



NULLI E DA SANZIONARE GLI ACCERTAMENTI AUDIOVISIVI DELLE AZIENDE DI RACCOLTA RIFIUTI

di Massimiliano Mancini (massimiliano.mancini@hotmail.it)^a

ABSTRACT: *Spesso le aziende di gestione dei servizi ambientali utilizzano telecamere e, addirittura, fototrappole nascoste, per rilevare il rispetto da parte dei cittadini delle disposizioni sul conferimento dei rifiuti urbani, senza nemmeno rispettare gli obblighi di informativa e di segnalazione dell'area videosorvegliata o di valutazione d'impatto-DPIA e, come se non bastasse, su questi comportamenti illegali si basa la successiva sanzione elevata dagli organi di polizia, aumentando la gravità della violazione e il numero di soggetti responsabili. Come qualificare il comportamento degli operatori e dei comandanti di polizia locale che, omettendo gravemente il loro dovere d'ufficio, invece di sanzionare chi gli presenta degli accertamenti illeciti li utilizza per sanzionare illegalmente i cittadini?*

KEYWORDS: #privacy #GDPR #valutazione d'impatto #dpi #pia #trattamento dati personali #DPO #Data Protection Officer #RPD #responsabile protezione dati #sanzioni amministrative #sanzioni illecite #omissione di atti d'ufficio #videosorveglianza #fototrappole #bodycam #Massimiliano Mancini #Esperti UPLI #UPLI #Unione Polizia Locale Italiana

INDICE

Premessa 1; L'applicazione del principio di liceità ai sistemi di videosorveglianza e fototrappole 2; La qualifica del personale delle aziende che svolgono servizi ecologici 3; La liceità del trattamento da parte delle aziende che svolgono servizi ecologici 4; L'obbligo della Valutazione d'impatto-DPIA per chi esegue videosorveglianza 5; Le conseguenze 5.

PREMESSA

La videosorveglianza è diventata quasi la wunderwaffen, ossia l'arma segreta, per risolvere tutti i problemi di sicurezza delle città e assicurare quindi i cittadini in ogni caso.

In nome della sicurezza quindi si sta assistendo a una ossessiva proliferazione di occhi elettronici che, in nome del nobile scopo della sicurezza si crede -molto erroneamente- che sia tutto lecito e quindi che il fine giustifichi ogni mezzo.

Ma non è così! Anzi spesso la reazione al crimine -e spesso molto più lievemente a fattispecie di illecito amministrativo- è essa stessa una grave illegalità!

Così accade spesso che gli enti che dovrebbero tutelare la legalità commettono più gravi illeciti dei cittadini che sanzionano in nome della legge alla quale essi si sentono -erroneamente e intollerabilmente- al di sopra.

^a Segretario Generale UPLI, criminologo, già comandante dirigente di Polizia Locale e Provinciale, DPO/RPD e consulente privacy in enti pubblici e aziende private esperto in DPIA.



Basta pensare, ad esempio, ai comuni che installano impianti di videosorveglianza oppure che posizionano fototrappole senza nemmeno la valutazione d'impatto sul trattamento dei dati, comportamento gravissimo che non solo rende illecito qualsiasi accertamento ma comporta anche una sanzione da 10.000.000 € (dieci milioni di euro)!

E poi ci sono addirittura operatori e comandanti di polizia locale che, omettendo il loro dovere di ufficio, invece di sanzionare chi gli consegna immagini e filmati acquisiti illegalmente, come accade quando le aziende di raccolta dei rifiuti urbani, municipalizzate o private appaltatrici del servizio, riprendono cittadini che smaltiscono irregolarmente rifiuti senza rispettare gli obblighi di legge (informative, segnalazione sistemi di ripresa, valutazione d'impatto-DPIA, ecc.), utilizzano tali immagini illecite per sanzionare i cittadini!

Ancora peggio, in altri casi i comandi di polizia locale sono conniventi verso la propria amministrazione comunale che ha installato fototrappole o sistemi di videosorveglianza senza eseguire la valutazione d'impatto-DPIA o senza nemmeno rendere corretta informativa e segnalazione del sistema o, addirittura, se ne rendono complici utilizzandoli essi stessi, omettendo di sanzionare e di inibire l'impianto abusivo, commettendo dei gravi reati penali per sanzionare - illecitamente - delle violazioni amministrative!

L'APPLICAZIONE DEL PRINCIPIO DI LICEITÀ AI SISTEMI DI VIDEOSORVEGLIANZA E FOTOTRAPPOLE

L'articolo 5 del Regolamento UE/2016/679 (GDPR)¹ stabilisce che i dati personali sono trattati in modo lecito corretto e trasparente nei confronti dell'interessato (principio di liceità, correttezza e trasparenza).

La videosorveglianza è lecita quando si verificano le condizioni espressamente previste dalla normativa e precisamente ricorre almeno una delle seguenti condizioni:

- sia esclusa l'applicazione della normativa sulla privacy di cui al Regolamento UE/2016/679-GDPR (GDPR art.1 c.2).
- vi è il consenso dell'interessato al trattamento dei propri dati personali per una o più specifiche finalità (GDPR art.6);
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (GDPR art.6).

Per quello che riguarda il primo punto, il Regolamento UE 2016/679 esclude dall'applicazione della normativa sulla privacy alcune finalità per le quali, di conseguenza, si può sempre, tra l'altro, svolgere audiovisive e utilizzarle senza rispettare particolari obblighi, i casi tuttavia sono specifici e tassativi:

¹ Reg. UE/2016/679 GDPR, art.5 (Principi applicabili al trattamento di dati personali) c.1 "1. 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 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»)».



- attività che non rientrano nell'ambito di applicazione del diritto dell'Unione e quindi l'attività di Interpol svolta al di fuori dell'Unione europea (GDPR art.1 c.2 cit. lettera b)²;
- accertamento e perseguimento di reati o esecuzione di sanzioni penali (GDPR art.1 c.2 cit. lettera d)³;
- la prevenzione e la repressione di minacce per l'ordine e la sicurezza pubblica (GDPR art.1 c.2 cit. lettera d)⁴.

Tutte queste attività devono essere svolte esclusivamente dalle forze di polizia, governative e locali, solo quindi esse sono illecite se svolte da altri soggetti, poiché richiedono particolari qualifiche e funzioni e specificatamente la qualifica di agente o ufficiale di pubblica sicurezza e di agente o ufficiale di polizia giudiziaria.

LA QUALIFICA DEL PERSONALE DELLE AZIENDE CHE SVOLGONO SERVIZI ECOLOGICI

L'art.358 c.p.⁵ definisce il "pubblico servizio" le attività disciplinate da norme imperative, come è disciplinata la raccolta di rifiuti solidi urbani, che assolvono una pubblica funzione, quale è la gestione dell'igiene pubblica, ma caratterizzata dalla mancanza di poteri autoritativi e certificativi propri dei pubblici ufficiali, con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale.

Di conseguenza, gli addetti alla raccolta dei rifiuti solidi urbani sono a ogni effetto di legge incaricati di pubblico servizio e ciò vale sia per i dipendenti pubblici, sia per i dipendenti delle municipalizzate e anche per quelli delle aziende private appaltatrici del servizio⁶.

Quindi non si può ritenere che le aziende che svolgono servizi ecologici possano essere escluse dall'applicazione integrale della normativa sulla privacy e in particolare su quanto prescritto in tema di videosorveglianza in ogni forma essa sia realizzata, incluse quindi le telecamere mobili e le fototrappole.

Tuttavia i dipendenti delle aziende ecologiche, potrebbero, in via episodica, rilevare con sistemi audiovisivi illeciti penali, derogando dal rispetto delle norme in materia di trattamento dei dati personali, in virtù proprio della qualifica di incaricati di pubblico servizio che gli impone l'obbligo di proporre denuncia direttamente o a mezzo della polizia giudiziaria (art.331 c.p.p.)⁷, ma ciò non

² Reg. UE 2016/679 art.1 (Oggetto e finalità) c.2: «Il presente regolamento non si applica ai trattamenti di dati personali: ...omissis... b) effettuati dagli Stati membri nell'esercizio di autorità che rientrano nell'ambito di applicazione del titolo V capo 2 TUE; ...omissis...»

³ Reg. UE 2016/679 art.1 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 ...omissis...»

Reg. UE 2016/679 art.1 c.2: «Il presente regolamento non si applica ai trattamenti di dati personali ...omissis... d) effettuati dalle autorità competenti a fini di ...omissis... salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.»

⁵ Codice Penale art.358 (Nozione della persona incaricata di un pubblico servizio) «1. Agli effetti della legge penale sono incaricati di un pubblico servizio coloro i quali a qualunque titolo prestano un pubblico servizio. 2. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale.»

⁶ Cfr. Cassazione Penale, sezione V, sentenza 3901 del 31/01/2001.

⁷ Codice Penale, art.331 (Denuncia da parte di pubblici ufficiali e incaricati di pubblico servizio): «1. Salvo quanto stabilito dall'articolo 347 i pubblici ufficiali e gli incaricati di un pubblico servizio che nell'esercizio o a causa delle loro funzioni o del loro servizio hanno M.Mancini-Nulli e da sanzionare gli accertamenti audiovisivi delle aziende di raccolta rifiuti.



legittima a preordinare mezzi e attività a tale fine -ad esempio installando fototrappole- poiché l'attività giurisdizionale penale non è preventiva ma scaturisce solo a seguito di notizia di reato.

LA LICEITÀ DEL TRATTAMENTO DA PARTE DELLA AZIENDE CHE SVOLGONO SERVIZI ECOLOGICI

Al di fuori dei casi di esclusione dell'applicazione della normativa sulla privacy l'acquisizione di immagini audiovisive è lecita solo quando vi sia una delle seguenti condizioni:

1. vi sia il consenso dell'interessato (GDPR art.6 c.1 p.a)⁸ espresso o implicito, informato e per le specifiche finalità;
2. si renda necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (GDPR art.6 c.1 p.a)⁹.

Il consenso dell'interessato deve essere dimostrato esplicitamente da chi tratta i dati (GDPR art.6 c.1 p.a)¹⁰ e quindi da chi ha eseguito le riprese audiovisive, ciò può avvenire in tutti i modi previsti dalla norma e quindi anche dimostrando di aver presegnalando l'area sottoposta alla videosorveglianza prima che vi si acceda.

Derogare al consenso preventivo dell'interessato è possibile solo nei casi espressamente previsti dalla legge, ad esempio nel caso di impianti di rilevamento da remoto delle sanzioni previsti dal Codice della Strada, ma la legge non lo consente per altri casi di violazioni amministrative e in particolare in tema ambientale.

Quindi sono illeciti, e di conseguenza nulli, e deve essere sanzionato il soggetto che ha eseguito il rilevamento con sistemi audiovisivi senza dare preventiva informativa agli interessati, anche con tabelle esposte prima dell'accesso all'area videosorvegliata purché conformi alle disposizioni delle Linee Guida del Comitato Europeo per la Protezione dei Dati (*European Data Protection Board – EDPB*) n.3/2019 sul trattamento dei dati personali attraverso dispositivi video.

In ogni caso la gestione degli impianti di videosorveglianza per il rilevamento degli illeciti amministrativi, per ogni finalità, è sempre soggetta alla normativa sulla privacy e in particolare a:

- a. Regolamento UE/2016/679-GDPR;
- b. Linee Guida del Comitato Europeo per la Protezione dei Dati (*European Data Protection Board – EDPB*) e in particolare la n.3/2019 sul trattamento dei dati personali attraverso dispositivi video del 29 gennaio 2020.

notizia di un reato perseguibile di ufficio devono farne denuncia per iscritto anche quando non sia individuata la persona alla quale il reato è attribuito.2. La denuncia è presentata o trasmessa senza ritardo al pubblico ministero o a un ufficiale di polizia giudiziaria.»

⁸ 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: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; ...omissis...”.

⁹ 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: ...omissis... c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.”.

¹⁰ Reg. UE/2016/679 GDPR, art.7 (Condizioni per il consenso) c.1 “1. Qualora il trattamento sia basato sul consenso il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.”.



L'OBBLIGO DELLA VALUTAZIONE D'IMPATTO-DPIA PER CHI ESEGUE VIDEOSORVEGLIANZA

La Valutazione d'impatto-DPIA è obbligatorio in tutti i casi generali previsti dall'articolo 35 comma 1 del Regolamento UE 2016/679 GDPR¹¹ e, in particolare, nei casi specifici indicati nel provvedimento del Garante per la Protezione dei Dati Personali 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 il 25 maggio 2018.

Questa procedura è espressamente e inderogabilmente prevista in tutti i casi in cui si esegua la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (art.35 c.3 p.c GDPR)¹² e deve essere eseguita prima di installare qualsiasi sistema di ripresa audiovisiva.

Evidentemente non si fa alcuna distinzione di obblighi tra le riprese eseguite da sistemi di videosorveglianza gestiti dagli enti pubblici, forze di polizia, uffici comunali, e quelli gestiti dalle società di diritto privato, come sono le municipalizzate e le società private appaltatrici del servizio di raccolta dei rifiuti solidi urbani.

Tuttavia, nel caso delle società private appare molto difficile che il Garante della Privacy possa ritenere accettabile la Valutazione d'impatto-DPIA, finalizzata all'accertamento delle violazioni amministrative in materia ambientale, da parte di un soggetto che ha ben altri scopi che non le funzioni di polizia amministrativa.

In ogni caso è illecito il rilevamento audiovisivo dei cittadini da parte delle società che esercitano i servizi ambientali se non abbiano la DPIA ed essa sia stata accettata dal Garante per la Privacy e che non abbiano avvisato con idonei pannelli l'area sottoposta alla videosorveglianza.

LE CONSEGUENZE

Laddove le forze di polizia -locali e nazionali- ricevano documentazione audiovisiva da parte delle aziende di gestione di servizi ambientali e raccolta dei rifiuti solidi urbani hanno, come organo di polizia, l'obbligo di verificare:

- a) che il soggetto che trasmette il dato sia autorizzato dal titolare del trattamento che ha eseguito la ripresa al fine di rendere lecita e legittima la comunicazione;
- b) che il titolare del trattamento dei dati abbia eseguito la valutazione d'impatto-DPIA nei modi di legge e che quindi sia stato ritenuto lecito il trattamento;
- c) che l'area sottoposta a videosorveglianza sia stata opportunamente segnalata ai cittadini.

Laddove non abbia certezza di questi elementi l'operatore di polizia dovrà:

¹¹ Reg. UE/2016/679 GDPR, art.35 c.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, ..."*.

¹² Reg. UE/2016/679 GDPR, art.35 c.3 *"La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: ...omissis... c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico."*.



- a) contestare al titolare del trattamento dei dati, fosse anche la stessa amministrazione dalla quale dipendono, la violazione dell'art.35 c.1 soggetto ai sensi dell'art.83 c.4 GDPR alla sanzione amministrativa sino a dieci milioni di euro e, nel caso di aziende private, sino al 2% del fatturato aziendale se superiore¹³;
- b) informare il Garante per la Protezione dei Dati Personali della violazione rilevata.

Cosa ne consegue laddove gli organi di polizia basassero su accertamenti illegittimi la sanzione elevata a carico del cittadino:

1. la nullità assoluta dell'atto elevato a carico del trasgressore, in quanto basato su violazione di legge;
2. la responsabilità in concorso per violazione della violazione dell'art.35 c.1 soggetto ai sensi dell'art.83 c.4 GDPR alla sanzione amministrativa sino a dieci milioni di euro;
3. ulteriori fattispecie omissive o dolose da valutare in sede penale.

PER ULTERIORI APPROFONDIMENTI SUL TEMA:

M.Mancini, Illegali gli impianti di videosorveglianza, fototrappole, body cam privi di valutazione d'impatto-DPIA, <https://www.unionepolizialeitaliana.it/sito/2021-01/>

M.Mancini, Come si esegue la valutazione d'impatto sul trattamento dei dati-DPIA, <https://www.unionepolizialeitaliana.it/sito/2021-02/>

¹³ Reg. UE/2016/679 GDPR, art.83 (Condizioni generali per infliggere sanzioni amministrative pecuniarie) c.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...".