Eventi paralleli

Workshop di approfondimento

Videosorveglianza Urbana Integrata

Evento favorito da

BETTINI
VIDEO & SECURITY TECHNOLOGY

Workshop di approfondimento

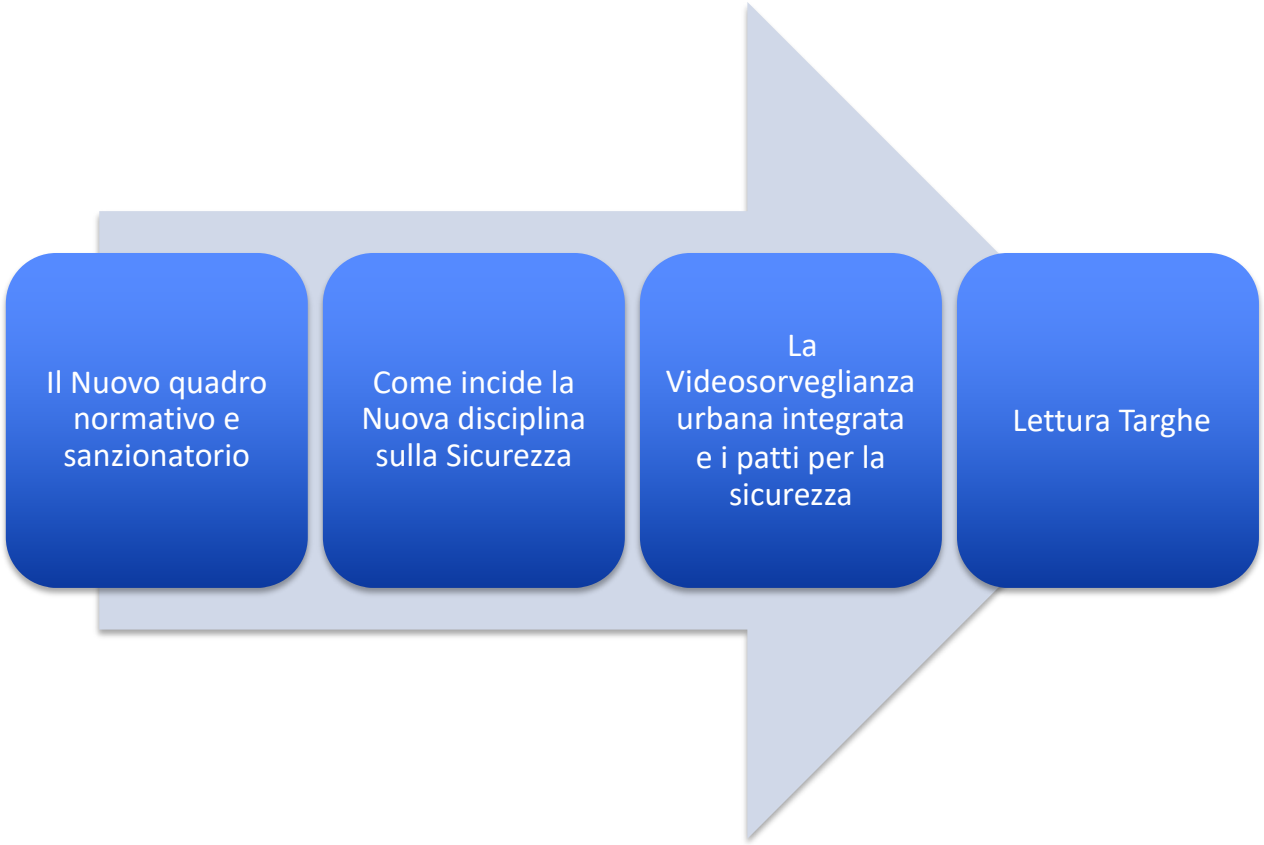
Videosorveglianza Urbana Integrata

Videosorveglianza urbana integrata e la nuova disciplina privacy

Marco Soffientini

Avvocato esperto di privacy e diritto delle nuove tecnologie

STRUTTURA DELLA PRESENTAZIONE: La Videosorveglianza Urbana tra GDPR e Direttiva 680/2016



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

EVOLUZIONE TECNOLOGICA

Biometria

Geolocalizzazione

Cloud

Videosorveglianza

GLOBALIZZAZIONE

Condivisione di dati

Big Data

Smart City

Sorveglianza di massa

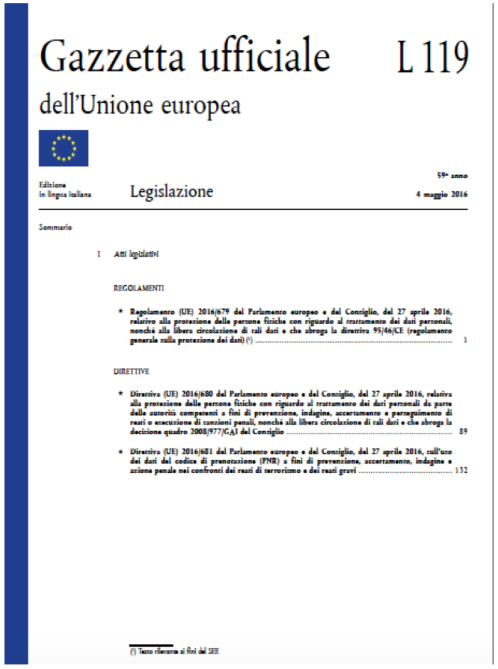

Gazzetta ufficiale L 119
dell'Unione europea
Legislazione

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

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

REGOLAMENTO UE 2016/679

GENERAL DATA PROTECTION REGULATION – GDPR -



Gazzetta ufficiale L 119
dell'Unione europea

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

Sommario

I Atti legislativi

REGOLAMENTI

* Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (1) 1

DIRETTIVE

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

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

(1) Testo rilevante ai fini del SEE

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

SANZIONI –ART. 83 -

SOCIAL E MINORI –ART. 8 -

DIRITTO ALL'OBLIO –ART. 17 -

Diritto alla portabilità dei dati – ART. 20 -

RESPONSABILITA' VERIFICABILE – ART. 5.2 -

Diritto di accesso dell'interessato – ART. 15 -

Registro delle attività di trattamento – ART. 30 -

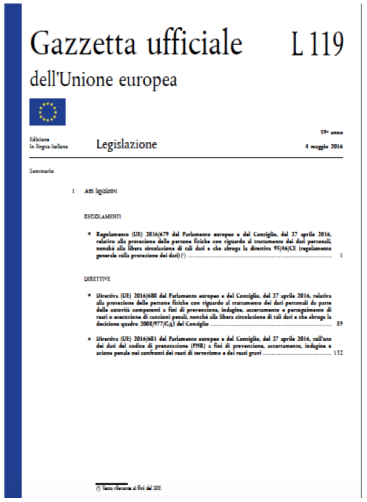
Notifica di una violazione dei dati personali – ART. 33 -

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

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

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

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


Gazzetta ufficiale L 119
dell'Unione europea
Legislazione

LE SANZIONI NEL GDPR

ART. 83, Paragrafo 4 GDPR

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

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

ART. 83, Paragrafo 5 GDPR

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

DIRETTIVA 2016/680

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

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

D.lgs 18 Maggio 2018, n. 51

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

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

CODICE DELLA PRIVACY

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

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

integrato con le modifiche introdotte dal

DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"
(in G.U. 4 settembre 2018 n.205)

1

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

VIDEOSORVEGLIANZA:LE PRINCIPALI FONTI NORMATIVE

REGOLAMENTO UE 2016/679


DIRETTIVA 680/2016 – D.LGS 51/2018

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

STATUTO DEI LAVORATORI – L. n.300/1970

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

PACCHETTO SICUREZZA 2017: "Disposizioni urgenti in materia di sicurezza delle città"

Il decreto-legge 20 febbraio 2017, n. 14, recante "Disposizioni urgenti in materia di sicurezza delle città", convertito, con modificazioni, dalla legge 18 aprile 2017, n.48, indica i patti sottoscritti dal Prefetto e dal Sindaco tra i principali strumenti per la promozione della sicurezza urbana (art. 5).

prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria attraverso l'installazione di **sistemi di videosorveglianza**

PATTI TRA PREFETTURA E SINDACO
(ART. 5 D.L. 20 Febbraio, n.14)

Sono i principali strumenti per la promozione della sicurezza urbana

Cosa sono:

I patti - che tengono conto anche delle esigenze delle aree rurali confinanti con il territorio urbano – definiscono concretamente gli interventi da mettere in campo incidendo su specifici contesti territoriali.

Obiettivi:

Tra gli obiettivi prioritariamente perseguiti la norma individua la prevenzione e il contrasto dei fenomeni di criminalità diffusa e predatoria attraverso l'installazione di **sistemi di videosorveglianza** per i quali è stata autorizzata una spesa complessiva di trentasettemilioni di euro, riferita al triennio 2017/2019

Sette milioni di euro per il 2017 e quindici milioni di euro per ciascuno degli esercizi finanziari 2018 e 2019.

Le modalita` di presentazione delle richieste di ammissione ai suddetti finanziamenti, nonche´ i criteri di ripartizione delle risorse, sono stati definiti con decreto del Ministro dell'Interno, di concerto con il Ministro dell'Economia e delle Finanze, in data 31 gennaio 2018 (art. 2)

DM 31.01.2018

Non e' comunque ammesso il finanziamento per la sostituzione o la manutenzione di sistemi di videosorveglianza gia' realizzati

1. Sottoscrizione dei «patti»
2. Approvazione del «progetto»

L'art. 2 del DM 31.01.2018 fissa i requisiti necessari per accedere all'erogazione del contributo.

1 In particolare, alla lettera a) del comma 1, è previsto che possono fare domanda solo i Comuni **che hanno sottoscritto i patti** di cui all'art. 5, comma 1, del D.L. 20.02.2017, n. 14 , **il cui testo contempli tra le misure anti degrado l'installazione di sistemi di videosorveglianza** in determinate aree del territorio comunale o infra-comunale.

2 Altra condizione di ammissibilita` del finanziamento che va evidenziata è la preventiva **approvazione del progetto di videosorveglianza** in sede di Comitato provinciale per l'ordine e la sicurezza pubblica.

2O Febbraio 2017

D.L. 20.02.2017, n.14 (conv. L. 18.04.2017, n.48) – Disposizioni Urgenti in materia di sicurezza delle città

24 Gennaio 2018

Linee Generali sulla sicurezza integrata (in attuazione dell'articolo 2, D.L n.14/2017, con. L. n. 48/2017)

Le Linee generali sulla sicurezza integrata adottate con accordo in Conferenza Unificata nell'individuare le comunicazioni riguardanti le statistiche sull'andamento della delittuosità elaborate in forma consolidata dal CED Interforze ex art. 8 della Legge 121/1981 come uno strumento idoneo ai fini dello scambio informativo tra la polizia locale e le forze di polizia,

precisa (pag.5) come i dati in questione saranno forniti in forma di elaborazione statistica anonima, tuttavia «in un ottica di doverosa tutela della *privacy* secondo le indicazioni fornite dal Garante per la protezione dei dati personali, i Prefetti espungeranno dalle comunicazioni i rilievi statistici che, per la loro ridotta entità numerica, possono consentire l'agevole identificazione dei soggetti interessati, secondo i criteri dell'articolo 5 del Codice di deontologia e buona condotta per i trattamenti dei dati personali per scopi statistici»

Per effetto dell'articolo 20, commi 3 e 4, del d.lgs 101 del 2018 Il Garante ha verificato la conformità al Regolamento UE 2016/679 delle disposizioni contenute nei codici deontologici.

Con Provvedimento n. 515 del 19 dicembre 2018 ha pubblicato (G.U. n.11 del 14 gennaio 2019) le nuove regole deontologiche per trattamenti ai fini statistici ai sensi dell'articolo 20, comma 4, del d.lgs 10 agosto 2018, n.101.

Il Garante ha confermato l'articolo 5 e quindi anche il criterio di cui all'articolo 5.1.e

Il rispetto delle disposizioni contenute nelle regole deontologiche costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali e il mancato rispetto delle stesse comporta l'applicazione della sanzione di cui **all'art. 83, paragrafo 5 del Regolamento** (artt. 2-quater, comma 4, e 166, comma 2, del Codice).

26 Luglio 2018

Linee Guida per l'Attuazione della Sicurezza Urbana

NELLA SEDUTA DI CONFERENZA STATO CITTA' ED AUTONOMIE LOCALI DEL 26 LUGLIO 2018 E' STATO ADOTTATO L'ACCORDO SULLE LINEE GUIDA PER L'ATTUAZIONE DELLA SICUREZZA URBANA.

Si precisa nell'accordo che sull'utilizzo integrato degli **impianti di videosorveglianza** i patti per la sicurezza dovranno prevedere una disciplina coerente e conforme ai principi stabiliti dalle linee generali secondo cui i trattamenti di dati di polizia sono ammessi solo nei casi e per le finalità stabilite da specifiche disposizioni di legge.

«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»).

Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi **all'ubicazione**, un **identificativo online** o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. (Art. 4, n. 1 GDPR)

LETTURA TARGHE

La Corte di Cassazione, con sentenza 44940 del 2 dicembre 2011, ha ritenuto dato personale *"anche il numero di targa del veicolo, a nulla rilevando che esso sia visibile a tutti quando l'auto circola per strada. Ciò che rileva, ovviamente non è il numero in sè, ma il suo abbinamento ad una persona. Del resto, in tal senso si è orientata la giurisprudenza di questa di Corte, ad es. con riferimento al numero di utenza cellulare di un soggetto. Anche in questo caso, per altro, soccorre la stessa lettera della legge (art. 4, comma 1, lettera b) che qualifica "dato personale" qualunque informazione relativa ad una persona (fisica), identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".*

LA GESTIONE DEI SISTEMI DI LETTURA TARGHE E INTEGRAZIONE AL S.C.N.T.T.

PROFILI PRIVACY

CIRC. MIN. INT. 28 FEBBRAIO 2017

Secondo la Circolare Ministeriale il riversamento dei dati delle targhe acquisiti dalle telecamere Comunali alla banca dati del Sistema Nazionale Targhe e Transiti ospitato presso il Centro Elettronico Nazionale della Polizia di Stato sito in Napoli, essendo finalizzato ad attività di sicurezza pubblica deve essere interconnesso in maniera tale che il Comitato Provinciale per l'Ordine e la Sicurezza Pubblica possa verificare la sussistenza dei **profili autorizzativi delle Forze di Polizia a competenza generale e delle Polizie locali**.

I profili autorizzativi delle forze di polizia e della polizia locale dipendono dalla finalità perseguita

* Art. 53 CdP abrogato dall'articolo 49, comma 1 D.lgs 18 Maggio 2018, n. 51.

Il contenuto dei patti . . . .

[OMISSIS] Occorre tenere presente che i sistemi di videosorveglianza attivati dalle Forze di polizia rispondono alle finalità di prevenzione generale dei reati e di salvaguardia della sicurezza pubblica. Essi, pertanto, sono utilizzabili per finalità di contrasto a fenomeni delittuosi o di prevenzione delle possibili turbative dell'ordine e della sicurezza pubblica di esclusiva competenza statale che esorbitano l'ambito della sicurezza urbana, come definita dall'art. 4 del D.L. n. 14 del 2017.

Tenuto conto di ciò, l'utilizzazione in comune dei sistemi dovrà avvenire in ossequio al principio del *rispetto delle rispettive competenze,* in più momenti ribadito dal decreto legge e a quelli di «pertinenza e non eccedenza» dei trattamenti dei dati personali rispetto ai compiti istituzionali assegnati, sanciti dal ricordato «Codice della Privacy».

In sede di applicazione pratica l'utilizzazione in comune degli apparati di videosorveglianza e, quindi, delle immagini riprese avverrà in maniera selettiva, garantendo alla Polizia Locale di disporre degli apparati delle Forze di polizia dislocati nelle aree urbane dove si presentano i fenomeni rilevanti per la sicurezza urbana o che comunque appaiono di interesse per l'assolvimento degli specifici compiti istituzionali demandate alle stesse polizie locali.

Con la stessa logica, saranno individuati gli apparati di videosorveglianza attivati dagli Enti locali, rilevanti per le attività di tutela dell'ordine e della sicurezza pubblica riservate alle Forze di Polizia.

Linee generali, 24 gennaio 2018 pag.9

Un caso pratico: brevi cenni

TEMPI DI CONSERVAZIONE DELLE IMMAGINI

L'istituto della 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.

Provv. 08.04.2010, § 3.2.1.

L'istituto della verifica preliminare (c.d. *prior checking*), previsto dall'articolo 17 del Codice Privacy, rappresenta una clausola di salvaguardia per i dati personali, che non sono né sensibili né giudiziari, ma che, in determinate condizioni, corrono "rischi specifici".

La Verifica Preliminare nella Videosorveglianza

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

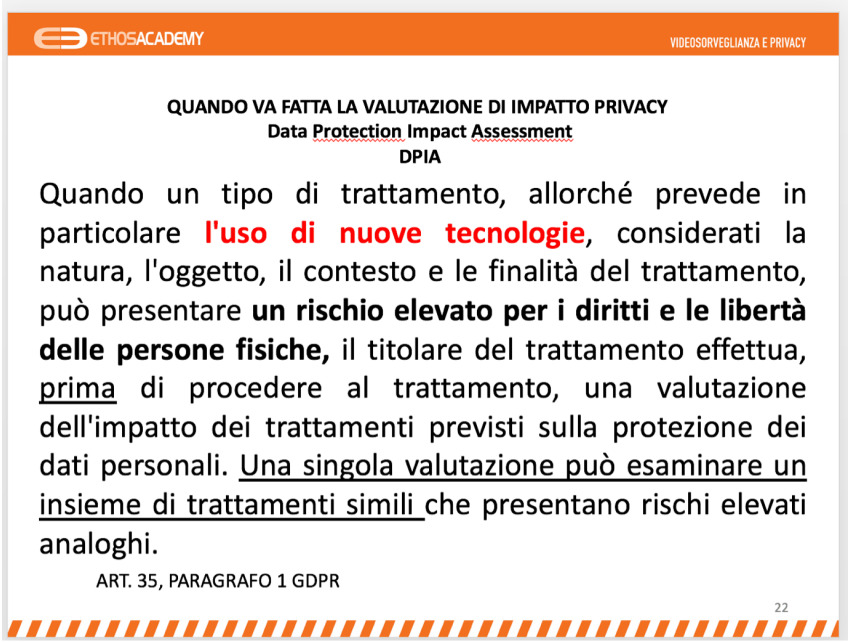
- dei **sistemi di videosorveglianza abbinati a dati biometrici**;
- degli **impianti dotati di software, che consentono il Riconoscimento delle persone**;
- dei **sistemi c.d. intelligenti**, che cioè non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente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

~~VERIFICA PRELIMINARE~~

DPIA

Con la piena attuazione del GDPR 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 di effettuazione di valutazioni di impatto in piena autonomia.

OBIETTIVO DELLA DPIA


ETHOSACADEMY VIDEOSORVEGLIANZA E PRIVACY

QUANDO VA FATTA LA VALUTAZIONE DI IMPATTO PRIVACY
Data Protection Impact Assessment
DPIA

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,** il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

ART. 35, PARAGRAFO 1 GDPR

22

Rispettare i «PRINCIPI»

GESTIRE I «RISCHI»

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

Tempi di conservazione delle immagini del sistema di Videosorveglianza

La conservazione delle immagini
§ 3.4.3. Provv.08.04.2010

Il **paragrafo 3.4.3 del Provv. 08.04.2010** afferma che per i Comuni, e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, il termine massimo di durata della conservazione dei dati sia 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"*.

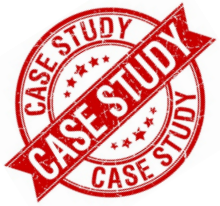
La conservazione delle immagini
§ 3.4.4. Provv.08.04.2010

Ne segue che si rende **necessario** richiedere una **verifica preliminare** nel caso di **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 effettiva in corso.

Sia per il settore privato che per quello pubblico, un tempo di allungamento superiore alla settimana necessita di una richiesta al Garante (c.d. verifica preliminare ai sensi dell'art. 17 del Codice Privacy), avendo cura di evidenziare l'eccezionalità della richiesta rispetto al principio di proporzionalità.

Appare opportuno precisare che ***non deve essere sottoposta ad una verifica preliminare*** *del Garante l'esigenza di conservare le immagini anche oltre il periodo di una settimana sopra indicato qualora* ***intervenga*** *una* ***specifica richiesta*** *in tale senso* ***dell'autorità giudiziaria*** *o di polizia giudiziaria in relazione a un'attività investigativa in corso.*

Linee Guida per i Comuni in materia di Videosorveglianza – Anci – Pag. 23



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

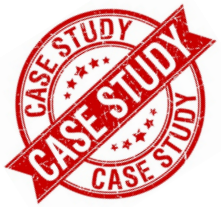
Tempi di conservazione delle targhe dei veicoli riprese dai sistemi di Videosorveglianza della polizia municipale.

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

Conservazione delle targhe dei veicoli

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

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



Conservazione delle targhe dei veicoli

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

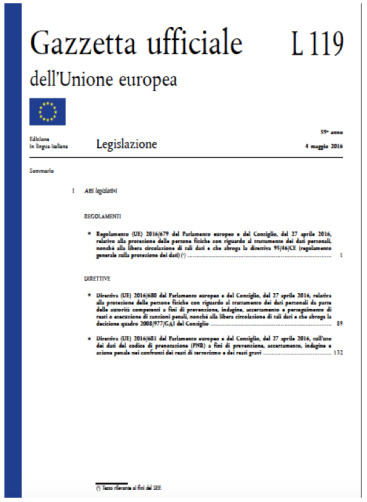
Con riferimento al caso di specie, il **provvedimento consente** quindi un prolungamento del termine di conservazione delle immagini anche in presenza di richieste della polizia giudiziaria motivate però in relazione a specifiche e puntuali attività investigative in corso, **dovendosi escludere una preventiva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

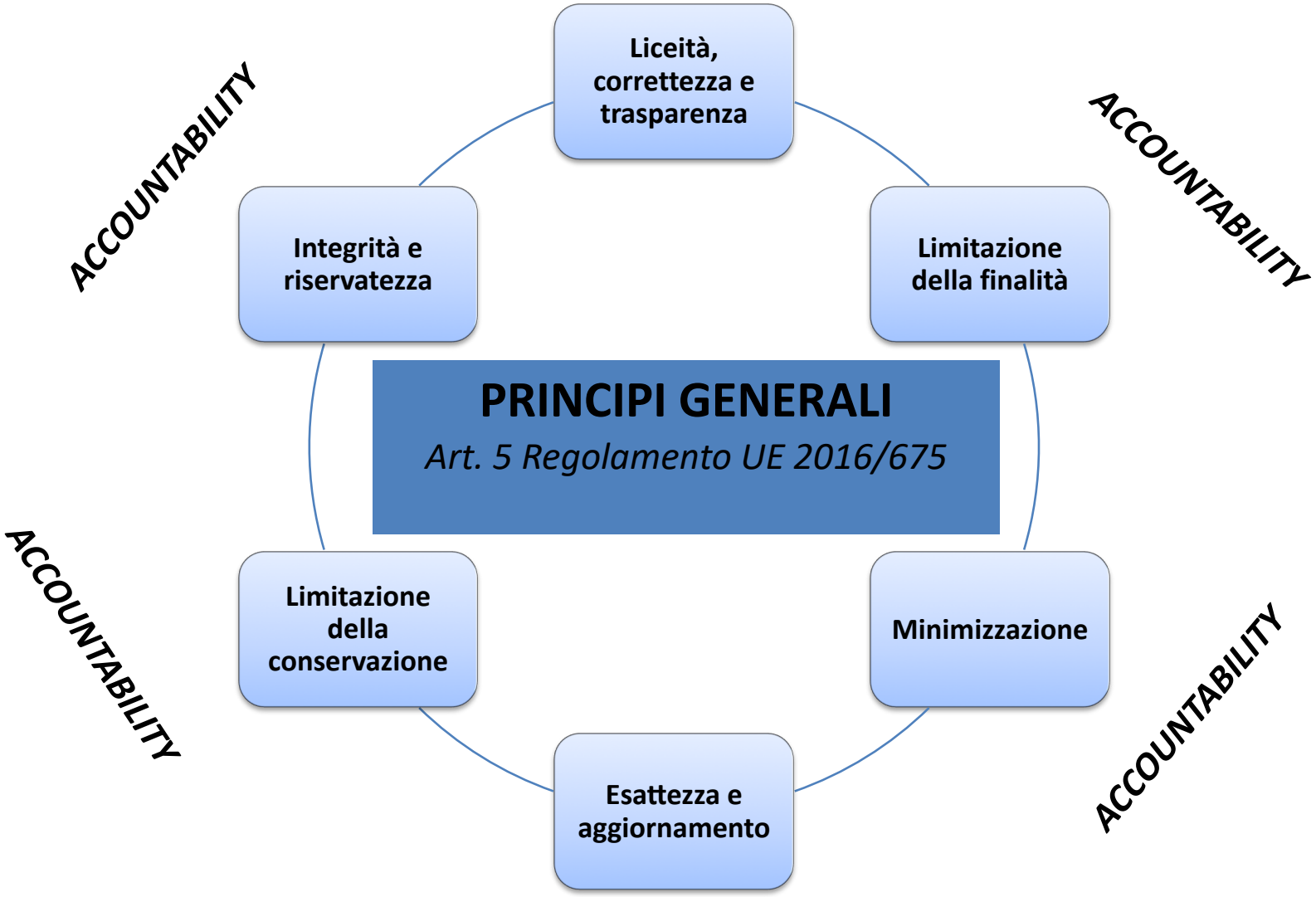
COME RISPETTARE LA DISCIPLINA PRIVACY

BREVI CENNI

IL PRINCIPIO DELL'ACCOUNTABILITY

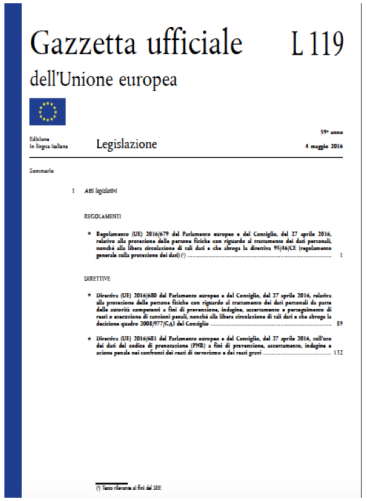
Il principio dell'accountability o di responsabilizzazione consiste nel dovere del titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate al fine di dimostrare che il trattamento è effettuato conformemente al regolamento.


Gazzetta ufficiale L 119
dell'Unione europea
Legislazione



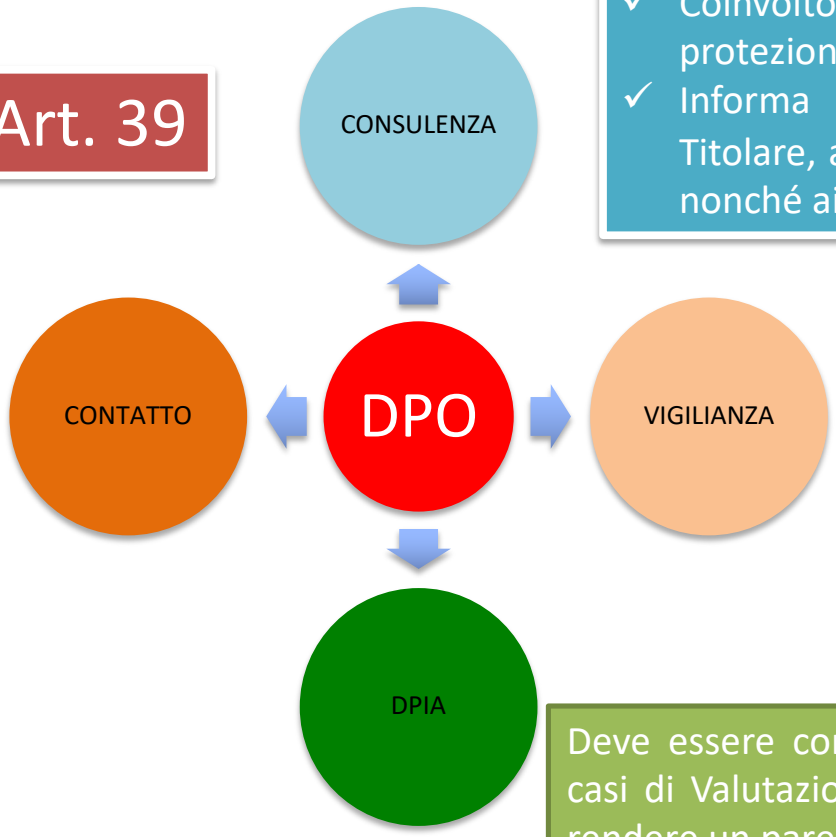
LA VALUTAZIONE DI IMPATTO PRIVACY
D.P.I.A.: Data Protection Impact Assessment

Espressione del principio dell'accountability o di responsabilizzazione è la Valutazione di impatto privacy finalizzata a dimostrare di aver predisposto misure tecniche e organizzative adeguate.


Gazzetta ufficiale L 119
dell'Unione europea
Legislazione

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

COMPITI - Art. 39



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

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

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

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

CONCLUDENDO . . .

I TRATTAMENTI DI DATI VANNO ELABORATI NEL RISPETTO DELLA NUOVA DISCIPLINA PRIVACY AL FINE DI GARANTIRE IL NECESSARIO BILANCIAMENTO TRA CONTRAPPOSTI INTERESSI, QUELLO DELLA SICUREZZA PUBBLICA E QUELLO DELLA RISERVATEZZA DELLE PERSONE.

Grazie
per l'attenzione!

Continua a seguirci su
www.secsolutionforum.it