

PRIVACY E VIDESORVEGLIANZA NEGLI ENTI LOCALI

Dott. MARCO MASSAVELLI

Consulente ed Esperto Anci Risponde

DI CHE COSA PARLIAMO

- *La normativa di riferimento*
- *I soggetti della privacy nel Comune*
- *La videosorveglianza*

LE QUESTIONI DI MAGGIOR INTERESSE

Nel webinar si approfondiranno gli adempimenti a carico del Comune e in particolare del Comando di Polizia Locale relativi alla gestione privacy e degli impianti di videosorveglianza.

Verranno proposte soluzioni pratiche per la risoluzione delle diverse problematiche che potrebbe trasformarsi in controlli e sanzioni da parte del Garante Privacy.

NORMATIVA DI RIFERIMENTO

- ▶ **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)
- ▶ **DECRETO LEGISLATIVO 30 giugno 2003, n.196** recante il “Codice in materia di protezione dei dati personali” 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

Articolo 4 - Definizioni

Ai fini del presente regolamento s'intende per:

«**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;

Articolo 4 - Definizioni

- ▶ **«trattamento»:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

I SOGGETTI DELLA PRIVACY

IN RELAZIONE ALLE AMMINISTRAZIONI COMUNALI e ALLE POLIZIE LOCALI

Articolo 4 - Definizioni

► «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

COMUNE / SINDACO

I titolare del trattamento dei dati e i soggetti designati nella videosorveglianza comunale

Per quanto riguarda un sistema di videosorveglianza comunale, il titolare è il Comune (o, eventualmente, l'Unione di Comuni).

Nell'ambito di un'Amministrazione comunale, specie in strutture complesse, si delinea così la necessità di una **titolarità diffusa tra i vari soggetti che partecipano all'azione dell'Ente**: in tal senso è il vigente art. 2-quaterdecies del D.Lgs. 196/2003, a **individuare un nuovo soggetto, il designato al trattamento**.

Il comma 1 di tale disposizione consente infatti **l'attribuzione di specifici compiti e funzioni a soggetti incardinati nella struttura dell'organizzazione, espressamente designati dal titolare e sotto la sua diretta Autorità**.

È evidente che tali soggetti debbano essere individuati tra quelli che, per ruolo, esperienza e competenze, si rivelino figure di alto profilo in grado di fornire garanzia di rispetto della normativa in materia di privacy e sicurezza del trattamento.

I titolare del trattamento dei dati e i soggetti designati nella videosorveglianza comunale

Questa “delega” di funzioni tipiche del titolare, per quanto riguarda lo specifico ambito dei dati trattati per mezzo della videosorveglianza, **non può che ricadere sulla figura apicale del settore competente, ossia il Dirigente-Comandante o comunque il responsabile della Polizia locale che rivestirà così, in quota parte, il ruolo di titolare del trattamento.**

La titolarità del trattamento può però anche essere congiunta tra più soggetti che, condividendo finalità e procedure di trattamento, si accordano internamente al fine di stabilire le rispettive prerogative e amministrare unitariamente la gestione dei dati personali, pur mantenendo ciascuno le proprie attribuzioni.

I titolare del trattamento dei dati e i soggetti designati nella videosorveglianza comunale

Questa è ad esempio l'ipotesi di **contitolarità del trattamento che può essere perseguita nel caso di sistemi di videosorveglianza intercomunale o interforze**: da una parte il Comune, titolare del trattamento per finalità di sicurezza urbana, dall'altra il Ministero dell'interno o il Comando Generale dell'Arma dei Carabinieri per il perseguimento di finalità di pubblica sicurezza (attuate dalle Forze di polizia); il perseguimento di queste finalità pur partendo da presupposti differenti, in realtà convergono creando un'area di parziale sovrapposizione del trattamento.

Per questo motivo, oltre che espressamente previsto dall'art. 26 del Regolamento UE, è **quanto mai opportuno che esista un dettagliato accordo tra i soggetti che partecipano al trattamento in contitolarità, al fine di stabilire in modo univoco le prerogative di ciascuno senza che le sovrapposizioni nella gestione dei dati possano creare problematiche sia dal punto di vista operativo che da quello di tutela della privacy.**

Articolo 24

Responsabilità del titolare del trattamento

- ▶ Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento **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.** Dette misure sono riesaminate e aggiornate qualora necessario.

Articolo 25

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

► 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.

► 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.

Articolo 4 - Definizioni

▶ «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

IN COMUNE CHI E'?

Il responsabile esterno del trattamento dei dati nella videosorveglianza comunale

Quando il trattamento dei dati deve essere eseguito da un soggetto esterno all'Amministrazione titolare, la responsabilità formale di tale porzione di trattamento deve essere affidata a questo soggetto.

In materia di videosorveglianza può rendersi necessario nominare uno o più responsabili esterni del trattamento qualora vi siano soggetti – pubblici o privati – che svolgono attività di gestione dei dati personali raccolti dal titolare.

È questo ad esempio il caso di società partecipate o società private che intervengono a qualsiasi titolo nel corso del trattamento e che per tale motivo devono garantire il corretto e sicuro esercizio delle proprie funzioni a tutela della privacy

ALTRI SOGGETTI - ART. 4 GDPR

«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Articolo 29

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

► **CHI SONO IN COMUNE/POLIZIA LOCALE?**

Responsabile della protezione dei dati

Articolo 37

Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

- a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
- c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Articolo 35

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. Il titolare del trattamento, allorché svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

Articolo 35

Valutazione d'impatto sulla protezione dei dati

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.

4.L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

Articolo 35

Valutazione d'impatto sulla protezione dei dati

CONTENUTO

- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
- d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

VALUTAZIONE DI IMPATTO PER VIDEOSORVEGLIANZA

Provvedimento GARANTE 11 ottobre 2018

Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione di impatto:

- ▶ *Trattamenti automatizzati finalizzati ad assumere decisioni che producono effetti giuridici oppure tali da incidere in modo significativo sull'interessato*
- ▶ *Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati*

L'adozione della valutazione di impatto sulla protezione dei dati personali

Di particolare rilievo è la questione inerente la pubblicazione di informazioni concernenti la dislocazione e gli aspetti tecnici relativi agli impianti di videosorveglianza in uso o condivisi con le Forze di polizia, per finalità di controllo del territorio e tutela dell'ordine e della sicurezza pubblica.

Sul punto si è espresso il **TAR Lazio, sez. I, sentenza 1° agosto 2022, n. 10825**, censurando la divulgazione di informazioni di questo tipo “che, pur non costituendo segreto d'ufficio in senso proprio, per la loro particolare riservatezza”, in funzione delle finalità di prevenzione e repressione dei reati, **“costituiscono certo notizie che non possono essere rese di dominio pubblico”**.

Su questa scorta il giudice amministrativo individua tali informazioni tra quelle inaccessibili e quindi sottratte ad ogni tipo di ostensione a norma dell'**art. 3, comma 1, lett. d)**, del **D.M. 10 maggio 1994, n. 415** (atti e documenti concernenti l'organizzazione ed il funzionamento dei servizi di polizia) e, quindi, escluse anche dalle procedure di accesso civico e di accesso civico generalizzato, rispettivamente previste dagli artt. 5 e 5-bis del D.Lgs. 14 marzo 2013, n. 33

EDPB EUROPEAN DATA PROTECTION BOARD

Linee guida 3/2019

sul trattamento dei dati personali attraverso dispositivi video

AMBITO DI APPLICAZIONE

2.1 Dati personali

La sorveglianza sistematica e automatizzata di uno spazio specifico con mezzi ottici o audiovisivi, per lo più a scopo di protezione della proprietà, o per proteggere la vita e la salute delle persone, è divenuta un fenomeno significativo dei nostri giorni.

Questa attività comporta la raccolta e la conservazione di informazioni grafiche o audiovisive su tutte le persone che entrano nello spazio monitorato, identificabili in base al loro aspetto o ad altri elementi specifici.

L'identità di tali persone può essere stabilita sulla base delle informazioni così raccolte. Questo tipo di sorveglianza consente inoltre un ulteriore trattamento dei dati personali per quanto riguarda **la presenza e il comportamento delle persone nello spazio considerato.**

EDPB EUROPEAN DATA PROTECTION BOARD

Il rischio potenziale di un uso improprio di tali dati aumenta in rapporto alla dimensione dello spazio monitorato e al numero di persone che lo frequentano.

Ciò si riflette nel RGPD all'articolo 35, paragrafo 3, lettera c), che impone l'esecuzione di una valutazione d'impatto sulla protezione dei dati in caso di sorveglianza sistematica su vasta scala di un'area accessibile al pubblico, e all'articolo 37, paragrafo 1, lettera b), che impone ai responsabili del trattamento di designare un responsabile della protezione dei dati se la tipologia di trattamento, per sua natura, richiede il monitoraggio regolare e sistematico degli interessati.

Tuttavia, il regolamento non si applica al trattamento di dati che non hanno alcun riferimento a una persona, ad esempio se una persona non può essere identificata, direttamente o indirettamente.

Esempio Il RGPD non è applicabile alle fotocamere false (vale a dire qualsiasi fotocamera che non funziona come una fotocamera e quindi non elabora alcun dato personale).

Esempio Le registrazioni ad alta quota rientrano nell'ambito di applicazione del RGPD solo se, in queste circostanze, i dati trattati possono essere correlati a una determinata persona.

Esempio Una videocamera è integrata in un'automobile per fornire assistenza al parcheggio. Se la videocamera è costruita o regolata in modo tale da non raccogliere alcuna informazione relativa a una persona fisica (ad esempio targhe o informazioni che potrebbero identificare i passanti), il RGPD non è applicabile.

LICEITÀ DEL TRATTAMENTO

Prima di procedere, **si devono specificare dettagliatamente le finalità del trattamento (articolo 5, paragrafo 1, lettera b)).**

La videosorveglianza può servire a molti scopi, ad esempio a supporto della protezione della proprietà e di altri beni, della protezione della vita e dell'integrità fisica delle persone o a raccogliere elementi di prova in vista di procedimenti giudiziari civili.

Queste finalità del monitoraggio devono essere documentate per iscritto (articolo 5, paragrafo 2) e devono essere specificate per ogni telecamera di sorveglianza in uso. Le telecamere utilizzate per lo stesso scopo da un unico titolare del trattamento possono essere oggetto di una documentazione unitaria.

Inoltre, gli interessati devono essere informati delle finalità del trattamento ai sensi dell'articolo 13.

Ciò contrasta inoltre con il principio secondo il quale i dati personali vengono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato [cfr. articolo 5, paragrafo 1, lettera a)].

LICEITÀ DEL TRATTAMENTO

In linea di principio, ogni fondamento di diritto ai sensi dell'articolo 6, paragrafo 1, può fornire una base giuridica per il trattamento dei dati di videosorveglianza.

Ad esempio, l'articolo 6, paragrafo 1, lettera c), si applica quando la normativa nazionale prevede l'obbligo di mettere in atto in sistema di videosorveglianza.

Tuttavia, nella pratica, le disposizioni più suscettibili di essere utilizzate sono:

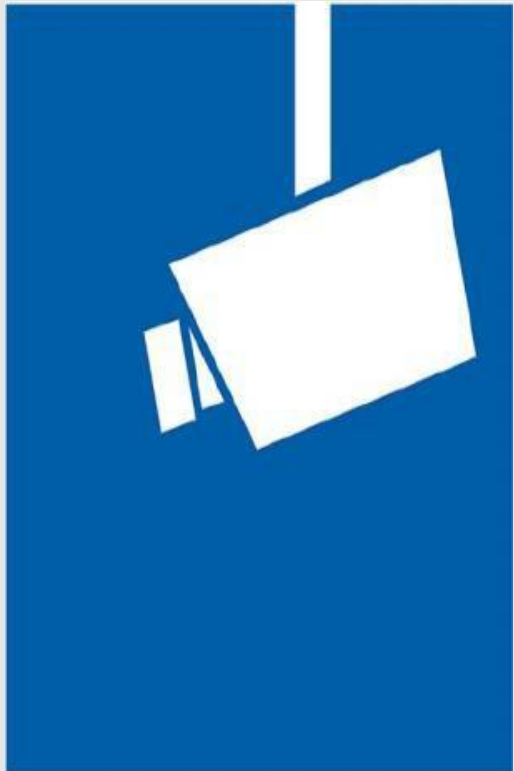
- ▶ Articolo 6, paragrafo 1, lettera f) (legittimo interesse)
- ▶ **Articolo 6, paragrafo 1, lettera e) (necessità al fine di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).**

In casi piuttosto eccezionali il titolare del trattamento potrebbe invocare l'articolo 6, paragrafo 1, lettera a) (consenso) come base giuridica .

OBBLIGHI DI TRASPARENZA E INFORMAZIONE

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.** A norma del RGPD gli obblighi generali di trasparenza e informazione sono sanciti dall'articolo 12 e seguenti del RGPD. Le «Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679 (WP260)» del gruppo di lavoro “Articolo 29”, approvate dal comitato europeo per la protezione dei dati il 25 maggio 2018, forniscono ulteriori dettagli. In linea con il punto 26 del WP260, è l'articolo 13 del RGPD che si applica se i dati personali sono raccolti «[...] presso l'interessato mediante osservazione (ad es. utilizzando dispositivi o software per catturare dati in modo automatizzato quali telecamere, [...])».

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, punto35; WP89, punto22). **Per quanto riguarda la videosorveglianza, le informazioni più importanti devono essere indicate sul segnale di avvertimento stesso (primo livello), mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).**



Video surveillance!

L'informativa completa sul trattamento dei dati è disponibile:

- presso i locali del titolare (reception, casse, ecc.)
- sul sito internet (URL)...
- altro

LA REGISTRAZIONE E' EFFETTUATA DA

CONTATTI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (se applicabile):

.....

FINALITÀ DELLA VIDEOSORVEGLIANZA

È POSSIBILE ACCEDERE AI PROPRI DATI ED ESERCITARE GLI ALTRI DIRITTI RICONOSCIUTI DALLA LEGGE RIVOLGENDOSI A



Per consultare la Banca dati di Anci Risponde

<https://ancirisponde.ancidigitale.it/>

Per richieste di informazioni sul Servizio Anci Risponde e/o sugli altri servizi:

- Tel. 06 83394257-2
- info@ancidigitale.it
- www.ancidigitale.it

Per informazioni sulle formule di abbonamento

- ✓ <https://www.ancidigitale.it/servizi/>



N° IT315348