓ Se si hanno competenze e strumenti informatici adeguati effettuare il CD dei files con impronta digitale e poi creare la copia e lavorare sulla copia
- ✓ Inserire i files acquisiti su CD / DVD non modificabili
- ✓ Acquisire il file su un supporto con verbale indicando nome files percorso, dimensione, ecc.
- ✓ Effettuare una copia su altro supporto ed inserire il primo supporto in busta chiusa e sigillata
- ✓ La non modificabilità si può certificare con adeguati strumenti informatici od adeguate procedure interne che garantiscano la parte sulla non modificabilità del file acquiisto in origine verbalizzando le operazioni

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 424

Quali sono gli errori frequenti degli operatori di Polizia ?

- Utilizzo degli apparati senza base regolamentare
- Utilizzo degli apparati senza tracciamento
- Utilizzo degli apparati fuori dai casi previsti

Dr. Domenico Giannetta — Esperto Sicurezza Urbana Integrata — 425

Quali sono gli errori frequenti degli operatori di Polizia ?

- Utilizzo degli in maniera indiscriminata
- Estrazione dei dati di registrazione nei casi non previsti
- Attivazione degli apparati senza informativa

Dr. Domenico Giannetta — Esperto Sicurezza Urbana Integrata — 426

Quali sono gli errori frequenti degli operatori di Polizia ?

- Utilizzo degli apparati nei locali al chiuso per riprendere colloqui con colleghi
- Utilizzo degli apparati per sanzioni al codice della strada
- Utilizzo degli apparati in modalità non criptata

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 427

Quali sono gli errori frequenti degli operatori di Polizia ?

- Estrazione e condivisione tra colleghi o sul web dei video
- Mancata consegna dell'apparato a fine turno
- Utilizzo dell'apparato non in dotazione al Comando

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 428


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
STOP
MODULISTICA
1. Regolamento
2. Delibera di Consiglio Comunale
3. Data Protection Impact Assessment
4. Parere DPO
5. Accordo RSU
6. Consultazione Preventiva del Garante - Art. 24 d.lgs. 51/2018
7. Autorizzazione
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
429


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
Legittima la registrazione di conversazioni tra colleghi a fini difensivi
SVILUPPO

Lavoro subordinato - Licenziamento per giusta causa - Registrazioni di conversazioni tra il dipendente e i colleghi di lavoro - Utilizzo a fini difensivi - Consenso dei presenti - Necessità - Esclusione - Legittimità della condotta - Sussiste.

L'utilizzo a fini difensivi di registrazioni di colloqui tra il dipendente e i colleghi sul luogo di lavoro non necessita del consenso dei presenti, in ragione dell'imprescindibile necessità di bilanciare le contrapposte istanze della riservatezza da una parte e della tutela giurisdizionale del diritto dall'altra e pertanto di contemperare la norma sul consenso al trattamento dei dati con le formalità previste dal codice di procedura civile per la tutela dei diritti in giudizio. Ne consegue che è legittima, e inidonea ad integrare un illecito disciplinare, la condotta del lavoratore che abbia effettuato tali registrazioni per tutelare la propria posizione all'interno dell'azienda e per precostituirsi un mezzo di prova, rispondendo la stessa, se pertinente alla tesi difensiva e non eccedente le sue finalità, alle necessità conseguenti al legittimo esercizio di un diritto. *Corte di cassazione, sezione lavoro, sentenza 2/11/2021, n. 31204*

Dr. Domenico Giannetta Esperto Diritto Amministrativo 431

Lavoro - Licenziamento - Illegittimità - Reintegrazione del lavoratore - Registrazione di conversazioni effettuate sul posto di lavoro - Insaputa dei colleghi - Nessuna diffusione all'esterno - Esigenze di tutela dei propri diritti.

Non solo è illegittimo ma scatta anche la reintegra del dipendente licenziato, per grave violazione della privacy, per aver registrato, e filmato, delle conversazioni ad insaputa dei colleghi, senza averle mai diffuse all'esterno, ed al solo fine di precostituirsi degli elementi di difesa per salvaguardare la propria posizione in azienda.

Corte di cassazione, sezione lavoro, sentenza 10 maggio 2018, n. 11322

Dr. Domenico Giannetta Esperto Diritto Amministrativo 432

Prova civile - Documentale (prova) - Riproduzioni meccaniche - Valore probatorio - Colloquio tra lavoratore e datore di lavoro - Registrazione ad opera del primo - Natura - Utilizzazione in giudizio - Ammissibilità - Illecito disciplinare - Esclusione - Fondamento.

La registrazione fonografica di un colloquio tra presenti, rientrando nel "genus" delle riproduzioni meccaniche di cui all'art. 2712 cod. civ., ha natura di prova ammissibile nel processo civile, sicché **la sua effettuazione, operata dal lavoratore ed avente ad oggetto un colloquio con il proprio datore di lavoro, non integra illecito disciplinare.** Né tale condotta, comunque scriminata ex art. 51 cod. pen., in quanto esercizio del diritto di difesa, la cui esplicazione non è limitata alla sede processuale, può ritenersi lesiva del rapporto fiduciario tra lavoratore e datore di lavoro, che concerne esclusivamente l'affidamento di quest'ultimo sulle capacità del dipendente di adempimento dell'obbligazione lavorativa.

• *Corte di cassazione, sezione lavoro, sentenza 29/12/2014, n. 27424*

Dr. Domenico Giannetta Esperto Diritto Amministrativo SAFETY & SECURITY 433

Licenziamento disciplinare - Illegittimità - Reintegrazione del dipendente nel posto di lavoro - Conseguenze economiche - Detrazione dell'aliunde perceptum - Ricorso in cassazione - Motivi di ricorso - Travisamento di fatti - Inammissibilità - Accesso diretto al materiale probatorio - Operazione non consentita in sede di legittimità - Documento e prova documentale - Riproduzioni meccaniche - Registrazione fonografica - Valore probatorio - Illecito disciplinare - E' escluso - Esercizio del diritto di difesa - Giusta causa - Giustificato motivo - Insussistenza - Indennità previdenziali ricevute dal lavoratore - Detrazione del danno risarcibile dovuto dal datore - Possibilità - Esclusione - Fondamento.

Il dipendente può registrare le telefonate e le conversazioni effettuate con il proprio superiore se il suo scopo è quello di utilizzare le registrazioni per precostituirsi una prova a discarico per impugnare il licenziamento. Con questa affermazione la Cassazione ha affermato il carattere di prova in sede civile, nonché penale, della registrazione tra persone. L'iniziativa del dipendente non lede il rapporto di fiducia con il datore di lavoro, in quanto egli è tenuto ad adempiere l'obbligazione lavorativa, ma non anche a non condividere i segreti non funzionali alle esigenze produttive o commerciali dell'impresa; e rientra nel raggio d'azione dell'articolo 51 del Cp che scrimina una tale condotta in nome dell'esercizio del diritto di difesa, che ha portata generale e vale anche per le attività svolte prima che la controversia sia stata instaurata.

• *Corte di cassazione, sezione lavoro, sentenza 29 dicembre 2014, n. 27424*

Dr. Domenico Giannetta Esperto Diritto Amministrativo SAFETY & SECURITY 434

KRATOS ACADEMY UNIVERSITÀ POPOLARE — ESAARCO CONFEDERAZIONE — TÜV SÜD

Legittime le foto e i video fatti dai controllori su treni e autobus pubblici ai passeggeri privi di carta d'identità o altro documento di riconoscimento?

A quanto pare, anche i controllori di treni e autobus hanno iniziato ad avvalersi degli smartphone per scattare fotografie. Ma in questo caso **l'oggetto dello scatto è il passeggero senza biglietto privo di documenti di riconoscimento.** E ciò al fine di contrastare il fenomeno sempre più diffuso della dichiarazione di false generalità. In questo modo, tramite il supporto fotografico e l'eventuale ausilio dei social network, è possibile identificare il soggetto in questione anche in un momento successivo e contestare il reato di false dichiarazioni al pubblico ufficiale. Ma è lecito tale comportamento? Un controllore può fotografare il passeggero senza biglietto?

Dr. Domenico Giannetta — Esperto Diritto Amministrativo — SAFETY & SECURITY — 436

Sul punto **non esiste una normativa specifica** ma ci sia consentito esporre i nostri pareri in forma dubitativa, sia da un versante che dall'altro. Esistono infatti **ragionamenti che militano a favore di una soluzione ed altri in favore di quella opposta.** In attesa di maggiori chiarimenti, soprattutto da parte del Garante della privacy, è quindi bene prendere una posizione prudente su un argomento che, sino ad oggi, non è mai stato trattato.

Il controllore non può fotografare i passeggeri senza biglietto

Iniziamo dalla tesi secondo cui **il controllore non sarebbe legittimato a fare la fotografia** al volto dei passeggeri che, senza biglietto, sono anche sprovvisti di documenti di riconoscimento.

Sicuramente, la presenza su treni e autobus del cartello con l'avviso all'utenza del fatto che i controllori possono fotografare i volti dei passeggeri senza documenti non può rendere lecito un comportamento che non lo è.

Non è corretto neanche il richiamo – che su tali cartelli è possibile rinvenire – all'articolo 13 della legge 689/1981. Tale norma, che si applica in generale agli accertamenti delle violazioni amministrative (come appunto l'utilizzo dei mezzi pubblici senza biglietto), consente agli organi addetti al controllo di «procedere a **ispezioni di cose e di luoghi** diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra preparazione tecnica».

La disposizione fa esplicito riferimento alle foto di cose e luoghi e non anche di persone. L'esempio tipico è quello della Polizia che, intervenuta sul luogo di un sinistro stradale, al fine di redigere il verbale e verificare con attenzione le responsabilità dei conducenti, fotografi le auto coinvolte nello sconto e le relative targhe.
Del resto, il concetto di «rilievo» cui si riferisce la norma ha sempre ad oggetto oggetti inanimati e non anche i volti delle persone.
Esiste poi l'articolo 349 del Codice di procedura penale in forza del quale la polizia giudiziaria «procede alla identificazione della persona nei cui confronti vengono svolte le indagini e delle persone in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti». Anche questa norma non può essere applicata al controllore: innanzitutto perché non è un agente di polizia giudiziaria (tanto più se si tratta di dipendente di società privata) e, in secondo luogo, perché le sue indagini non sono rivolte ad accertare la commissione di un reato ma di un semplice illecito amministrativo.

A militare ancora **a favore della tesi dell'illegittimità delle foto scattate dai controllori vi sono le questioni legate al rispetto della normativa sulla privacy.** Innanzitutto, il viaggiatore deve poter sapere chi è il titolare del trattamento dei dati, come e per quanto tempo le immagini vengono conservate, come visionarle e chiederne la cancellazione. Tutti adempimenti che richiedono la trasparenza nei confronti del cittadino e, il più delle volte, il nulla osta del Garante della privacy o quantomeno la comunicazione dell'attività, coinvolgendo l'immagazzinamento dei dati di soggetti privati.
Chi assicura che per la foto non venga usato il cellulare privato del controllore e non quello di servizio? Come verrà trattato il dato personale e con quali misure di sicurezza?

Tutte queste domande – che legittimamente il cittadino può e deve porsi – non possono trovare risposta né nel cartello esposto sul mezzo pubblico né in una normativa apposita che, al momento, non esiste.

Ecco perché, secondo tutte queste interpretazioni, **il controllore non può fotografare il passeggero** senza biglietto, anche se al solo fine di prevenire la commissione di un reato, quello di false attestazioni al pubblico ufficiale o all'incaricato del pubblico servizio.

Il controllore può fare foto ai passeggeri senza documenti

Analizziamo ora l'opposta tesi che, di certo, ha numerosi punti altrettanto – se non maggiormente – convincenti rispetto alla prima interpretazione.

Il controllore può fare foto ai passeggeri senza biglietto che non danno le proprie generalità in quanto non contrario alla normativa sulla privacy.

Questo perché:

- l'art. 6 par. 1 lett. e) del Regolamento Ue sulla Privacy (il GDPR) afferma che **il trattamento dei dati personali è lecito quando «è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento»;**
- **il controllore è un pubblico ufficiale nell'esercizio delle sue funzioni** e, in quanto tale, è dotato di poteri autoritativi e certificativi connessi all'accertamento delle violazioni in materia di trasporti (Cass. sent. n. 45465/2018), tant'è che chi dichiara false generalità commette reato (art. 495 Cod. pen.);

- **l'art. 13 L. n.689/1981 ha una formulazione disgiuntiva** (lo prova la virgola posta dopo «ispezioni di cose e luoghi diversi dalla privata dimora» che separa tale frase dalla successiva precisazione «a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica»);
- sotto altro profilo potrebbe anche ritenersi che il trattamento sia lecito ai sensi dell'art. 6 par. 1 lett. b) Regolamento Ue GDPR («è necessario all'esecuzione di un contratto di cui l'interessato è parte», cioè il contratto di trasporto, ai fini di ottenere il pagamento del biglietto e la fornitura dei dati in caso di mancanza di titolo di viaggio);
- se il passeggero, richiesto dal controllore, non dichiara le proprie generalità commette il reato di cui all'art. 651 Cod. pen. E allora la foto serve alla sua identificazione;

Dr. Domenico Giannetta Esperto Diritto Amministrativo 443

- **il cittadino/passeggero avrebbe comunque i diritti previsti dal Codice sulla privacy** per sapere come e da chi verranno trattati i suoi dati (come verrà utilizzata la foto, con comparazione in banche dati o utilizzo di software, ecc., e per quanto tempo verrà conservata negli archivi);
- **anche se un passeggero dovesse denunciare il controllore che lo ha fotografato per trattamento illecito di dati personali,** abuso di potere o qualsiasi reato, non potrebbe essere condannato perché opera la scriminante dell'adempimento di un dovere art. 51 Cod. pen.

Dr. Domenico Giannetta Esperto Diritto Amministrativo 444

Quando il controllore potrebbe fare foto ai passeggeri?

C'è una via di mezzo tra queste due tesi? Ci sono degli elementi che tra il nero e il bianco danno una sfumatura di grigio e consentono al controllore di **fare foto ai passeggeri senza documenti** solo a certe condizioni e senza violare alcuna legge o le disposizioni sulla privacy?

Ecco una possibile **sintesi tra le due interpretazioni** contrapposte che abbiamo appena visto:

- **è legittimo il trattamento di un'immagine** per motivi di giustizia o di polizia ma è necessario tenere in considerazione il modo in cui avviene il trattamento dei dati dei cittadini;
- **il controllore di un mezzo pubblico** non è un poliziotto ma può inoltrare l'immagine scattata al titolare del trattamento dei dati affinché sia opportunamente tutelata;
- **il controllore non può in alcun modo divulgare** l'immagine scattata;
- **il passeggero ha il diritto di sapere** chi è il titolare del trattamento dei dati; quest'ultimo ha il dovere di fornire ai passeggeri l'adeguata informativa nel caso in cui sia prevista l'acquisizione della loro immagine;

- **il controllore, come detto, non è titolare del trattamento** dei dati ma solo un incaricato del trattamento; ciò significa che, prima di **scattare una foto a un passeggero**, dovrà ricevere l'atto di nomina, poiché non può trattare tali dati «se non è istruito in tal senso dal titolare del trattamento», come impone l'art. 29 del GDPR;
- **è possibile perseguire l'interesse del titolare** del trattamento dei dati sono se non lede le libertà, i diritti fondamentali ed i legittimi interessi del cittadino coinvolto, cioè: il passeggero deve attendersi il corretto trattamento dei suoi dati ma deve anche prevedere che se sale su un mezzo pubblico senza biglietto può essere multato o segnalato in qualsiasi momento;

Dr. Domenico Giannetta Esperto Diritto Amministrativo 447

- **prevalgono i princìpi di minimizzazione e di proporzionalità del trattamento:** va conservata la minor quantità possibile di dati e solo quelli che servono in rapporto alla tipologia del trattamento e alla finalità da perseguire.

Come si riassume, in senso pratico, tutto questo?
L'estrema sintesi ci dice che **il controllore si dovrebbe limitare a multare il passeggero senza biglietto senza fotografarlo**.

Dr. Domenico Giannetta Esperto Diritto Amministrativo 448

Nel caso in cui il viaggiatore non abbia un documento e il controllore decida di fotografarlo per una successiva identificazione, dovrebbe anche dimostrare di avere messo in atto ogni possibile comportamento volto a far vedere che quel trattamento dei dati era necessario.

La soluzione migliore, in ogni caso, di fronte alla mancata possibilità di identificare il passeggero abusivo sarebbe quella di chiamare le forze dell'ordine o, al limite, fotografarlo in caso di fuga.

Dr. Domenico Giannetta Esperto Diritto Amministrativo 449

Il Comune che decide di avvalersi di un servizio informatico per il pagamento delle sanzioni stradali **dovrà prestare particolare attenzione alla sicurezza dei sistemi messi a disposizione dai fornitori.** Formalizzando in maniera dettagliata gli accordi con i responsabili esterni del trattamento per evitare che in caso di problematiche tecniche l'eventuale sanzione ricada anche sul titolare.

Lo ha evidenziato il Garante per la protezione dei dati personali con l'ordinanza ingiunzione n. 419 del 2 dicembre 2021.

Un cittadino incorso nei rigori del codice stradale ha effettuato il pagamento di una sanzione utilizzando il servizio on-line messo a disposizione dal Comune tramite una società privata **riscontrando che era sufficiente inserire un numero progressivo di verbale e una data per aver accesso a verbali di soggetti sconosciuti, con tanto di fotografia dell'infrazione.**

Spid
La tua identità digitale

Con il Sistema Pubblico di Identità Digitale accedi in un click ai servizi online della Pubblica Amministrazione e dei privati aderenti, ogni volta che su un sito o un'app trovi il pulsante "Entra con SPID".

Dr. Domenico Giannetta Esperto Diritto Amministrativo SAFETY & SECURITY 453

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 454

Quale reato si commette nel violare la privacy di chi entra in una toilette pubblica o in un bagno privato come quello dell'ufficio, del negozio, del bar?

Non è uno scherzo, anche se così potrebbe sembrare: piazzare una telecamera nascosta in bagno potrebbe configurare un grave reato.
I chiarimenti vengono da una recente sentenza della Cass. sent. n. 15267/20 del 19.05.2020.
Non è la prima volta che i giudici si sono trovati a giudicare un caso simile, a testimonianza del fatto che l'idea non è poi così originale. Se poi nel bagno entrano anche bambini, le cose si mettono molto male per il responsabile di tale gesto.
Per stabilire però quale reato si commette nel posizionare una **telecamera nascosta in bagno** è necessario innanzitutto verificare dove si trova il bagno, ossia se si tratta di un bagno pubblico, di uno in un'abitazione privata o se in un ufficio.

Telecamera nascosta nel bagno di un luogo privato
Chi nasconde una telecamera nel bagno di un'abitazione altrui, **quindi in un luogo privato, commette il reato di «interferenze illecite nella vita privata». È prevista la reclusione da 6 mesi a 4 anni.**
Se però nel bagno entra anche un **minore d'età, scatta la condanna per produzione di materiale pedopornografico.** Infatti, **per la Cassazione, la riproduzione degli organi genitali della minore, pur in assenza di una rappresentazione lasciva, ha carattere pornografico;** non è necessario, per la configurabilità del reato di detenzione di materiale pedopornografico, un coinvolgimento in attività sessuali esplicite, reali o simulate, o, comunque, uno scopo sessuale. **Al contrario «è sufficiente il carattere pornografico delle immagini».**

Telecamera nascosta nel bagno dell'ufficio

L'ufficio viene considerato, dalla giurisprudenza, come un luogo equiparato alla prima dimora. Dunque, **chi posiziona una telecamera nel bagno del luogo di lavoro commette ugualmente il reato di «interferenze illecite nella vita privata».**

Affinché scatti il reato è necessario che la telecamera sia in funzione e le immagini siano visibili. Quindi, **non c'è illecito penale se la telecamera è scarica o semplicemente spenta, né se è mal posizionata tanto da non riuscire a riprendere alcuna scena.**

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 457

Telecamera nascosta in un bagno pubblico

Secondo la Cassazione sent. n. 10418/2015: **«Integra la contravvenzione di cui all'art. 660 c.p.** — e non il più grave delitto preveduto e punito dall'art. 615-bis c.p. né quello previsto dall'art. 610 c.p. — **l'installazione di una telecamera nel bagno dell'ente pubblico in quanto, trattandosi di luogo accessibile sia al pubblico che al personale dipendente del Comune, il fatto non risulta commesso in uno dei luoghi indicati dall'art. 614 c.p.».**

Posizionare una telecamera in un bagno pubblico può invece configurare il diverso – e sicuramente più blando – **reato di molestie punito dall'articolo 660 del codice penale con l'arresto fino a sei mesi o con l'ammenda fino a 516 euro.**

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata SAFETY & SECURITY 458

Chiaramente, anche in questo caso, **se dovesse risultare che nel bagno sono entrati dei minorenni,** allora potrebbe configurarsi – come anticipato già sopra – **il più grave delitto di pedopornografia**.
Secondo un'altra pronuncia, sempre a firma della Suprema Corte, **la telecamera nascosta sotto la porta di una toilette pubblica in modo da captare immagini di chi si trovi all'interno di essa** (nella specie, bagno di una stazione) – **considerato che la toilette pubblica non può essere considerata un domicilio – integra il reato di violenza privata.**

Cass. sent. n. 11522/2009: «Integra il reato di violenza privata (art. 610 c.p.) – e non quello di interferenze illecite nella vita privata (art. 615 bis c.p.) – la condotta di colui che introduca una telecamera sotto la porta di una toilette pubblica in modo da captare immagini di un minore che si trovi all'interno di essa (nella specie bagno di una stazione) – considerato che là toilette pubblica non può essere considerata un domicilio, ex art. 614 c.p. richiamato dall'art. 615 bis, neppure nel tempo in cui sia occupata da una persona. (La Corte ha osservato che l'interesse tutelato dall'art. 610 c.p. è la libertà morale – da intendersi come libertà di determinarsi spontaneamente – che ricomprende nel suo ambito non solo la facoltà di formare liberamente la propria volontà ma anche quella di orientare i propri comportamenti in conformità delle determinazioni liberamente assunte; d'altro canto, non è necessario che la condotta incriminata sia esplicitamente connotata da violenza o minaccia essendo sufficiente qualsiasi mezzo idoneo a privare coattivamente l'offeso della libertà di determinazione e di azione)».

In tale occasione, la Cassazione ha messo nero su bianco le seguenti parole: **«Va qualificata come violenza privata** (art. 610 c.p.) **la condotta di chi abbia introdotto una telecamera sotto la porta di un bagno pubblico in modo da captare immagini intime della persona che ivi si era chiusa, giacché, ai fini della configurabilità del reato "de quo", non è richiesta una condotta esplicitamente connotata da violenza o minaccia, posto che il requisito della violenza si identifica in qualsiasi mezzo idoneo a privare coattivamente l'offeso, anche per un lasso di tempo brevissimo, della libertà di determinazione e di azione: ciò che, in effetti, deve ritenersi a fronte di una imposizione insidiosa di una costrizione posta in essere contro il dissenso ragionevolmente prevedibile** (e solo successivamente manifestato) **della persona offesa».**

Infine, il servizio di osservazione realizzato dalla polizia giudiziaria per mezzo di una telecamera installata all'interno di un bagno di un locale pubblico non configura una forma di intercettazione tra presenti - Cass. sent. n. 6962/2003.

Telecamera nascosta nel bagno di un bar o di un negozio

Che succede, invece, se si chiede di entrare nel bagno di un bar, di un ristorante o di un altro esercizio commerciale e lì è posizionata una telecamera nascosta, non segnalata da alcun cartello?

Secondo la Cassazione, **un pubblico esercizio non può essere considerato "luogo di privata dimora".** Questo significa che la polizia giudiziaria è ben libera di posizionare telecamere di controllo. Ma neanche il proprietario del bagno va incontro a limiti: in questo caso, posizionare una telecamera in un bagno privato non è reato. **L'illecito penale scatta nell'ipotesi in cui le immagini dovessero essere diffuse.**

Codice Penale - Art. 610 Violenza privata

Chiunque, con violenza o minaccia, costringe altri a fare, tollerare od omettere qualche cosa è punito con la reclusione fino a quattro anni.

La pena è aumentata se concorrono le condizioni prevedute dall'articolo 339.

NOTE PROCEDURALI:
Arresto: *facoltativo in flagranza* (381 *c.p.p.*).
Fermo di indiziato di delitto: *non consentito.*
Misure cautelari personali: *consentite* (280, 287 *c.p.p.*).
Autorità giudiziaria competente: *Tribunale monocratico (*33ter *c.p.p.)*
Procedibilità: *d'ufficio* (50 *c.p.p.*).

Cass. pen. n. 17794/2017

Integra il delitto di violenza privata la condotta di colui che occupa il parcheggio riservato ad una specifica persona invalida in ragione del suo "status", impedendone l'accesso, e, quindi, privandola della libertà di determinazione e di azione. (Fattispecie in cui l'imputato aveva abusivamente occupato il parcheggio riservato ad uno specifico disabile dalle 10,40 del mattino alle 2 di notte, ora in cui l'autovettura veniva coattivamente rimossa dalla polizia locale).

(Cassazione penale,Sez. V,sentenza n. 17794 del 7 aprile 2017)

Cass. pen. n. 1786/2017

Ai fini dell'integrazione del delitto di violenza privata (art. 610 cod. pen.) è necessario che la violenza o la minaccia costitutive della fattispecie incriminatrice comportino la perdita o, comunque, la significativa riduzione della libertà di movimento o della capacità di autodeterminazione del soggetto passivo, essendo, invece, penalmente irrilevanti, in virtù del principio di offensività, i comportamenti che, pur costituendo violazioni di regole deontologiche, etiche o sociali, si rivelino inidonei a limitarne la libertà di movimento, o ad influenzarne significativamente il processo di formazione della volontà. (Fattispecie in cui la S.C. ha escluso la sussistenza del reato nella condotta dell'imputato che, al fine di fare rispettare il regolamento condominiale, aveva reiteratamente minacciato, aggredito ed ingiuriato alcuni minorenni che facevano rumori giocando nel cortile condominiale con dei palloni, ed aveva tagliato questi ultimi con un coltello, in quanto tale condotta non aveva impedito ai giovani di riprendere gli stessi giochi). *(Cassazione penale,Sez. V,sentenza n. 1786 del 16/01/2017)*

Codice Penale – Art. 614 Violazione di domicilio

Chiunque s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero vi s'introduce clandestinamente o con inganno, è punito con la reclusione da uno a quattro anni (615; 14 Cost.).

Alla stessa pena soggiace chi si trattiene nei detti luoghi contro l'espressa volontà di chi ha diritto di escluderlo, ovvero vi si trattiene clandestinamente o con inganno.

Il delitto è punibile a querela della persona offesa (120; 336 c.p.p.).

La pena è da due a sei anni, e si procede d'ufficio (50 c.p.p.), se il fatto è ommesso con violenza sulle cose (392), o alle persone (581, 582), ovvero se il colpevole è palesemente armato.

NOTE PROCEDURALI:

Arresto: facoltativo in flagranza (381 c.p.p.).

Fermo di indiziato di delitto: non consentito.

Misure cautelari personali: primo e quarto comma, consentite (280, 287 c.p.p.); secondo comma, non consentite.

Autorità giudiziaria competente: Tribunale monocratico (33 ter c.p.p.).

Procedibilità: primo e secondo comma, a querela di parte (336 c.p.p.); quarto comma, d'ufficio (50 c.p.p.).

Ratio Legis

La ratio di tale disposizione si coglie nella considerazione che i luoghi di dimora non sono intesi solo nella loro materialità, ma anche come proiezione spaziale della persona, la cui libertà individuale si estrinseca nell'interesse alla tranquillità e sicurezza dei luoghi in cui si svolge la propria vita privata.

Cass. pen. n. 10498/2018
Ai fini della configurabilità del reato di violazione di domicilio (art. 614 c.p.), non possono essere considerati luoghi di privata dimora quelli normalmente destinati ad attività di lavoro, di studio e di svago, ai quali chiunque possa accedere senza necessità di preventivo consenso da parte dell'avente diritto, nulla rilevando che in essi possano anche svolgersi occasionalmente atti della vita privata, ferma restando, tuttavia, l'operatività della tutela penale con riguardo alle parti di detti luoghi (quali, ad esempio, retrobottega, bagni privati o spogliatoi), che abbiano eventualmente assunto le caratteristiche proprie dell'abitazione in quanto destinate anche allo svolgimento di atti della vita privata in modo riservato e con preclusione dell'accesso da parte di estranei. (Nella specie, in applicazione di tali principii, è stata esclusa la sussistenza del reato di violazione di domicilio in un caso in cui la condotta posta in essere dagli imputati era consistita nell'ingresso arbitrario, a scopo dimostrativo, nei locali di un istituto privato di istruzione).
(Cassazione penale,Sez. V,sentenza n. 10498 del 8 marzo 2018)

Codice Penale – Art. 615 bis Interferenze illecite nella vita privata

Chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'art. 614, è punito con la reclusione da sei mesi a quattro anni.

Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo.

I delitti sono punibili a querela della persona offesa (120; 336 c.p. p.); tuttavia si procede d'ufficio (50 c.p.p.) e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale (357) o da un incaricato di un pubblico servizio (358), con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato.

NOTE PROCEDURALI:

Arresto: facoltativo in flagranza (381 c.p.p.).

Fermo di indiziato di delitto: non consentito.

Misure cautelari personali: consentite (280, 287 c.p.p.).

Autorità giudiziaria competente: Tribunale monocratico (33 ter c.p.p.).

Procedibilità: a querela di parte (336 c.p.p.); d'ufficio (50 c.p.p.) se ricorre l'ipotesi prevista dal terzo comma.

Ratio Legis

Il legislatore ha introdotto tale norma per far fronte alle sempre più presenti minacce alla riservatezza personale (privacy) legate all'evoluzione delle moderne tecnologie

Cass. pen. n. 4669/2018

L'art. 615-bis cod. pen., che punisce la condotta di chi procura immagini o notizie attinenti alla vita privata, che si svolgono in luoghi di privata dimora utilizzando mezzi di ripresa visiva o sonora, è configurabile anche nell'ipotesi tentata qualora, adoperando tali strumenti, l'imputato non sia riuscito a procurarsi immagini o notizie della vita privata altrui. (Fattispecie in cui l'imputato, introducendo nel bagno dell'ufficio riservato al personale femminile una microtelecamera, a causa di un guasto tecnico di quest'ultima, non era riuscito a riprendere alcuna delle utenti).
(Cassazione penale, Sez. V, sentenza n. 4669 del 31 gennaio 2018)

Cass. pen. n. 34151/2017

Ai fini della integrazione del reato di interferenze illecite nella vita privata (art. 615 bis cod. pen.), deve escludersi che le scale condominiali ed i relativi pianerottoli siano "luoghi di privata dimora" cui estendere la tutela penalistica alle immagini ivi riprese, trattandosi di zone che non assolvono alla funzione di consentire l'esplicazione della vita privata al riparo di sguardi indiscreti, essendo destinati all'uso di un numero indeterminato di soggetti
(Cassazione penale, Sez. V, sentenza n. 34151 del 12 luglio 2017)

Codice Penale – Art. 660 Molestia o disturbo alle persone

Chiunque, in un luogo pubblico o aperto al pubblico, ovvero col mezzo del telefono, per petulanza o per altro biasimevole motivo, reca a taluno molestia o disturbo è punito con l'arresto fino a sei mesi o con l'ammenda fino a € 516 (162 bis, 659, 688).

Ratio Legis

La norma in esame è diretta a tutelare l'ordine pubblico, preservando nello specifico la sicurezza e la tranquillità dei consociati

Cass. pen. n. 19924/2014

In tema di molestia o disturbo alle persone, la contravvenzione di cui all'art. 660 cod. pen. che mira a prevenire il turbamento della pubblica tranquillità attuato mediante l'offesa alla quiete privata, integra fattispecie distinta, autonoma e concorrente rispetto al reato di atti persecutori di cui all'art. 612 bis cod. pen. in cui non viene assorbita per la diversità dei beni giuridici tutelati.
(Cassazione penale, Sez. I, sentenza n. 19924 del 14 maggio 2014)

Cass. pen. n. 3758/2014

Il reato di molestia di cui all'art. 660 cod. pen. non è necessariamente abituale, per cui può essere realizzato anche con una sola azione di disturbo o di molestia, purché ispirata da biasimevole motivo o avente il carattere della petulanza, che consiste in un modo di agire pressante ed indiscreto, tale da interferire sgradevolmente nella sfera privata di altri. (Fattispecie nella quale è stato escluso che integrasse la contravvenzione una sola telefonata, effettuata in orari normali, al fine, non di molestare, ma di ingiuriare e minacciare la persona offesa).

(Cassazione penale, Sez. I, sentenza n. 3758 del 28 gennaio 2014)

Cass. pen. n. 19924/2014

In tema di molestia o disturbo alle persone, la contravvenzione di cui all'art. 660 cod. pen. che mira a prevenire il turbamento della pubblica tranquillità attuato mediante l'offesa alla quiete privata, integra fattispecie distinta, autonoma e concorrente rispetto al reato di atti persecutori di cui all'art. 612 bis cod. pen. in cui non viene assorbita per la diversità dei beni giuridici tutelati.

(Cassazione penale, Sez. I, sentenza n. 19924 del 14 maggio 2014)

Cass. pen. n. 17787/2008

Il reato di molestie o disturbo alle persone, pur non essendo per sua natura necessariamente abituale, in quanto può essere realizzato anche con una sola azione di disturbo o di molestia, può però assumere tale forma, incompatibile con la continuazione allorché non sia stata tanto la modalità delle condotte poste in essere, quanto la loro reiterazione assillante (nella specie numerose telefonate di tono offensivo) a determinare l'effetto pregiudizievole dell'interesse tutelato.
(Cassazione penale, Sez. I, sentenza n. 17787 del 5 maggio 2008)

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 481


Consigli per rispettare la privacy se si usa un DRONE a fini ricreativi
1. SEGUI SEMPRE LE REGOLE
Usare i droni per scopi ricreativi è lecito e divertente, ma occorre sempre rispettare la privacy degli altri e informarsi bene sulle regole previste dall'ENAC per far volare i Sistemi Aeromobili a Pilotaggio Remoto (www.enac.gov.it).
1997 2017
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE


2. FAI ATTENZIONE ALLE RIPRESE
Se si fa volare a fini ricreativi un drone munito di fotocamera in un luogo pubblico (parchi, strade, spiagge) è meglio evitare di invadere gli spazi personali e l'intimità delle persone. La diffusione di riprese realizzate con il drone (sul web, sui social media, in chat) può avvenire solo con il consenso dei soggetti ripresi, fatti salvi particolari usi connessi alla libera manifestazione del pensiero, come quelli a fini giornalistici. Negli altri casi, quando è eccessivamente difficile raccogliere il consenso degli interessati, è possibile diffondere le immagini SOLO se i soggetti ripresi non sono riconoscibili, o perché ripresi da lontano, o perché si sono utilizzati appositi software per oscurare i loro volti. Occorre poi evitare di riprendere e diffondere immagini che contengono dati personali come targhe di macchine, indirizzi di casa, ecc. Le riprese che violano gli spazi privati altrui (casa, giardino domestico) sono invece SEMPRE da evitare, anche perché si potrebbero violare norme penali.

3. RISPETTA GLI ALTRI

La presenza di un drone che effettua riprese nelle vicinanze può dare la **sensazione di essere osservati**, inducendo disagio e influenzando il normale comportamento delle persone. E' quindi buona regola usare questi strumenti **senza invadere la sfera personale degli altri**, magari anche comunicando preventivamente le proprie intenzioni. Ad esempio, se si vuole far volare un drone per riprendere una festa nel proprio giardino di casa, sarebbe bene prima avvisare i vicini, che hanno il diritto di chiedere di **non** essere - anche **solo inavvertitamente** - ripresi nel loro privato. Un'altra buona pratica da seguire è quella di fare in modo che il **pilota** del drone sia **sempre ben visibile,** così da non suscitare sospetti o allarme negli altri.

4. NON DIVENTARE UN «ORECCHIO INDISCRETO»

Non si possono usare droni per captare **volontariamente** conversazioni altrui. Eventuali **frammenti di conversazione** registrati in modo **accidentale** possono essere utilizzati (ad esempio, per pubblicare un video online) **SOLO** se **NON** rendono riconoscibile il contesto, cioè il contenuto dei discorsi e le persone coinvolte.

5. A PROVA DI PRIVACY

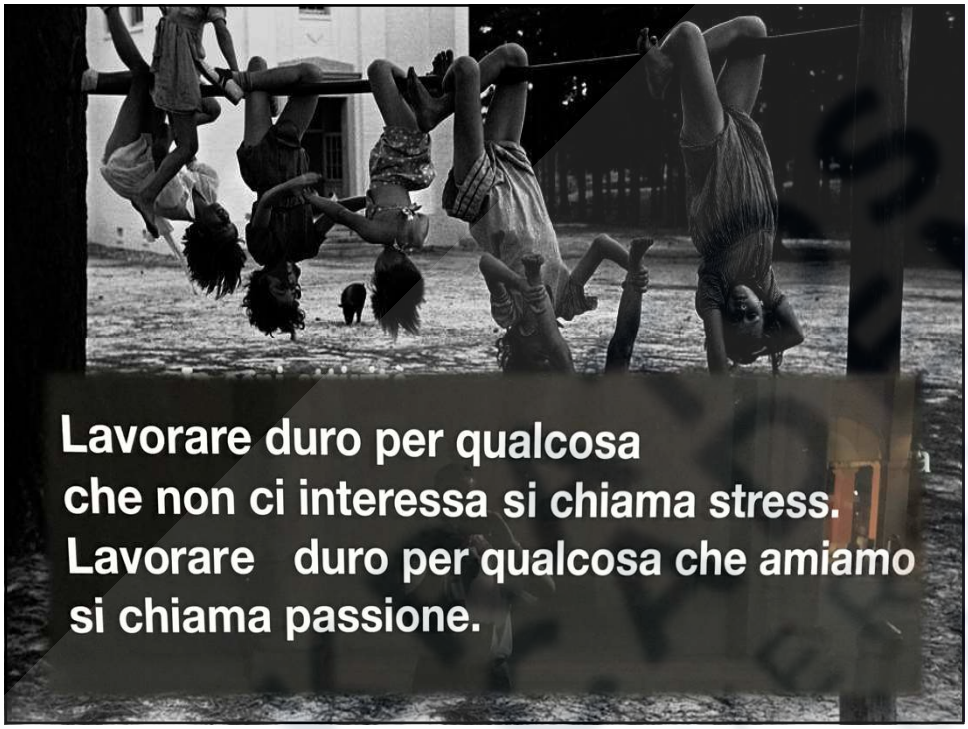
In base a quanto previsto dal nuovo Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679), i droni, come tutti i dispositivi elettronici, devono rispettare i principi di **privacy by design** e **privacy by default**. Cioè devono essere costruiti e configurati per raccogliere meno dati possibile.

6. COME TUTELARE LA TUA PRIVACY

Se è possibile individuare il pilota del drone, si possono chiedere a lui informazioni su come intende utilizzare le riprese ed eventualmente **negare il consenso** al trattamento dei dati raccolti, specie se sono previste forme di diffusione delle immagini. **E nel caso si ritenesse di essere stati vittime di violazioni della propria privacy**, ci si può rivolgere al Garante per la protezione dei dati personali o, in alternativa, all'Autorità giudiziaria.


KRATOS ACADEMY
UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
... ?
... ?
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
489


KRATOS ACADEMY
UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
ALTRE DOMANDE?
NO! NO! GRAZIE!
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
490


Lavorare duro per qualcosa
che non ci interessa si chiama stress.
Lavorare duro per qualcosa che amiamo
si chiama passione.


KRATOS ACADEMY
UNIVERSITÀ POPOLARE
ESAARCO
CONFEDERAZIONE
ESERCENTI AGRICOLTURA ARTIGIANATO COMMERCIO
TÜV SÜD
Dr. Domenico Giannetta
Esperto Sicurezza Urbana Integrata
SAFETY & SECURITY
492

Di tutto restano tre cose:

la certezza che stiamo sempre iniziando,

la certezza che abbiamo bisogno di continuare,

la certezza che saremo interrotti prima di finire.

Pertanto, dobbiamo fare dell'interruzione un nuovo cammino, della caduta un passo di danza, della paura una scala, del sogno un ponte, del bisogno un incontro.

Fernando Pessoa

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 493

Mi auguro di aver suscitato una giusta dose di curiosità intorno all'argomento

Dr. Domenico Giannetta Esperto Sicurezza Urbana Integrata 494


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
Dr. Giannetta Domenico
Comandante Polizia Locale - Responsabile Suap - Esperto Sicurezza Urbana
Segretario Nazionale PL (Associazione Professionale Polizia Locale)
Docente Scuola Regionale Polizia Locale della Campania
Docente Scuola Regionale Polizia Locale della Puglia
Componente Comitato Tecnico Consultivo Regione Campania
Responsabile Regione Campania Formazione SULPL
Docente Master MA881 A.A. 2018/2019 – 2020/2021 – 2022/2023
Università Telematica Pegaso
Docente Corsi di Formazione A.A. 2020/2021- 2022/2023
Università Telematica Giustino Fortunato BN
Docente associato presso la Cattedra di Politiche e Strategie Operative per la Sicurezza Urbana – Anno 2021 - 2022
Polo Accademico Internazionale – Università degli Studi Unidemontaigne
Relatore Convegni Nazionali e Formatore :
Fondazione Gazzetta Amministrativa della Repubblica Italiana - PL – Sulpl - Aspol - Infopol s.r.l. - Edipol s.r.l. - Maggioli Editore S.p.A. - Assinter - Trevi Formazione – Officina della Formazione - La Formazione - Myo SpA - Centro Studi Bellunese - Consorzio Comuni di Bolzano - Formez PA - Logos PA – Isform & Consulting s.r.l.
Kratos Academy – Università Popolare
E-MAIL
Tel./Mail : 333/3052645 – 349/2312654 - giannetta.domenico@libero.it
Dr. Domenico Giannetta
Comandante Polizia Locale
SAFETY & SECURITY
495


KRATOS ACADEMY UNIVERSITÀ POPOLARE
ESAARCO CONFEDERAZIONE
TÜV SÜD
Dr. Giannetta Domenico
Comandante Polizia Locale - Responsabile Suap - Esperto Sicurezza Urbana
Segretario Nazionale PL (Associazione Professionale Polizia Locale)
Grazie dell'attenzione
e
Buon Lavoro
E-MAIL
Tel./Mail : 333/3052645 – 349/2312654 - giannetta.domenico@libero.it
Dr. Domenico Giannetta
Comandante Polizia Locale
SAFETY & SECURITY
496