LE GIORNATE
DI POLIZIA LOCALE
E SICUREZZA URBANA
CONVEGNO E MOSTRA ESPOSITIVA INTERNAZIONALE
DI TECNOLOGIE, SOLUZIONI E SERVIZI
RICCIONE

41ª EDIZIONE - 15-16-17 settembre 2022

IL CORRETTO TRATTAMENTO DEI DATI PERSONALI NELL'IMPIEGO DEI DISPOSITIVI MOBILI DI CATTURA DELLE IMMAGINI

GIUSEPPE ALVERONE

SESSIONE

BW1 - FOTOTRAPPOLE & PRIVACY. TRA CONTRASTO DEGLI ILLICETI AMBIENTALI E DATA PROTECTION. IL RUOLO DEGLI ACCERTATORI, DEI TECNICI E DEI DISPOSITIVI TECNOLOGICI ALLA LUCE DEL GDPR E DELLA DIRETTIVA POLIZIA

16/09/2022 – 11.00-13.00

IL CORRETTO TRATTAMENTO DEI DATI PERSONALI NELL'IMPIEGO DEI DISPOSITIVI MOBILI DI CATTURA DELLE IMMAGINI

di
Giuseppe Alverone – DPO dell'Arma dei Carabinieri

La complessità dell'ecosistema privacy. Il "framework normativo".

"NO SILVER BULLET" (non esiste il proiettile d'argento).

E', questo, il titolo di un famoso saggio con cui Fred Brooks, grande scienziato informatico americano, nel 1986 vinse il Turing Award, una sorta di premio oscar informatico.

In questo saggio, Brooks, per spiegare che non esiste una forma di sviluppo del software unica e risolutiva che potesse garantire guadagni doppi ogni 2 anni, faceva riferimento alla metafora del proiettile d'argento quale unica arma efficace e definitiva contro i lupi mannari, contro i mostri invincibili della tradizione sassone.

Questa metafora, che serve a spiegare come non esista una soluzione semplice per problemi complessi, si adatta molto bene anche alle difficoltà di gestire in modo corretto i trattamenti di dati personali eseguiti utilizzando i dispositivi mobili di cattura delle immagini, i.e. le cc.dd. fototrappole.

Infatti, per questo tipo di trattamenti non è possibile definire istruzioni generali, univoche ed efficaci, che possano garantire un utilizzo delle fototrappole che sia "compliant" (conforme) alla normativa privacy/data protection.

Ciò, soprattutto, in ragione della complessità dell'ecosistema della privacy/data protection che postula la necessità di un cambio di mentalità e di approccio da parte degli operatori delle Forze di Polizia nazionali e locali.

Tali operatori finora sono stati abituati a studiare e ad applicare il diritto con l'approccio mentale volto al formale adempimento delle norme giuridiche. Invero, si tratta di un paradigma a cui tutti gli studiosi del diritto sono stati abituati: si studiano le norme giuridiche individuando i relativi precetti e le relative sanzioni che vanno poi applicati ai casi concreti.

Orbene, un tale approccio, nell'ecosistema della privacy/data protection, non funziona affatto, poiché la normativa eurounitaria che regola questa materia, non contiene precetti ma pone invece un "framework normativo", i.e. un insieme di principi fondamentali e di requisiti che sono meramente stabiliti, senza alcuna indicazione su *come* debbano essere applicati o soddisfatti. Così, ogni Organizzazione, pubblica o privata, che determini finalità e mezzi dei trattamenti di dati personali, assume il ruolo privacy di "titolare del trattamento", e, come tale, è chiamata a scrivere le regole, al proprio interno, definendo le "politiche interne", le c.d. "policies", con il contestuale obbligo di essere sempre "accountable", i.e. in grado di dimostrare/comprovare il pieno rispetto dei citati principi che presidiano tutto il sistema della protezione dei dati.

Proposta di un metodo per la corretta gestione di un sistema di fototrappole

Quindi, in questo quadro così complesso e così nuovo per gli operatori di polizia non è possibile trovare il proiettile d'argento.

E' però possibile definire un metodo per la risoluzione in concreto dei problemi di gestione di questi sistemi.

Il metodo che propongo oggi è basato sul pieno rispetto del vincolo normativo e trova il suo baricentro nell'art. 2 decies del codice privacy novellato il quale stabilisce che *"i dati personali trattati in violazione della normativa privacy/data protection non possono essere utilizzati, salvo quanto previsto dall'articolo 160-bis"*.

L'art. 160 bis del codice della privacy - eccezione alla citata regola che pone il divieto di utilizzo dei dati - stabilisce che *"nel procedimento giudiziario (attenzione: non nel procedimento amministrativo) i.e. nel procedimento penale o civile, la validità, l'efficacia e l'utilizzabilità dei dati personali trattati*

in violazione della normativa privacy/data protection restano disciplinate dalle norme processuali di quegli ecosistemi".
Qual è la ricaduta pratica di questa norma? Gli operatori di polizia che basino una o più contestazioni di illecito amministrativo su dati personali raccolti tramite una gestione non corretta delle fototrappole, non solo espongono la loro amministrazione a pesanti sanzioni amministrative pecuniarie che potrebbero essere irrogate dal Garante della Privacy, ma - circostanza forse molto più dannosa - **con un effetto valanga** determinano il possibile annullamento delle centinaia e magari migliaia di procedimenti sanzionatori che abbiano attivato sulla base del citato trattamento illecito di dati personali.
Quindi, non è revocabile in dubbio che bisogna raccogliere e trattare dati personali in modo compliant cioè conforme alla normativa privacy

Il processo per disegnare un trattamento "compliant"
Ma come si fa ad essere sicuri che l'attività di trattamento è conforme?
Mettiamo un altro tassello.
L'art. 22, comma 1 del D.Lgs. 101/2018 che ha novellato il codice della privacy ed ha reso compatibili le norme privacy nazionali con quelle eurounitarie ha fissato un importantissimo principio:
"tutte le disposizioni dell'ordinamento nazionale in materia di privacy si interpretano e si applicano alla luce della disciplina dell'Unione europea".
Quindi ogni volta che un operatore di polizia è chiamato a progettare e regolare un'attività di trattamento di dati personali deve fare riferimento innanzitutto alla normativa Eurounitaria che è la normativa fondamentale nel senso che costituisce le fondamenta dell'intero sistema.
La prima cosa da fare è individuare qual è la finalità che si deve realizzare attraverso l'attività di trattamento dei dati.
Sulla base della finalità sarà possibile individuare il corpus normativo a cui bisogna fare riferimento.
Così. se dovrà essere compiuta un'attività di polizia, cioè se la finalità da realizzare è quella di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, allora dovrà essere applicata la Direttiva UE 2016/680 nota anche con l'acronimo LED (Law Enforcement Directive) che è stata recepita nel nostro Ordinamento con il D.Lgs. 51/2018.
Per tutte le altre finalità dovrà essere applicato il Regolamento UE 2016/679 noto con l'acronimo GDPR (General Data Protection Regulation).
Comunque, atteso che i principi del GDPR e della LED sono uguali, l'organizzazione del lavoro che viene di seguito descritto segue un unico paradigma. La sostanza è la stessa, cambiano solo i riferimenti normativi.
Dopo aver individuato il corpus normativo, occorre organizzare e progettare l'attività di trattamento in modo conforme alla normativa privacy. Sarà quindi necessario applicare il principio di privacy by design fissato dall'art. 25 del GDPR.
Secondo questo principio, il titolare del trattamento sia al momento di determinare i mezzi del trattamento (e.g. quando ad esempio decide di installare delle fototrappole) sia all'atto del trattamento stesso (e.g. quando implementa il sistema delle fototrappole) deve mettere in atto misure tecniche e organizzative adeguate cioè deve progettare il processo aziendale allineandolo ai principi di protezione dei dati.
Secondo questi principi - fissati dall'art. 5 del GDPR e dall'art. 3 del D.Lgs. 51/2018 – i dati personali devono essere:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»)
b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d. esatti e, se necessario, aggiornati («esattezza»);

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 («limitazione della conservazione»);
f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali («integrità e riservatezza»).

Questi sono i principi di protezione dei dati che costituiscono l'imprescindibile riferimento della compliance, della conformità.

ATTENZIONE: una qualsiasi attività di trattamento è quindi regolare, conforme, compliant solo se è pienamente rispettosa di tali principi, altrimenti, molto probabilmente, può costituire una violazione rilevante della privacy, sanzionabile.

La valutazione di impatto sulla protezione dei dati (c.d DPIA: Data Protection Impact Assessment)

Ma quanto descritto finora non basta. Gli adempimenti da porre in essere non sono finiti!

Per disegnare un corretto processo di gestione di un sistema di fototrappole occorre però un'ulteriore attività. Bisogna eseguire una valutazione di impatto sulla protezione dei dati la c.d DPIA (Data Protection Impact Assessment).

Infatti l'art. 35 del GDPR stabilisce che il titolare del trattamento, quando deve eseguire un trattamento che prevede l'uso di nuove tecnologie e che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, **prima di procedere al trattamento**, deve effettuare una valutazione di impatto.

Il comma 3 dello stesso art. 35 individua, in particolare, anche 3 categorie di trattamenti per i quali sussiste l'obbligo di eseguire una DPIA:

1. la profilazione,
2. il trattamento su larga scala di dati di particolare natura (i.e. quelli che una volta erano definiti dati sensibili) e
3. **la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.**

Quindi prima di avviare un processo di gestione di un sistema di fototrappole è necessario eseguire una DPIA.

Per svolgere correttamente una DPIA è necessario seguire pedissequamente le indicazioni fissate nell'allegato 2 delle Linee Guida dei Garanti Europei contrassegnate dalla sigla WP248 rev.01.

Questo allegato descrive 4 fasi di esecuzione della DPIA finalizzate rispettivamente a:

1. *descrivere sistematicamente il trattamento,*
2. *valutare la necessità e la proporzionalità del trattamento in relazione alle finalità.*
3. *gestire i rischi per i diritti e le libertà degli interessati;*
4. *coinvolgere il DPO ed eventualmente gli interessati.*

Simulazione dello sviluppo di una DPIA

Oggi, per dare un'idea di come bisogna procedere, simuleremo insieme lo sviluppo delle prime 2 parti di una DPIA relativa ad un processo di gestione di un sistema di fototrappole. Le restanti 2 parti, quelle relative alla gestione del rischio e al coinvolgimento del DPO hanno natura tecnica e necessitano di competenze specifiche.

Le prime 2 parti della DPIA sono comunque sufficienti a dare un'idea di come va applicato il principio di privacy by design a cui si è fatto cenno prima.

Allora, immaginiamo che un Comune voglia installare delle fototrappole nel territorio comunale.

In fase di design, di progettazione, i.e. già al momento della predisposizione del capitolato di appalto per l'acquisto del sistema, si dovrà stilare un documento in cui dovrà essere innanzitutto riportata una **descrizione sistematica del trattamento**.

Quindi bisognerà rispondere alle seguenti domande riportate nella prima parte dell'allegato 2 alle Linee Guida WP 248 rev.01:

1.Qual è la natura, l'ambito di applicazione, il contesto e la finalità del trattamento?

2. Quali sono le tipologie di dati personali trattati?

3. Chi sono i destinatari dei dati personali?
4. Qual è il periodo di conservazione dei dati raccolti e trattati?
5. Come si sviluppa il trattamento? (fornire una descrizione funzionale).
6. Quali sono gli «asset» utilizzati per il trattamento dei dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea)?
7. Esiste un codice di condotta approvato?
La seconda parte della DPIA è più complessa poiché prevede che debba essere **ben documentata la valutazione della necessità e della proporzionalità del trattamento in relazione alle finalità.**
In particolare si dovrà rispondere alle "key questions"(domande chiave) di seguito specificate.

Prima key question: Gli scopi del trattamento sono determinati, espliciti e legittimi ?
L'aggettivo "legittimi" riferito agli scopi impone di individuare le norme dell'Ordinamento Eurounitario o Nazionale che li preveda.
Quindi bisogna chiedersi: vi è una norma del diritto nazionale che in modo diretto o mediato attribuisce al Comune la legittimazione a perseguire questa finalità?
L'art. 198 del D.Lgs. 152/2006 «Norme in materia ambientale» rubricato «Competenze dei comuni», fissa la competenza dei comuni per la gestione dei rifiuti, stabilendo testualmente che *"i Comuni stabiliscono in particolare le misure per assicurare la tutela igienico-sanitaria in tutte le fasi della gestione dei rifiuti urbani".*
Inoltre, anche l'art. 6, comma 7 del D. L. n. 11/2009 convertito in Legge n. 38/2009, ci indica un altro possibile scopo, laddove sancisce che *"per la tutela della sicurezza urbana"*, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico. Inoltre l'art. 4 del D.L.14/2017 convertito in Legge 48/2017 chiarisce che "*si intende per sicurezza urbana il bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire anche attraverso interventi di riqualificazione, anche urbanistica, sociale e culturale, e recupero delle aree o dei siti degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio"*
Nel documento che riporta le attività poste in essere per sviluppare la DPIA andrà quindi esplicitata la finalità che oltre ad essere determinata è legittima perché prevista dalle norme richiamate.

Seconda key question: Quali sono le basi giuridiche che rendono lecito il trattamento?
I presupposti che rendono lecito un trattamento sono stabiliti dall'art. 6 del GDPR. Quello che qui interessa è indicato alla lettera e), ed è *l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, che, in base all'art. 6, par.3 del GDPR, deve essere indicato da una norma Eurounitaria o nazionale.
La norma nazionale che autorizza i Comuni ad eseguire attività di videosorveglianza, anche tramite fototrappole, è la stessa che pone la finalità cioè il citato art. 6 comma 7, laddove precisa che *i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico.*

Terza key question: i dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati?
Secondo il principio di minimizzazione dei dati, che include anche i principi di necessità e proporzionalità, bisogna verificare se, per realizzare questa finalità sia proprio necessario trattare dati personali dei cittadini in modo massivo tramite le fototrappole.
Al riguardo, il Provvedimento del Garante in materia di videosorveglianza dell'8 aprile 2010 [Doc. Web 1712680], tuttora valido, al punto 5.2. "Deposito dei rifiuti" prevede che "*in applicazione dei 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.3, l. 24 novembre 1981, n. 689).

ATTENZIONE: Questo è il punto centrale di tutto il design del trattamento. Bisogna argomentare bene e far comprendere che non è possibile far ricorso ad alternative meno impattanti, quali ad esempio servizi di appostamento del personale di polizia o sistemi di allarme nell'area.

Quarta key question: Qual è il periodo di conservazione dei dati ?

Con riguardo ai trattamenti di dati personali effettuati mediante sistemi di videosorveglianza, le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite. In particolare, "i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve a rilevare atti vandalici) – cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione".

Comunque per le finalità di cui stiamo parlando, sempre il D.L. 11/2009 offre un'indicazione chiara, laddove l'art.6, comma 8 stabilisce che "*la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza* ***è limitata ai sette giorni successivi alla rilevazione****, fatte salve speciali esigenze di ulteriore conservazione*."

Circa il prolungamento di tali tempistiche, questo è possibile in alcuni casi, ad esempio dietro richiesta dell'autorità giudiziaria o della polizia giudiziaria in relazione ad un'attività investigativa in corso.

Quinta key question: il trattamento che si sta progettando è corretto e trasparente?

Il punto 110 delle Linee Guida EDPB 3/2019 stabilisce che la normativa europea in materia di protezione dei dati dispone da tempo che gli interessati **debbano essere consapevoli** del fatto che è in funzione un sistema di videosorveglianza.

Dovrebbero cioè essere informati in modo dettagliato sui luoghi sorvegliati

Bisogna quindi verificare se sono state previste le informative cioè adeguata cartellonistica che renda consapevoli i cittadini di dove sono ubicate le fototrappole, e di tutte le informazioni relative al trattamento circa "chi", "come", "perché" e "per quanto tempo" tratta le immagini.

Il punto 111 delle citate Linee Guida prevede che, alla luce della quantità di informazioni da fornire all'interessato, i titolari del trattamento possono seguire un **approccio scalare**, optando per una combinazione di metodi al fine di assicurare la trasparenza (WP260, punto 35; WP89, punto 22).

Quindi il titolare del trattamento, anche in linea con le indicazioni del Garante (vds. provv. GPDP n. 214 del 9 giugno 2022 [doc. web n. 9794895]), deve:

- rendere l'informativa **"di primo livello",** mediante apposizione di **segnaletica di avvertimento** in prossimità della zona sottoposta a videosorveglianza con fototrappole;
- fornire anche "**informazioni di secondo livello"**, che devono "contenere tutti gli elementi obbligatori a norma dell'articolo 13 del GDPR ed essere facilmente accessibili per l'interessato.

In particolare, il **cartello di avvertimento**, come informazioni di **primo livello** dovrebbe contenere almeno:

1. le finalità del trattamento,
2. l'identità del titolare del trattamento
3. l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento"
4. le informazioni che potrebbero risultare inaspettate per l'interessato (e.g. la trasmissione di dati a terzi, in particolare se ubicati al di fuori dell'UE, e del periodo di conservazione). Se tali

informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale (senza alcuna registrazione di dati o trasmissione a soggetti terzi)

5. un chiaro riferimento al secondo livello di informazioni, un "rimando" (e.g. tramite un QR Code) al testo dell'informativa estesa sul sito istituzionale.

Il DPO, estrema risorsa per risolvere ogni problema privacy dell'Ente.

Qualunque problema o dubbio che emerga nel corso di tutte le attività istituzionali dell'Ente dovrebbe essere condiviso con il DPO che costituisce un imprescindibile punto di riferimento per tutti i dipendenti che trattano dati personali.

LE GIORNATE DI POLIZIA LOCALE E SICUREZZA URBANA

CONVEGNO E MOSTRA ESPOSITIVA INTERNAZIONALE
DI TECNOLOGIE, SOLUZIONI E SERVIZI

RICCIONE

Il corretto trattamento dei dati personali nell'impiego dei dispositivi mobili di cattura delle immagini

Giuseppe Alverone

ACCREDIA

acs UNI 11697:2017 Certified

Responsabile protezione dei dati

QR#VIOYHU#EXOOHW

(Fred Brooks)

Giuseppe Alverone

ACCREDIA

acs UNI 11697:2017 Certified

Responsabile protezione dei dati

D.Lgs.196/2003
Codice Privacy novellato

Art. 2-*decies (Inutilizzabilità dei dati)*

1. I dati personali trattati **in violazione** della disciplina rilevante in materia di trattamento dei dati personali **non possono essere utilizzati**, salvo quanto previsto dall'articolo 160-*bis*.

Art. 160-*bis* (*Validità, efficacia e utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento)*

1. La validità, l'efficacia e l'utilizzabilità **nel procedimento giudiziario** di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle **pertinenti disposizioni processuali**.

Giuseppe Alverone

acs UNI 11697:2017 Certified

Responsabile protezione dei dati

Art.22
D.Lgs. 101/2018

1. ***Il presente decreto e le disposizioni dell'ordinamento nazionale si interpretano e si applicano alla luce della disciplina dell'Unione europea in materia di protezione dei dati personali e assicurano la libera circolazione dei dati personali tra Stati membri ai sensi dell'articolo 1, paragrafo 3, del Regolamento (UE) 2016/679.***

Giuseppe Alverone

UNI 11697:2017
Certified

Responsabile protezione dei dati

SISTEMA NORMATIVO DATA PROTECTION

Finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali,

Dir. (UE) 2016/680
LED
(Law Enforcement Directive)

D.Lgs.51/20

Normativa nazionale

Altre finalità

Reg. (UE) 2016/679
GDPR
(General Data Protection Regulation)

Normativa nazionale

Giuseppe Alverone

UNI 11697:2017
Certified

Responsabile protezione dei dati

Articolo 25 GDPR

Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita

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, quali la pseudonimizzazione, volte ad **attuare in modo efficace i principi di protezione dei dati**, quali la minimizzazione, e a **integrare nel trattamento le necessarie garanzie** al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento**. Tale obbligo vale per la **quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità**. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Giuseppe Alverone
UNI 11697:2017 Certified
Responsabile protezione dei dati

Principi fondamentali
- art. 5 GDPR e art. 3 D.Lgs. 51/2018 -

I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ***(«liceità, correttezza e trasparenza»)***

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità ***(«limitazione della finalità»)***

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

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

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 ***(«limitazione della conservazione»)***

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali ***(«integrità e riservatezza»)***

Giuseppe Alverone

acs UNI 11697:2017 Certified

Responsabile protezione dei dati

Articolo 35 GDPR
Valutazione d'impatto sulla protezione dei dati

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**, 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.

2. …….

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.

Giuseppe Alverone
acs
UNI 11697:2017
Certified
Responsabile protezione dei dati

Allegato 2 alle *Linee Guida WP248 rev. 01* «criteri vincolanti»

Allegato 2 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- ☐ una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):
  - ☐ la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
  - ☐ vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
  - ☐ viene fornita una descrizione funzionale del trattamento;
  - ☐ sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
  - ☐ si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);
- ☐ la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):
  - ☐ sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
    - ☐ misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
      - ☐ finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
      - ☐ liceità del trattamento (articolo 6);
      - ☐ dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
      - ☐ limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
    - ☐ misure che contribuiscono ai diritti degli interessati:
      - ☐ informazioni fornite all'interessato (articoli 12, 13 e 14);
      - ☐ diritto di accesso e portabilità dei dati (articoli 15 e 20);
      - ☐ diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
      - ☐ diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
      - ☐ rapporti con i responsabili del trattamento (articolo 28);
      - ☐ garanzie riguardanti trattamenti internazionali (capo V);
      - ☐ consultazione preventiva (articolo 36).
- ☐ i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):
  - ☐ l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
    - ☐ si considerano le fonti di rischio (considerando 90);
    - ☐ sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
    - ☐ sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
    - ☐ sono stimate la probabilità e la gravità (considerando 90);
  - ☐ sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);
- ☐ le parti interessate sono coinvolte:
  - ☐ si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
  - ☐ si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).

Giuseppe Alverone

acs UNI 11697:2017 Certified

Responsabile protezione dei dati

DESCRIZIONE SISTEMATICA DEL TRATTAMENTO

(articolo 35, paragrafo 7, lettera a)):

1. Qual è la natura, l'ambito di applicazione, il contesto e la finalità del trattamento?
2. Quali sono le tipologie di dati personali trattati?
3. Chi sono i destinatari dei dati personali?
4. Qual è il periodo di conservazione dei dati raccolti e trattati?
5. Come si sviluppa il trattamento? *(fornire una descrizione funzionale).*
6. Quali sono gli «asset» utilizzati per il trattamento dei dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea)?
7. Esiste un codice di condotta approvato?

Giuseppe Alverone
acs UNI 11697:2017 Certified
Responsabile protezione dei dati

VALUTAZIONE DELLA NECESSITÀ E DELLA PROPORZIONALITÀ
(articolo 35, paragrafo 7, lettera b)

Sono state determinate le seguenti misure previste **per dimostrare la conformità**? (articolo 35, paragrafo 7, lettera d) e considerando 90):

- **misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base dei seguenti elementi di informazione**:
  - Gli scopi del trattamento sono determinati, espliciti e legittimi ? (articolo 5, paragrafo 1, lettera b) GDPR).
  - Quali sono le basi giuridiche che rendono lecito il trattamento ? (articolo 6 GDPR).
  - I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati - minimizzazione dei dati ? (articolo 5, paragrafo 1, lettera c) GDPR).
  - Qual è il periodo di conservazione dei dati ? (articolo 5, paragrafo 1, lettera e) GDPR).

Giuseppe Alverone
ACCREDIA
acs
UNI 11697:2017
Certified
Responsabile protezione dei dati

1. Gli scopi del trattamento sono determinati, espliciti e legittimi ? (articolo 5, paragrafo 1, lettera b) GDPR)

Art. 198 del D.Lgs. 152/2006 «*Norme in materia ambientale*» rubricato «Competenze dei comuni», fissa ***la competenza dei comuni per la gestione dei rifiuti*:**

«I Comuni stabiliscono in particolare le misure per assicurare la tutela igienico-sanitaria in tutte le fasi della gestione dei rifiuti urbani.

Art. 6, comma 7 del D. L. n. 11/2009 convertito in Legge n. 38/2009,

Per **la tutela della sicurezza urbana**, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico

Art. 4 del D.L.14/2017 convertito in Legge 48/2017

…si intende per **sicurezza urbana** il bene pubblico che afferisce alla **vivibilità e al decoro delle città**, da perseguire anche attraverso **interventi di riqualificazione, anche urbanistica**, sociale e culturale, e **recupero delle aree o dei siti degradati**, l'eliminazione dei fattori di marginalità e di esclusione sociale, **la prevenzione della criminalità, in particolare di tipo predatorio**….

Giuseppe Alverone
ACCREDIA
acsII UNI 11697:2017 Certified
Responsabile protezione dei dati

2. Quali sono le basi giuridiche che rendono lecito il trattamento ?(articolo 6 GDPR).

Articolo 6
Liceità del trattamento

a) **consenso**
b) **contratto**
c) **obbligo legale**
d) **salvaguardia di interessi vitali**
e) **esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri**
f) **legittimo interesse del titolare**

Art. 6, comma 7 del D. L. n. 11/2009 convertito in Legge n. 38/2009,
Per la tutela della sicurezza urbana, i comuni **possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico.**

Giuseppe Alverone
acs UNI 11697:2017 Certified
Responsabile protezione dei dati

3. I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati - minimizzazione dei dati ? (articolo 5, paragrafo 1, lettera c) GDPR)

Provvedimento GPDP in materia di videosorveglianza - 8 aprile 2010 [1712680]

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.3, l. 24 novembre 1981, n. 689).

Giuseppe Alverone
ACCREDIA
acs
UNI 11697:2017
Certified
Responsabile protezione dei dati

4. Qual è il periodo di conservazione dei dati ? (articolo 5, paragrafo 1, lettera e) GDPR).

Art. 6, comma 8 del D. L. n. 11/2009 convertito in Legge n. 38/2009

La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza **è limitata ai sette giorni successivi alla rilevazione**, fatte salve speciali esigenze di ulteriore conservazione.

Giuseppe Alverone
UNI 11697:2017 Certified
Responsabile protezione dei dati

5. Il trattamento che stiamo progettando è corretto e trasparente? (1)

Punto 110 delle Linee Guida EDPB 3/2019

La normativa europea in materia di protezione dei dati dispone da tempo che gli interessati **debbano essere consapevoli** del fatto che è in funzione un sistema di videosorveglianza. **Dovrebbero essere informati in modo dettagliato sui luoghi sorvegliati**

Giuseppe Alverone
UNI 11697:2017 Certified
Responsabile protezione dei dati

5. Il trattamento che stiamo progettando è corretto e trasparente? (2)

Il titolare del trattamento, in linea con le indicazioni del Garante **(vds. provv. GPDP n. 214 del 9 giugno 2022 [doc. web n. 9794895])**, deve:

- rendere l'informativa **"di primo livello"** mediante apposizione di **segnaletica di avvertimento** in prossimità della zona sottoposta a videosorveglianza con fototrappole;

- fornire anche **"informazioni di secondo livello"** che devono "contenere tutti gli elementi obbligatori a norma dell'articolo 13 del GDPR ed essere facilmente accessibili per l'interessato.

Giuseppe Alverone
UNI 11697:2017 Certified
Responsabile protezione dei dati

5. Il trattamento che stiamo progettando è corretto e trasparente? (3)

In particolare, il **cartello di avvertimento**, come informazioni di **primo livello** dovrebbe contenere almeno:

- **le finalità del trattamento;**
- **l'identità del titolare del trattamento;**
- **l'esistenza dei diritti dell'interessato,** unitamente alle informazioni sugli impatti più consistenti del trattamento;
- **le informazioni che potrebbero risultare inaspettate per l'interessato** (e.g. la trasmissione di dati a terzi, in particolare se ubicati al di fuori dell'UE, e del periodo di conservazione). Se tali informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale (senza alcuna registrazione di dati o trasmissione a soggetti terzi);
- **un chiaro riferimento al secondo livello di informazioni**, un "rimando" (e.g. tramite un QR Code) al testo dell'informativa estesa sul sito istituzionale.

Giuseppe Alverone

UNI 11697:2017 Certified

Responsabile protezione dei dati

….e per qualsiasi dubbio o problema

Giuseppe Alverone

acs UNI 11697:2017 Certified

Responsabile protezione dei dati

GRAZIE
PER L'ATTENZIONE

Giuseppe Alverone

UNI 11697:2017
Certified

Responsabile protezione dei dati