VADEMECUM VIDEOSORVEGLIANZA PER COMUNI ED UNIONI DI COMUNI

Sommario

Hanno partecipato alla stesura del presente documento (in ordine alfabetico):

Sergio Duretti, Lepida S.c.p.a.

Annalisa Minghetti, Lepida S.c.p.a.

Guido Nobili, Regione Emilia-Romagna

Silvio Noce, avvocato

Kussai Shahin, al tempo Lepida S.c.p.a.

Alberto Sola, Regione Emilia-Romagna

Premessa

L'utilizzo diffuso dei sistemi di videosorveglianza costituisce indubbiamente un aspetto rilevante in termini di tutela della riservatezza e di compressione di tale diritto, oltre ad influire anche sul comportamento dei cittadini, come sottolineato nelle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video dell'EDPB[1].

L'opportunità di proporre un vademecum nasce dalle istanze, di numero cospicuo ed esponenziale nel corso degli ultimi due anni, degli Enti locali che, anche sulla scorta di un quadro normativo maggiormente incentivante, hanno manifestato l'esigenza di avvalersi delle nuove tecnologie di videosorveglianza e, conseguentemente, di disciplinare tale utilizzo.

1. Oggetto del vademecum

Il presente documento si propone di fornire elementi d'ausilio agli Enti locali che implementano sistemi di vds e che sono tenuti a disciplinarne l'utilizzo nei seguenti ambiti:

1) Videosorveglianza per finalità di sicurezza urbana (Appendice A);
2) Videosorveglianza per finalità di sorveglianza rifiuti (Appendice B);
3) Focus su utilizzo di microcamere indossabili e dash cam (Appendice C);
4) Focus su utilizzo di aereomobili a pilotaggio remoto (Appendice D)
5) Videosorveglianza per finalità di tutela del patrimonio o dei dipendenti/collaboratori e di protezione dei dati personali e dei sistemi informativi (Appendice E)
6) Videosorveglianza e operazioni di monitoraggio del traffico veicolare (Appendice F)

2. La normativa in materia di protezione dei dati personali

La gestione della videosorveglianza comporta trattamenti di dati personali e, per questo motivo, rientra nel campo di applicazione del Regolamento UE 2016/679 el 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)", (di seguito anche solo "GDPR") e del Codice per la protezione dei dati personali (D.lgs. 196/2003).

Il trattamento dei dati personali effettuato a mezzo dei sistemi di videosorveglianza da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, rientra nel perimetro di applicazione di cui al D.lgs. 51/2018 "*Attuazione della direttiva (UE) 2016/680 del Parlamento europeo*

[1] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it

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".

3. Principi generali di trattamento

3.1 Il principio di liceità

I trattamenti di dati personali effettuati dagli Enti locali a mezzo dei sistemi di videosorveglianza sono effettuati a norma dell'articolo 6, paragrafo 1, lettera e) del GDPR poichè il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Gli interessi pubblici e i pubblici poteri di cui alla succitata condizione di liceità sono declinate, ai sensi dell'art. 2ter del D.lgs. 196/2003, da norme di legge o di regolamento, se previsto da legge.
Come di seguito più ampiamente descritto, sussistono profili di attuazione dei compiti di sicurezza urbana di cui al D.L. n. 14/2017 (convertito in L. 18 aprile 2017, n. 48) che rientrano certamente nel perimetro di attuazione del D.lgs. 51/2018.
Con il presente vademecum sono proposti inquadramenti normativi che legittimano i trattamenti effettuati dagli Enti negli ambiti di cui al par. 1 del documento.

3.2 Principio di necessità

Il trattamento di dati personali tramite un sistema di videosorveglianza è lecito solo se effettivamente necessario (cfr. Articolo 5, lettera c) del GDPR), anche con riferimento al trattamento di conservazione dei dati (vedi successivo punto 4.3).

I sistemi di videosorveglianza possono essere impiegati esclusivamente quando siano state giudicate insufficienti o inattuabili differenti misure alternative. In particolare, se i sistemi di videosorveglianza sono utilizzati per finalità di protezione dei beni, devono risultare inefficaci misure quali controlli da parte di personale addetto, sistemi di allarme, misure di protezione e controllo degli accessi.

I sistemi di videosorveglianza sono installati, configurati e programmati in modo da escludere ogni uso superfluo o ridondante di immagini e dati personali.

3.3 Principio di proporzionalità

Il trattamento di dati personali tramite un sistema di videosorveglianza è lecito solo se è rispettato il principio di proporzionalità (cfr. Articolo 5 lettera b) GDPR).

Le modalità di effettuazione del trattamento di dati tramite sistemi di videosorveglianza, così come le caratteristiche tecniche dei sistemi stessi, devono essere proporzionali agli scopi prefissati e valutate in funzione di ogni singola situazione concreta, come previsto dall'articolo 5, lettera c) del GDPR, prevedendo il principio di "minimizzazione dei dati".

3.4 Principio di finalità

Il trattamento di dati personali tramite un sistema di videosorveglianza è lecito solo se soddisfa il principio di limitazione delle finalità (cfr. Articolo 5 lettere a) e b) GDPR), ossia i dati sono trattati per scopi determinati, espliciti e legittimi.

In ciascuna delle Appendice del presente documento sono distintamente descritti gli scopi perseguiti dagli Enti locali a mezzo dei sistemi di videosorveglianza.

4. Le Misure di sicurezza

I trattamenti di dati personali effettuati a mezzo dei sistemi di videosorveglianza, in ragione dell'elevato livello di criticità correlato, richiedono l'implementazione di misure di sicurezza, tecnico-organizzative, atte a ridurre al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme.
E' pur vero che il GDPR impone tale valutazione a ciascun Ente, tuttavia, ai fini del presente documento, non può non essere valorizzata la produzione di linee guida da parte di AGID in materia di sicurezza informatica, cui gli Enti destinatari del presente documento sono tenuti a conformarsi.
Pertanto, pur ribadendo la persistenza in capo agli Enti dell'obbligo di effettuare un'analisi puntuale dei rischi specifici connessi ai trattamenti di dati personali oggetto del presente documento, sono proposti alcuni paradigmi di riferimento cui commisurare l'adeguatezza delle misure.

4.1 Il processo di procurement ICT

La fase di approvvigionamento di beni e servizi informatici degli Enti deve garantire la rispondenza di questi ad adeguati livelli di sicurezza. Si rappresenta, infatti, che i fornitori possono accedere, disporre e concorrere a produrre il patrimonio informativo delle pubbliche amministrazioni committenti, introducendo potenziali rischi informatici, con impatto in particolare su riservatezza, integrità, disponibilità.

Il processo di procurement di servizi ICT, qualora non contempli elementi di conformità ad un quadro di sicurezza informatica, può rendere vani o meno efficaci le misure già implementate dagli Enti a tutela del proprio patrimonio informativo.

In materia si segnala che costituiscono paradigma di riferimento le Linee Guida per la sicurezza nel procurement ICT[2]. Tra le molteplici istruzioni ivi contemplate sussistono, altresì, requisiti di sicurezza che le amministrazioni possono inserire nei propri capitolati di gara (nell'Allegato 1 è riportata per agevolarne la lettura l'Appendice A delle suddette linee guida) .

[2] https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_0_122261_725_1.html

4.2 La sicurezza del software utilizzato

AGID ha emanato le Linee guida per lo sviluppo del software sicuro[3] che costituiscono un framework cui è necessario conformare sia le azioni di sviluppo software, sia il software esistente o in fase di acquisto.

In tale ultimo caso, il Fornitore dovrebbe essere tenuto a presentare le evidenze di test di sicurezza effettuati sulla scorta degli standard internazionalmente riconosciuti, come citati nelle suindicate Linee guida.

4.3 Le misure organizzative

4.3.1 Ruoli e responsabilità

In seno all'Ente deve essere individuata la Struttura competente in materia di videosorveglianza, con riferimento alle diverse finalità di trattamento perseguibili. Al Dirigente di tale Struttura l'Ente dovrebbe demandare l'attuazione degli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dall'Ente a mezzo dei sistemi di videosorveglianza.

4.3.2 Autorizzazioni e profili coerenti

Il trattamento di dati personali mediante l'impiego di sistemi di videosorveglianza è consentito esclusivamente ai soggetti preventivamente autorizzati al trattamento. Si segnala che l'autorizzazione al trattamento deve avvenire per iscritto e deve essere circoscritta ad un numero limitato di persone. I profili di accesso al sistema di videosorveglianza devono essere configurati in funzione delle autorizzazioni ad una o più specifiche operazioni di trattamento previste.

I soggetti fornitori dei servizi correlati alla videosorveglianza sono nominati responsabili del trattamento ai sensi e per gli effetti di cui all'art. 28 del GDPR e in tutti i casi di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele, ad esempio, consentendo l'accesso alle immagini solo qualora sia indispensabile.

4.3.3 Tempi di conservazione delle immagini

Una delle novità più rilevanti della normativa in materia di protezione dei dati personali è certamente costituita dall'introduzione del principio di accountability.

In particolare il GDPR recepisce tale principio all'art. 24 il quale prevede che tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità 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 dei dati personali è effettuato conformemente al Regolamento. Dette misure devono essere riesaminate e aggiornate qualora necessario. Inoltre, se ciò è proporzionato rispetto alle attività di

[3] https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro

trattamento, le predette misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

Tale regime comporta un approccio profondamente differente rispetto al previgente assetto del Codice per la protezione dei dati personali, in cui cardini fondamentali dell'assetto normativo erano costituiti dagli interventi autorizzativi dell'Autorità. Gli effetti di tale mutata prospettiva si propagano anche sui Provvedimenti generali emessi dal Garante per la protezione dei dati personali, ivi compreso il Provvedimento in materia di videosorveglianza dell'8 aprile 2010. In tale Provvedimento, erano sottoposti ad autorizzazione preventiva i tempi di conservazione delle immagini superiori alle 24 ore. Il principio di accountability impone all'Ente che intende installare il sistema di videosorveglianza di valutare l'adeguatezza (valutazione che s'intende ex ante) delle misure da implementare, ivi compresa la rispondenza dei tempi di conservazione delle immagini alle finalità perseguite.

Pertanto, il tempo di conservazione deve essere valutato e stabilito in ragione dell'esaudimento delle finalità perseguite. In ordine alle finalità descritte nel presente documento si ritiene certamente congruo un tempo di conservazione delle immagini non superiore a sette giorni.

4.4 DPIA

L'articolo 35 del Regolamento UE 2016/679 richiede al Titolare del trattamento di effettuare, prima di procedere ad un trattamento che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, una valutazione dell'impatto dei trattamenti previsti.

Il Garante con delibera del 11 ottobre 2018 "Elenco delle tipologie di trattamenti soggetti a requisito di valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679"[4] ha ritenuto che (punto 5 dell'allegato) il "*trattamento della videosorveglianza nell'ambito del rapporto di lavoro*" costituisce trattamento per i quali è richiesta la valutazione d'impatto.

Per tutti i trattamenti di videosorveglianza di cui al par. 1 è richiesta la valutazione d'impatto.

[4] doc. web. n. 9058979

Allegato 1 - Requisiti di sicurezza eleggibili

REQUISITI GENERALI (INDIPENDENTI DALLA TIPOLOGIA DI FORNITURA)

R1	Il fornitore deve adottare al proprio interno le procedure e politiche di sicurezza definite dall'amministrazione committente, con particolare riferimento alle modalità di accesso ai sistemi dell'amministrazione, all'hardening (esempio installazione di soluzioni di end point security) dei dispositivi utilizzati dal fornitore, alla gestione dei dati dell'amministrazione.
R2	Il fornitore deve possedere la certificazione ISO/IEC 27001 e mantenerla per tutta la durata della fornitura.
R3	(alternativo al precedente) Anche se il fornitore non è certificato ISO/IEC 27001, almeno deve usare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) aggiornato nel tempo e/o predisporre un piano di qualità secondo lo standard ISO 10005
R4	Il fornitore deve far eseguire annualmente un audit sul proprio sistema di sicurezza, a proprie spese e da una società specializzata scelta previa approvazione della stazione appaltante. NB: Qualora applicabile, tale attività si incrocia con il requisito R2 (le verifiche dell'Ente Certificatore hanno cadenza pressoché annuale).
R5	L'amministrazione può, con un preavviso di 20 giorni solari, richiedere ulteriori attività di auditing secondo modalità concordate con il fornitore. Le risultanze di tali audit verranno comunicate all'amministrazione.
R6	L'amministrazione, direttamente o tramite terzi incaricati, può eseguire verifiche relative alla conformità della prestazione dei servizi rispetto a quanto stabilito nel capitolato tecnico oltre che nell'offerta tecnica se migliorativa.
R7	Il personale del fornitore che presta supporto operativo nell'ambito dei servizi di sicurezza dovrà possedere certificazione su specifici aspetti della sicurezza.
R8	Il fornitore deve disporre di una struttura per la prevenzione e gestione degli incidenti informatici con il compito d'interfacciarsi con le analoghe strutture dell'amministrazione e con le strutture centrali a livello governativo.
R9	Il fornitore deve dotarsi delle misure minime di sicurezza per limitare il rischio di attacchi informatici (riferimento DR-5)
R10	Il SOC del fornitore deve sovrintendere alla gestione operativa e continuativa degli incidenti informatici sui servizi erogati nell'ambito della fornitura.
R11	Il fornitore deve garantire il rispetto di quanto richiesto dalla normativa vigente in materia di sicurezza cibernetica, anche in riferimento ai contenuti del GDPR, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte e dei costi di attuazione nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, e adottando procedure tecniche e organizzative volte alla gestione di eventuali violazioni di dati personali
R12	Sulle reti messe a disposizione dal fornitore devono essere presenti di dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise).
R13	Il fornitore deve usare protocolli cifrati e meccanismi di autenticazione nell'ambito dei servizi erogati.
R14	Qualora il fornitore subisca un attacco, in conseguenza del quale vengano compromessi sistemi del committente da lui gestiti, deve farsi carico delle bonifiche del caso, e riportare i sistemi in uno stato di assenza di vulnerabilità.
R15	Il fornitore si impegna a trattare, trasferire e conservare le eventuali repliche dei dati oggetto di fornitura, ove autorizzate dalle amministrazioni, sempre all'interno del territorio dell'UE.
R16	Il fornitore deve dare disponibilità a far parte di un Comitato di Direzione Tecnica, eventualmente aperto anche a soggetti terzi, che tratti il tema della sicurezza, sia nell'ottica di favorire la risoluzione di temi aperti sia per introdurre eventuali varianti al contratto per fronteggiare nuove minacce o altro.
R17	Il fornitore deve condividere le informazioni necessarie al fine di garantire il corretto monitoraggio della qualità e della sicurezza, eventualmente pubblicando le stesse nel portale della fornitura.
R18	Il fornitore si impegna a sottoscrivere una clausola di non divulgazione (NDA) sui dati e sulle informazioni dell'amministrazione.
R19	Le soluzioni e i servizi di sicurezza proposti dal fornitore devono essere aggiornati dal punto di vista tecnologico, con riferimento all'evoluzione degli standard e del mercato; devono essere conformi alle normative e agli standard di riferimento applicabili; devono venire adeguati nel corso del contratto, senza oneri aggiuntivi, alle normative che l'UE o l'Italia rilasceranno in merito a servizi analoghi.

REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI SVILUPPO APPLICATIVO

R20	Il fornitore deve attenersi alla politica di sicurezza dell'amministrazione committente, con particolare riferimento all'accesso ai dati dell'amministrazione, che avverrà esclusivamente sui sistemi di sviluppo e test.

R21	In fase di analisi, il fornitore deve definire le specifiche di sicurezza (non funzionali) a partire dai requisiti espressi dall'amministrazione.
R22	In fase di progettazione codifica, il fornitore deve implementare le specifiche di sicurezza nel codice e nella struttura della basedati.
R23	Al termine del progetto, il fornitore deve rilasciare tutta la documentazione necessaria all'amministrazione per gestire correttamente quanto rilasciato anche sotto l'aspetto della sicurezza.

REQUISITI SPECIFICI PER FORNITURE DI OGGETTI CONNESSI IN RETE

R24	Supporto di protocolli sicuri e cifrati (HTTPS, SSH v2, ecc.).
R25	Filtraggio di indirizzi IP.
R26	Supporto di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.).
R27	Gestione di più profili con privilegi diversi.
R28	Funzionalità di "richiesta creazione o cambio della password al primo accesso".
R29	Blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso.
R30	Gli accessi degli utenti devono essere registrati su un archivio (log) non cancellabile con il reset.
R31	Gestione dei log di sistema (accessi, allarmi, ecc.).
R32	Il fornitore (anche in collaborazione con il produttore della tecnologia) deve offrire processi, unità organizzative e strumenti dedicati alla gestione di vulnerabilità scoperte sui prodotti oggetto della fornitura.
R33	Per gli apparati proposti deve essere disponibile documentazione tecnica (schede tecniche, manuali, guide operative) relativa alla corretta configurazione e gestione degli aspetti di sicurezza.

REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI GESTIONE REMOTA

R34	I meccanismi di autenticazione devono essere basati su meccanismi di crittografia asimmetrica, a chiave pubblica; la lunghezza delle chiavi va impostata sulla base della criticità della comunicazione da cifrare (ad esempio 256 bit per le meno critiche, 512 bit per le più critiche). La gestione e distribuzione delle chiavi e dei certificati è a carico del fornitore.
R35	Autorizzazione: sulla base delle credenziali fornite dall'utente, si devono individuare i diritti e le autorizzazioni che l'utente possiede e permetterne l'accesso alle risorse limitatamente a tali autorizzazioni.
R36	Confidenzialità nella trasmissione dei dati: le comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell'amministrazione devono essere cifrate.
R37	Fornire meccanismi che permettano di garantire l'integrità di quanto trasmesso (ad esempio meccanismi di hashing).
R38	Il fornitore deve descrivere nel dettaglio le soluzioni tecniche utilizzate (dispositivi hardware e software impiegato, modalità operative, politiche di sicurezza, …) per soddisfare i requisiti di sicurezza dell'amministrazione committente.
R39	In fase di attivazione del servizio, il fornitore deve concordare con l'amministrazione le modalità operative e le politiche di sicurezza, i livelli di gravità degli incidenti, le attività e le contromisure che dovranno essere svolte per contrastare le minacce.
R40	Il fornitore dovrà attenersi alle politiche di sicurezza definite dalla committente, con particolare riferimento alla definizione di ruoli e utenze per l'accesso ai sistemi gestiti.
R41	In caso di necessità, da parte degli operatori, di accesso a Internet, il fornitore deve utilizzare un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dall'amministrazione.
R42	In caso di rilevazione di un incidente di gravità elevata (con scala da definire a inizio fornitura), il fornitore deve dare immediata notifica, tramite canali concordati con l'amministrazione, dell'incidente rilevato e delle azioni da intraprendere, al Responsabile della Sicurezza indicato dall'amministrazione e agli organismi individuati dal legislatore a presidio della sicurezza cibernetica.
R43	Per ogni incidente di sicurezza, il fornitore s'impegna a consegnare all'amministrazione, entro il giorno successivo, un report che descriva la tipologia di attacco subito, le vulnerabilità sfruttate, la sequenza temporale degli eventi e le contromisure adottate.
R44	Su richiesta dell'amministrazione, il fornitore deve consegnare i log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT. Tali log dovranno essere inviati all'amministrazione entro il giorno successivo a quello in cui è avvenuta la richiesta.
R45	Il fornitore deve monitorare la pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite. Entro il giorno successivo al rilascio dell'upgrade/patch/hotfix, il fornitore deve avviare una valutazione, da rilasciarsi entro un numero giorni da stabilirsi, propedeutica all'installazione delle stesse sui dispositivi di sicurezza, che ad esempio identifichi la possibilità di applicare la patch immediatamente, o la necessità di apportare MEV o integrazioni prima di procedere alle installazioni.

APPENDICE A

VIDEOSORVEGLIANZA PER FINALITA' DI SICUREZZA URBANA

1. Inquadramento normativo

Il D.L. 20 febbraio 2017, n. 14, convertito in L. 18 aprile 2017, n. 48, ha definito come sicurezza urbana come "*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, la promozione della cultura del rispetto della legalità e l'affermazione di più elevati livelli di coesione sociale e convivenza civile*".

Tale norma assume particolare importanza in quanto introduce in norma di rango primario sia la nozione di sicurezza urbana che quella di sicurezza integrata, portando a compimento un percorso di normazione che ha avuto origine già negli anni Novanta del secolo scorso. La sicurezza integrata è "*la sicurezza per il benessere delle comunità territoriali*", perseguita in maniera sinergica da tutti gli attori istituzionali e dai vari livelli amministrativi. Ciò costituisce manifesta attuazione del terzo comma dell'articolo 118 della Costituzione (come modificato dalla riforma del 2001), che aveva prefigurato un coordinamento tra Stato e Regioni in materia di sicurezza pubblica. Una seconda importante novità contenuta nel decreto-legge è rappresentata dalla definizione di sicurezza urbana, in precedenza introdotta con il decreto ministeriale dell'agosto 2008, che definiva gli ambiti di intervento del potere di ordinanza dei sindaci.

Il Decreto-legge 14 del 2017 riprende quella nozione e la amplia, sottolineando quegli aspetti che vanno oltre il tradizionale recinto dell'ordine pubblico e della sicurezza pubblica, affermando espressamente che la sicurezza urbana riguarda "*il bene pubblico che afferisce alla vivibilità e al decoro della città*". Mette al centro della definizione la qualità della vita delle città e gli interventi che contribuiscono a migliorarla: la riqualificazione urbanistica delle aree degradate, l'inclusione sociale, il superamento delle marginalità sociali, la promozione della cultura della legalità e la prevenzione della criminalità di tipo predatorio. In questo quadro, i Comuni sono chiamati a svolgere un ruolo fondamentale nell'ambito della prevenzione situazionale e sociale, fornendo qualificati servizi pubblici, in grado di migliorare la qualità della vita.

Il legislatore ha, pertanto, legato indissolubilmente le azioni di sicurezza urbana al diritto dei cittadini al pieno godimento dei centri urbani, all'inclusione sociale e alla riqualificazione urbana. Tale stretta connessione costituisce anche il perimetro delle azioni esperibili dai sindaci e dagli enti locali ed elemento di distinzione dalle attività di pubblica sicurezza svolta dalle autorità di pubblica sicurezza.

Per quel che concerne l'istituto della "sicurezza pubblica" giova riportare un oramai risalente arresto della Corte Costituzionale, sentenza n. 77/1987, che ha definito la

"sicurezza pubblica" come la "*funzione inerente alla prevenzione dei reati o al mantenimento dell'ordine pubblico*".

La stessa Corte, con la sentenza n. 218/1988, produceva una distinzione efficace tra la "polizia amministrativa" e la "pubblica sicurezza" definendo rispettivamente la prima come quelle "*attività di prevenzione o di repressione dirette a evitare danni o pregiudizi che possono essere arrecati alle persone o alle cose nello svolgimento di attività ricomprese nelle materie sulle quali si esercitano le competenze regionali, senza che ne risultino lesi o messi in pericolo i beni o gli interessi tutelati in nome dell'ordine pubblico*" e la seconda come l'insieme delle "*misure preventive e repressive dirette al mantenimento dell'ordine pubblico*". Definizioni i cui effetti sono evidenti negli interventi normativi degli anni a venire (cfr. l'art. 159 del d.lgs. 1112/1998).

In particolare, «[l]a funzione di polizia di sicurezza […] riguarda […] le misure preventive e repressive dirette al mantenimento dell'ordine pubblico e, pertanto, si riferisce alla attività di polizia giudiziaria e a quella di pubblica sicurezza; la funzione di polizia amministrativa riguarda, diversamente, l'attività di prevenzione e repressione diretta ad evitare danni o pregiudizi a persone o cose nello svolgimento di attività rientranti nelle materie affidate alla competenza regionale» (sentenza n. 290 del 2001).

La definizione di ordine pubblico e sicurezza «nulla aggiunge alla tradizionale nozione […]», che «riserva allo Stato […] le funzioni primariamente dirette a tutelare beni fondamentali, quali l'integrità fisica o psichica delle persone, la sicurezza dei possessi ed ogni altro bene che assume primaria importanza per l'esistenza stessa dell'ordinamento».

Non qualsiasi interesse pubblico alla cui cura siano preposte le pubbliche amministrazioni, dunque, «ma soltanto quegli interessi essenziali al mantenimento di una ordinata convivenza civile».

Siffatta precisazione «è necessaria ad impedire che una smisurata dilatazione della nozione di sicurezza e ordine pubblico si converta in una preminente competenza statale in relazione a tutte le attività che vanificherebbe ogni ripartizione di compiti tra autorità statali di polizia e autonomie locali» (sentenza n. 290 del 2001).

In seguito alla riforma del Titolo V la Corte ha ripreso il solco interpretativo già tracciato osservando come fossero assegnate allo Stato le funzioni dirette a prevenire e a reprimere reati, in vista della tutela di «*interessi fondamentali, quali l'integrità fisica e psichica delle persone, o la sicurezza dei beni*» (da ultimo, tra le tante, sentenza n. 116 del 2019 e, nello stesso senso, sentenza n. 208 del 2018), tutti ricompresi nella «*ordinata e civile convivenza nella comunità nazionale*» (sentenza n. 148 del 2018).

La delimitazione dell'ambito materiale di competenze tra le autorità di pubblica sicurezza e la polizia locale viene definito, in aderenza alla sentenza n. 290/2001, rappresentando che gli «"*interessi pubblici primari" che vengono in rilievo ai fini considerati sono […] unicamente gli interessi essenziali al mantenimento di una ordinata convivenza civile:*

risultando evidente come, diversamente opinando, si produrrebbe una smisurata dilatazione della nozione di sicurezza e ordine pubblico, tale da porre in crisi la stessa ripartizione costituzionale delle competenze legislative, con l'affermazione di una preminente competenza statale potenzialmente riferibile a ogni tipo di attività» (sentenza n. 300 del 2011). La potestà legislativa regionale può essere esercitata non solo per disciplinare generici interessi pubblici, come pure affermato nella sentenza n. 290 del 2001, ma anche per garantire beni giuridici fondamentali tramite attività diverse dalla prevenzione e repressione dei reati (sentenza n. 300 del 2011).

Nella sentenza n. 285/2019 la Corte Costituzionale osserva che "*La sicurezza può ben assumere una possibile declinazione pluralista, coerente con la valorizzazione del principio autonomistico di cui all'art. 5 della Costituzione: ad una sicurezza in «senso stretto» (o sicurezza primaria) può essere affiancata, infatti, una sicurezza «in senso lato» (o sicurezza secondaria), capace di ricomprendere un fascio di funzioni intrecciate, corrispondenti a plurime e diversificate competenze di spettanza anche regionale. Alle Regioni è così consentito realizzare una serie di azioni volte a migliorare le condizioni di vivibilità dei rispettivi territori, nell'ambito di competenze ad esse assegnate in via residuale o concorrente, come, ad esempio, le politiche (e i servizi) sociali, la polizia locale, l'assistenza sanitaria, il governo del territorio*".

Il D.L. 14/2017 ha accolto tale ampio concetto di sicurezza disponendo che a mezzo di apposite linee generali, da adottare con accordo sancito in sede di Conferenza unificata (su proposta del Ministro dell'interno), gli attori Istituzionale dovessero «coordinare, per lo svolgimento di attività di interesse comune, l'esercizio delle competenze dei soggetti istituzionali coinvolti, anche con riferimento alla collaborazione tra le forze di polizia e la polizia locale», nei settori di intervento ivi indicati, tenendo conto della «necessità di migliorare la qualità della vita e del territorio e di favorire l'inclusione sociale e la riqualificazione socio-culturale delle aree interessate».

Nel disegno del legislatore statale, infatti, l'intervento delle polizie locali dovrebbe assicurare le precondizioni per un più efficace esercizio delle classiche funzioni di ordine pubblico, per migliorare il contesto sociale e territoriale di riferimento, postulando l'intervento dello Stato in relazione a situazioni non altrimenti correggibili se non tramite l'esercizio dei tradizionali poteri coercitivi.

E nelle «Linee generali delle politiche pubbliche per la sicurezza integrata (art. 2 del decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48)», approvate nella seduta della Conferenza unificata del 24 gennaio 2018, è espressamente rappresentato che le autonomie territoriali possono dotarsi di «*strumenti di "prevenzione situazionale" che […] mirano a ridurre le opportunità di commettere reati unitamente alle misure volte a sostenere la partecipazione dei cittadini alla ricostituzione della dimensione comunitaria e al miglioramento complessivo delle condizioni sociali, abitative e dei servizi ("prevenzione comunitaria") e agli interventi di prevenzione sociale finalizzati al contenimento dei fattori criminogeni*

La Corte Costituzionale con la citata sentenza n. 285/2019 rappresenta che le iniziative di «prevenzione» e di «lotta» alla criminalità devono necessariamente essere riferite ad attività che non comportano l'esercizio di poteri coercitivi o autoritativi tipici delle funzioni relative all'art. 117, secondo comma, lettera h), Cost. Ed anche con riferimento alle azioni di controllo del territorio l fine di garantire, in concorso con le forze di polizia dello Stato, la sicurezza urbana degli ambiti territoriali di riferimento», l'eventuale assegnazione di compiti attinenti alla pubblica sicurezza, tra cui evidentemente rientra l'attività di pattugliamento del territorio, non può essere decisa unilateralmente dalla Regione, pena l'invasione della competenza esclusiva dello Stato ai sensi dell'art. 117, secondo comma, lettera h), Cost. (sentenza n. 167 del 2010; nello stesso senso, sentenza n. 35 del 2011).

Dal punto di vista operativo, si rappresenta che numerose sono le disposizioni del nostro ordinamento che disciplinano le interazioni tra la polizia locale e l'autorità di pubblica sicurezza, quale ad es.

- il combinato disposto dei commi 1, lettera c), e 2 dell'art. 5 della legge 7 marzo 1986, n. 65 (Legge-quadro sull'ordinamento della polizia municipale) che prevede che possano essere assegnati alla polizia municipale compiti ausiliari di pubblica sicurezza, ma solo su decisione del prefetto, previa comunicazione al sindaco; la medesima legge stabilisce
- l'art. 3 della medesima norma che prevede che gli addetti alla polizia municipale «collaborano, nell'ambito delle proprie attribuzioni, con le Forze di polizia dello Stato», ma solo «previa disposizione del sindaco, quando ne venga fatta, per specifiche operazioni, motivata richiesta dalle competenti autorità»
- con riguardo al controllo del territorio, il comma 8 dell'art. 12 del decreto-legge 13 maggio 1991, n. 152 (Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa), convertito, con modificazioni, nella legge 12 luglio 1991, n. 203, assegna al Ministro dell'interno il potere di emanare direttive «per la realizzazione a livello provinciale, nell'ambito delle potestà attribuite al prefetto […], di piani coordinati di controllo del territorio

2. L'inquadramento con la normativa in materia di protezione dei dati personali

Come riportato dalle "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video" del 20.01.2020, il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, rientra nella direttiva (UE) 2016/680.

La polizia locale rientra, pertanto, nella definizione di Autorità di cui all'art. 2 lett. g) del D.lgs. 51/2018. Tuttavia, il perimetro di azione definito nel paragrafo precedente assegna connotati di marginalità alle azioni della polizia locale che è possibile ricondurre

nell'alveo dello stesso D.lgs. 51/2018; la parte preponderante dell'azione di polizia locale deve essere, pertanto, ricondotta alla disciplina di cui al Regolamento UE 2016/679.

Tale assunto spiega i propri effetti anche nei sistemi integrati di videosorveglianza, per i quali la ripartizione di compiti e responsabilità non può che seguire i binari della titolarità del trattamento distinta e parallela.

È pur auspicabile che i sistemi di videosorveglianza siano integrati tra le forze di polizia, tuttavia le finalità perseguite a mezzo di tali sistemi e le configurazioni di accesso, visione, conservazione (ecc.) devono essere coerenti con la definizione dei perimetri di azione riconosciuti in capo alle diverse organizzazioni.

E', pertanto, irricevibile configurare le relazioni tra le autorità di pubblica sicurezza e le polizie locali in termini di contitolarità dei trattamenti che discendono dall'utilizzo dei sistemi di videosorveglianza.

3. Informativa per il trattamento dei dati personali

Gli Enti locali rendono nota ai cittadini la presenza di sistemi di videosorveglianza a mezzo di informativa cartellonistica.

Sul proprio sito istituzionale pubblicano un'informativa per il trattamento dei dati personali che presenti i contenuti di cui all'art. 13 del GDPR oppure, ove applicabile, di cui all'art. 10 del D.lgs. 51/2018.

Si ritiene, infatti, che rendere palese l'utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una efficace funzione di deterrenza.

L'informativa può non essere resa in tutti i casi in cui costituisca ostacolo concreto delle specifiche ragioni di tutela della sicurezza urbana, con specifico riferimento ad azioni di prevenzione della criminalità, in particolare di tipo predatorio.

4. Sistemi integrati di videosorveglianza

Il ricorso a sistemi integrati di videosorveglianza tra diversi soggetti pubblici (ed anche privati) costituisce espresso auspicio del legislatore e corollario del principio della sicurezza integrata di cui ai paragrafi che principiano la presente appendice.
Si ritiene, pertanto, che ogniqualvolta sia installato un sistema di videosorveglianza da parte degli Enti locali sia atto coerente con l'impianto normativo attuale condividerne specifiche e finalità con il Comitato metropolitano di cui all'art. 6 del D.L. n. 14/2017 e/o con il Comitato provinciale per l'ordine e la sicurezza pubblica di cui all'art. 20 della L. 121/1981.

Come già sottolineato in precedenza, l'implementazione di sistemi integrati di videosorveglianza non comporta la contitolarità dei trattamenti di dati personali che ne derivano. Da ciò deriva che ciascun titolare tratta le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali.

Ciò anche nel caso in cui la gestione tecnologica del sistema sia assegnata ad un unico Soggetto, il quale sarà nominato responsabile del trattamento ai sensi e per gli effetti di cui all'art. 28 del GDPR.

APPENDICE B

VIDEOSORVEGLIANZA PER FINALITA' DI SORVEGLIANZA RIFIUTI

1. Il quadro normativo

Il divieto assoluto di abbandono dei rifiuti sul suolo, nel sottosuolo e nelle acque superficiali sotterranee è sancito dagli artt. 192 e 255 del decreto legislativo 3 aprile 2006, n. 152.

La violazione di tale divieto comporta una sanzione penale, se l'abbandono è riconducibile ad un'attività di impresa o ad un ente, o amministrativa, se si tratta di rifiuti di natura domestica abbandonati dai privati cittadini.

Il Garante nel provvedimento dell'8 aprile 2010 già osservava "*l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi. Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente* (art. 13, legge 24 novembre 1981, n. 689) "

Il degrado ambientale generato dall'abbandono di rifiuti è violazione della vivibilità e del decoro delle città posti alla base del concetto di sicurezza urbana di cui al D.lgs. 14/2017.

2. L'aderenza ai principi di liceità, finalità e proporzionalità

Tali violazioni costituiscono, altresì, un costo rilevante per la collettività, in quanto la rimozione dei rifiuti ed il loro smaltimento sono posti a carico degli enti proprietari delle strade o dei comuni nel cui territorio vengono abbandonati.

Per di più, si tratta di una fattispecie di illecito il cui accertamento, non supportato da strumenti, è ostico: o si è colti in flagranza oppure vi sono testimoni oculari.

L'effetto deterrente costituito dalla presenza di un sistema di videosorveglianza ha fatto registrare evidenze significative.

In molti Enti sono state utilizzate anche telecamere mobili, le cosiddette «fototrappole» che, posizionate nelle zone più a rischio, perché isolate oppure facilmente raggiungibili con mezzi idonei a trasportare rifiuti ingombranti, sono servite a rilevare e sanzionare tutti coloro che scaricano materiale non autorizzato.

Il dato esperienziale fornisce evidenze in ordine alla scarsa efficacia di strumenti e sistemi di controllo alternativi.

Pertanto, la valutazione di aderenza ai principi di liceità, finalità e proporzionalità di cui al GDPR di sistemi di videosorveglianza aventi finalità di lotta al degrado derivante dall'abbandono dei rifiuti e alla comminazione delle sanzioni previste dalla legge non può che giungere ad esiti positivi.

Si rappresenta che, in ogni caso, è necessario che il sistema di videosorveglianza che si intende implementare rispetti (tra le altre cose) il principio di minimizzazione; l'Ente dovrà pertanto esperire una valutazione in termine di necessità riferita alle caratteristiche di tale sistema (numero di telecamere, brandeggiabilità, registrazione h24 o con sensori di movimento ecc. ecc.).

3. Informativa per il trattamento dei dati personali

L'Ente è tenuto ad affiggere cartelli informativi nei punti e nelle aree in cui si svolge la videosorveglianza, che contengano anche indicazioni su come e dove reperire un testo completo contenente tutti gli elementi di cui all´art. 13 del Regolamento

APPENDICE C

UTILIZZO DI MICROCAMERE INDOSSABILI (BODYCAM) E DI DASH CAM

Premessa

La crescente richiesta da parte degli Enti di utilizzo di strumenti portatili di registrazione video (ad es. body cam e dash cam) è certamente correlata ad una specificità delle registrazioni video in termini di vicinanza, di fruibilità, di immediatezza e, non si sottovaluti, di deterrenza.

Per quel che concerne le body cam la portata di tali video non consente una percezione esaustiva del contesto di riferimento e comporta un livello elevato di rischi specifici per i diritti e le libertà fondamentali dei cittadini, anche di rilievo costituzionale (diritto alla riservatezza e alla protezione dei dati personali ex art. 2 Cost. e libertà di circolazione ex art. 16 Cost.), e richiede una precipua regolamentazione che ne disciplini l'utilizzo in stretta aderenza alle cautele prevista dalla normativa in materia di protezione dei dati personali.

In linea generale, si sottolinea come la possibilità di riprodurre gli interventi esperiti relativi ad azioni volte alla tutela della sicurezza urbana, ad esempio, elude le cosiddette "distorsioni percettive", ovvero la possibilità che in ragione di un intervento a forte impatto emotivo il soggetto coinvolto possa percepire suoni, azioni e successione temporale in maniera involontariamente difforme dal reale.

Per quanto concerne le dash cam si rileva che l'impiego di tali strumenti comporta rischi elevati per i diritti e le libertà delle persone poiché costituisce strumento suscettibile di essere utilizzato per azioni di sorveglianza indiscriminata di massa

1. L'aderenza ai principi di liceità, finalità e proporzionalità

Le esigenze rappresentate dagli Enti convergono nella quasi totalità verso un utilizzo di tali strumenti volto alla tutela della sicurezza urbana, come declinata nel presente documento.

Specificatamente, gli Enti considerano l'opportunità di utilizzare tali strumenti in costanza di specifiche esigenze di ordine e sicurezza connesse alle peculiarità di un determinato servizio, anche operativi, potenzialmente atti a pregiudicare la sicurezza degli operatori o di terze persone coinvolte dalle operazioni.

Si ritiene che l'utilizzo di microcamere indossabili e di dash cam debba essere limitato alle situazioni di effettiva necessità per prevenire un pericolo o per altra concreta ed individuata esigenza, che non possa essere altrimenti soddisfatta, prevedibile o sopraggiunta, nel corso dello svolgimento delle attività istituzionali.

In ogni caso l'Ente attiva la procedura di cui all'art. 4, comma 1, legge 20.5.1970, n. 300.

Inoltre, l'Ente è tenuto ad adottare un atto di natura regolamentare in ordine all'utilizzo di tale strumento da parte della polizia locale.

Si ritiene che sia in ogni caso consentito l'utilizzo di tali strumenti ai fini dell'acquisizione puntuale e specifica di fonti di prova sia penali che amministrative, ovvero nei casi in cui gli utilizzi degli stessi **non comportino attività di sorveglianza sorveglianza indiscriminata di massa, anche preterintenzionale**.

2. Minimizzazione dei dati e modalità d'utilizzo

Il trattamento di dati effettuati a mezzo di tali strumenti dovrà essere configurato in maniera tale da trattare solo dati pertinenti e non eccedenti.

A titolo esemplificativo, si ritiene che

- il trattamento di dati debba essere effettuato in modo trasparente, ovverosia devono essere implementate misure che rendano manifesto l'utilizzo delle body cam (ad es. gli agenti devono avvisare che è in corso la registrazione) e delle dash cam (ad es. informativa grafica con attivazione delle luci rotanti/lampeggianti in caso di attivazione della registrazione);
- l'attivazione della registrazione a mezzo delle body cam sia demandata all'agente sul campo, mentre l'attivazione della registrazione delle dash cam sia demandata ai soli agenti all'interno dell'autoveicolo;
- deve essere individuata la tipologia di eventi in cui è prevista l'attivazione dei dispositivi
- può essere consentita la visualizzazione delle immagini raccolte solo al personale a ciò autorizzato ed in presenza di predefinite circostanze
- in ogni caso dovrebbe essere esperita una prima fase di sperimentazione con un numero esiguo di dispositivi per acquisire contezza in ordine all'utilizzo materiale degli stessi e all'efficacia degli stessi rispetto alle finalità perseguite

L'Ente dovrebbe adottare un Disciplinare a mezzo del quale regolamentare l'impiego dei dispositivi citati.

Specificatamente, devono essere previste le condizioni che ne consentono l'attivazione, e quelle in cui è esclusa l'attivazione. Il disciplinare dovrà indicare altresì il modo in cui potranno essere utilizzati tali dispositivi, avvertendo della necessità di adottare particolari cautele in casi particolari.

Devono essere, altresì, esplicitati gli impieghi che l'Ente può effettuare in ordine alle immagini videoregistrate.

Con il medesimo disciplinare interno la società fornirà altresì specifiche istruzioni ai soggetti autorizzati in servizio presso la centrale operativa (forniti di specifiche credenziali e incaricati della visualizzazione delle immagini in tempo reale) circa le ipotesi in presenza delle quali inviare soccorsi e/o avvisare le forze di polizia

3. Durata della conservazione delle immagini video

La definizione del tempo di conservazione delle immagini è strettamente correlata alle finalità per cui le stesse sono trattate.

Non è escluso che siano previste tempistiche differenti in ordine alla tipologia di impiego. A mero titolo esemplificativo, nel caso di immagini inerenti fattispecie di reato perseguibili a querela, queste potrebbero essere conservate per il termine massimo di presentazione della querela oppure nel caso di immagini inerenti reati precedibili d´ufficio saranno conservate fino a cessate esigenze dell´ A.G.; nel caso di registrazione di immagini non rilevanti in ragione della finalità per cui sono state effettuate si potrebbe procedere alla cancellazione immediata.

In ogni caso, l'Ente è tenuta a predisporre meccanismi di cancellazione automatica delle informazioni allo scadere del termine previsto per la conservazione dei dati, anche immediata nei casi di non rilevanza delle immagini registrate.

4. Misure di sicurezza

Richiamando quanto già riportato in tema di sicurezza informatica nella parte generale del presente vademecum, e senza alcuna pretesa d'esaustività, si rappresenta che l'Ente dovrebbe in ogni caso

- registrare e tracciare le operazioni di accesso ed estrazione dei dati raccolti effettuate dai soggetti a ciò specificamente autorizzati

- adottare specifiche misure affinché gli operatori che hanno in dotazione i dispositivi non possano effettuare operazioni di modifica, cancellazione e duplicazione delle immagini raccolte

- utilizzare tecniche di cifratura ai fini della conservazione delle immagini con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

- implementare tecniche di cancellazine irreversibile

APPENDICE D)

AEROMOBILI A PILOTAGGIO REMOTO

E' indubbio che l'utilizzo dei droni possa costituire un elemento di potenziamento e riqualificazione delle azioni di prevenzione, indagine, accertamento e perseguimento di reati.

E' indubbio, altresì, che tale utilizzo comporti rischi elevatissimi per i diritti e le libertà delle persone e interferisce direttamente con i diritti al rispetto della vita privata e alla protezione dei dati di carattere personale, tutelati a norma dell'articolo 8 della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali ("CEDU") e dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea ("Carta"), anche quando questi sono impiegati dalle forze dell'ordine.

Principio di liceità

Si ritiene che sia in ogni caso consentito l'utilizzo dei droni ai fini dell'acquisizione puntuale e specifica di fonti di prova sia penali che amministrative, ovvero nei casi in cui gli utilizzi degli stessi **non comportino attività di sorveglianza sorveglianza indiscriminata di massa, anche preterintenzionale**. A titolo esemplificativo si ritiene lecito l'utilizzo dei droni ai fini delle attività dell'ente in materia di pianificazione territoriale ed urbanistica, della definizione del Piano Antenne o del monitoraggio di cantieri, rilievi e ispezioni.

Gli orientamenti del (fu) Gruppo di lavoro articolo 29 per la protezione dei dati con il Parere 01/2015

D'altra parte, come già ampiamente sottolineato dal (fu) Gruppo di lavoro articolo 29 per la protezione dei dati con il Parere 01/2015 sulle questioni riguardanti il rispetto della vita privata e la protezione dei dati connesse all'uso di droni del 16 giugno 2015 "*in base all'articolo 52, paragrafo 1, della Carta e all'articolo 8, paragrafo 2 della CEDU, tali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta* ***devono essere conformi alla legge ("previste dalla legge"),*** *apportate solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui ("perseguono uno o più finalità legittime previste all'articolo 8, paragrafo 2, della CEDU e sono necessari in una società democratica).*

Di conseguenza, la polizia e altre autorità di contrasto che utilizzano droni devono assicurarsi di disporre di una valida base giuridica per il trattamento di dati personali".

Nel parere succitato, oltre a fornire elementi utili ai fini dell'espletamento delle indagini di aderenza ai principi di proporzionalità e necessità, viene ribadito che devono essere "*posti limiti all'uso di droni per le attività di sorveglianza, al fine di evitarne una pratica diffusa o l'impiego per segnalare obiettivi in base all'analisi dei dati. Pertanto, i droni*

devono essere utilizzati soltanto per una serie strettamente limitata e giustificata di finalità, che potrebbero essere elencate previamente e, in ogni caso, con limiti geografici e temporali."

In sintesi, l'utilizzo di droni per le finalità di prevenzione, indagine, accertamento e perseguimento di reati deve essere necessariamente previsto da una norma di legge o di regolamento, se previsto da legge.

Le medesime condizioni di liceità devono essere rispettate anche nel perseguimento di infrazioni civili a mezzo dell'utilizzo dei droni.

Gli interventi del legislatore italiano

Il legislatore italiano ha, pertanto, disciplinato tali aspetti con l'art. 5 comma 3sexies del D.L. 7/2015 disponendo che "*Fermo restando quanto disposto dal codice della navigazione e dalla disciplina dell'Unione europea, con decreto del Ministro dell'interno, di concerto con il Ministro della difesa, con il Ministro dell'economia e delle finanze e con il Ministro delle infrastrutture e dei trasporti, da emanare, sentito l'Ente nazionale per l'aviazione civile (ENAC), entro centoventi giorni dalla data di entrata in vigore della presente disposizione, sono* ***disciplinate le modalita' di utilizzo, da parte delle Forze di polizia, degli aeromobili a pilotaggio remoto, comunemente denominati 'droni', ai fini del controllo del territorio per finalita' di pubblica sicurezza****, con particolare riferimento al contrasto del terrorismo e alla prevenzione dei reati di criminalita' organizzata e ambientale, nonche' per le finalita' di cui all'articolo 2, comma 1, del decreto legislativo 19 agosto 2016, n. 177, e, per il Corpo della guardia di finanza, anche ai fini dell'assolvimento delle funzioni di polizia economica e finanziaria di cui all'articolo 2 del decreto legislativo 19 marzo 2001, n. 68. All'attuazione del presente comma si provvede nell'ambito delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente e comunque senza nuovi o maggiori oneri a carico della finanza pubblica.((L'utilizzo di aeromobili a pilotaggio remoto da parte del personale abilitato del Corpo di polizia penitenziaria e' previsto nell'ambito delle funzioni svolte dal predetto personale ai sensi dell'articolo 5 della legge 15 dicembre 1990, n. 395, per assicurare una piu' efficace vigilanza sugli istituti penitenziari e garantire la sicurezza all'interno dei medesimi)).* "

Con Decreto del 29 aprile 2016 il Ministero dell'Interno ha disciplinato le modalita' di impiego dei sistemi aeromobili a pilotaggio remoto (SAPR) in dotazione o in uso alle Forze di polizia.

All'art. 2 del medesimo Decreto viene disposto che per Forze di polizia devono intendersi quelle di cui all'art. 16, della legge 1° aprile 1981, n. 121, ovverosia l'Arma dei Carabinieri, il Corpo della Guardia di Finanza e, in parte, Corpo degli agenti di custodia e il Corpo forestale dello Stato.

Conclusioni

Sono da intendersi come escluse da tale definizione le polizie locali.

Ne deriva che gli Enti locali non possono utilizzare aeromobili a pilotaggio remoto, comunemente denominati 'droni', per le finalità di "sicurezza urbana", per il controllo del territorio e più in generale in tutti i casi in cui dall'utilizzo degli stessi possa derivare monitoraggio e sorveglianza, anche solo potenziale, degli individui con correllati rischi elevatissimi per i diritti e le libertà delle persone e alle interferenze con i diritti al rispetto della vita privata e alla protezione della riservatezza degli stessi.

APPENDICE E)

Videosorveglianza per finalità di tutela del patrimonio o dei dipendenti/collaboratori e di protezione dei dati personali e dei sistemi informativi

Premessa

Gli Enti locali, nella loro qualità di datori di lavoro, possono installare un sistema di videosorveglianza nelle sedi di lavoro, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nel rispetto delle altre garanzie previste dalla normativa di settore in materia di installazione di impianti audiovisivi e altri strumenti di controllo (art. 4 della l. 300/1970).

Quando si effettuano trattamenti di dati personali mediante sistemi di videosorveglianza, deve essere garantito il rispetto dei principi di:

- liceità;

- necessità;

- proporzionalità;

- finalità.

Principio di liceità

Il rispetto degli interessi e/o i diritti e le libertà fondamentali degli interessati è assicurato dall'aderenza del trattamento a:

- alle prescrizioni della normativa vigente in materia di protezione dei dati personali (regolamento UE n. 679/2016 e D. Lgs. 196/03, c.d. "Codice Privacy");
- alle disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi;
- alle norme riguardanti la tutela dei lavoratori (L. 300/70, c.d. "Statuto dei Lavoratori");
- alle prescrizioni in materia dell'Autorità Garante per la protezione dei dati personali (tra cui il "Provvedimento in materia di videosorveglianza" dell'8 aprile 2010);

Le immagini raccolte tramite sistemi di videosorveglianza non possono in alcun modo essere utilizzate per controlli, anche se indiretti, sull'attività lavorativa del personale.

Principio di necessità

I sistemi di videosorveglianza sono installati, configurati e programmati in modo da escludere ogni uso superfluo o ridondante di immagini e dati personali. Non è

consentito, pertanto, l'utilizzo di videocamere brandeggiabili, di sistemi di zoom o di ingrandimento delle immagini se non con mero adattamento bidimensionale dell'immagine fissa.

Finalità (limitazione delle)

Il trattamento di dati personali tramite un sistema di videosorveglianza è lecito solo se soddisfa il principio di limitazione delle finalità (cfr. Articolo 5 lettere a) e b) GDPR), ossia i dati sono trattati per scopi determinati, espliciti e legittimi. Tali legittimi scopi sono:

a) tutela del patrimonio o delle persone;

b) protezione dei dati personali e dei sistemi informativi;

È invece ammesso l'impiego di sistemi di videosorveglianza come misura complementare al miglioramento della sicurezza all'interno o all'esterno degli edifici degli Enti, o allo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa degli Enti, o di terzi sulla base di immagini utili in caso di fatti illeciti.

Soggetti autorizzati

Il trattamento di dati personali mediante l'impiego di sistemi di videosorveglianza è consentito esclusivamente ai soggetti preventivamente autorizzati (responsabili e/o "incaricati"). I profili di accesso di tali soggetti devono essere configurati in funzione delle funzioni assegnate (specifiche operazioni di trattamento previste).

Le operazioni di registrazione e consultazione dei dati registrati sono ammesse solo nei casi in cui sia indispensabile per gli scopi perseguiti. In particolare, la consultazione dei dati registrati può essere effettuata soltanto:

- per esigenze di manutenzione degli impianti;
- per assistenza alla competente Autorità giudiziaria;
- nel caso di visite ispettive da parte dell'Autorità Garante per la protezione dei dati personali;
- in caso di richiesta di accesso dell'interessato ai propri dati personali.

Tempo di conservazione delle immagini

Il GDPR dispone che il titolare del trattamento adotta politiche e attua misure adeguate a garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme allo stesso Regolamento (principio di accountability).

Tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento. Dette misure sono riesaminate e

aggiornate qualora necessario. Inoltre, se ciò è proporzionato rispetto alle attività di trattamento, le predette misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

Tale regime comporta un approccio profondamente differente rispetto al previgente assetto del Codice per la protezione dei dati personali, in cui cardini fondamentali dell'assetto normativo erano costituiti dagli interventi autorizzativi dell'Autorità. Gli effetti di tale mutata prospettiva si propagano anche sui Provvedimenti generali emessi dal Garante per la protezione dei dati personali, ivi compreso il Provvedimento in materia di videosorveglianza dell'8 aprile 2010. In tale Provvedimento, erano sottoposti ad autorizzazione preventiva i tempi di conservazione delle immagini superiori alle 24 ore. Il principio di accountability impone all'organizzazione che intende installare il sistema di videosorveglianza di valutare l'adeguatezza (valutazione che s'intende *ex ante*) delle misure che da implementare, ivi compresa la rispondenza dei tempi di conservazione delle immagini alle finalità perseguite.

Gli Enti sono tenuti, pertanto, a valutare l'efficacia di un determinato periodo di conservazione rispetto alle esigenze e alle finalità perseguite.

Si ritiene che il tempo di conservazione necessario al perseguimento delle finalità di tutela del patrimonio o dei dipendenti/collaboratori e di protezione dei dati personali e dei sistemi informativi non dovrebbe essere superiore ai sette giorni, fatte salve speciali esigenze di ulteriore conservazione ad esempio correlate a specifiche richieste dell'Autorità Giudiziaria. Le immagini devono essere cancellate con sovrascrittura automatica.

Informativa per il trattamento dei dati personali

Le zone soggette a videosorveglianza devono essere adeguatamente segnalate e agli interessati deve essere fornita idonea informativa, in aderenza alle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate dall'EDPB il 29 gennaio 2020.

Accordo con le rappresentanze sindacali aziendali/Autorizzazione Ispettorato

L'installazione dei sistemi di videosorveglianza dai quali possa derivare la possibilità di controllo a distanza dell'attività dei lavoratori, può essere giustificata solamente per esigenze (fra le altre) di tutela del patrimonio aziendale.

In ogni caso, l'installazione è possibile previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali, oppure ove non sia stato possibile raggiungere tale accordo, solo in quanto preceduta da apposita autorizzazione dell'Ispettorato del lavoro.

Non costituisce condizione di liceità l'acquisizione del consenso dei lavoratori acquisito dal datore di lavoro.

Sotto il profilo sanzionatorio l'art. 171 del D.lgs. 196/2003 prevede che "*la violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, e' punita con le sanzioni di cui all'articolo 38 della medesima legge*". Tale norma prevede che per i casi meno gravi sia comminata la sanzione alternativa dell'ammenda da € 154,00 a € 1549,00 o dell'arresto da 15 giorni ad un anno, pena che può essere aumentata fino al quintuplo dal Giudice se la ritiene inefficace in relazione alle condizioni economiche del reo.

Si ritiene applicabile a tale fattispecie l'istituto della "prescrizione obbligatoria" di cui all'art. 15 del D.lgs. 124/2004 il qual stabilisce che "*Con riferimento alle leggi in materia di lavoro e legislazione sociale la cui applicazione è affidata alla vigilanza della direzione provinciale del lavoro, qualora il personale ispettivo rilevi violazioni di carattere penale, punite con la pena alternativa dell'arresto o dell'ammenda ovvero con la sola ammenda, impartisce al contravventore una apposita* **prescrizione obbligatoria** *ai sensi degli articoli 20 e 21 del decreto legislativo 19 dicembre 1994, n. 758, e per gli effetti degli articoli 23 e 24 e 25, comma 1, dello stesso decreto*".

In altri termini, gli Ispettori del lavoro, agendo in qualità di polizia giudiziaria ex art. 55 c.p.p., qualora ritengano il fatto non grave, dovrebbero ordinare al Datore di lavoro di sanare la situazione (e, quindi, di procedere con l'accordo sindacale o con l'autorizzazione dell'Ispettorato) entro un termine congruo, comunicando la notizia di reato al Pubblico ministero.

Dopo aver verificato l'avvenuto adempimento della prescrizione, gli Ispettori dovrebbero ammettere il datore di lavoro a pagare, in sede amministrativa, nel termine di trenta giorni, una somma pari ad ¼ dell'importo massimo dell'ammenda stabilita per la contravvenzione commessa, per poi informare il P.M. dell'avvenuto adempimento.

E' prevista la sanzione dell'arresto congiunta all''ammenda.

Per i casi più gravi non potrà trovare applicazione il procedimento di "prescrizione obbligatoria" di cui al citato art. 15 del D.lgs. 124/2004 e, pertanto, l'Ispettorato non impartirà al datore le prescrizioni volte alla rimozione o modifica delle irregolarità riscontrate e, per di più, la sanzione non può essere oggetto di oblazione.

La gravità della fattispecie è determinata da elementi quali assenza di esigenze organizzative, produttive e di sicurezza del lavoro, la presenza di impianti occulti e elementi specifici quali il numero di telecamere, il loro posizionamento, la tipologia di videocamere, il tempo di conservazione delle immagini ecc.

Tali aspetti costituiscono elementi di valutazione anche con riferimento alle sanzioni amministrative che il Garante potrebbe comminare nei confronti del datore di lavoro.

APPENDICE F)

Videosorveglianza e operazioni di monitoraggio del traffico veicolare

Premessa

A fronte di una estrema varietà e complessità dei fenomeni di traffico sulla rete stradale, cresce l'esigenza di monitoraggio e controllo dei flussi.

Tali attività comportano trattamenti di dati personali che, se non definite in aderenza ai principi di privacy by design e by default, producono l'insorgere di rischi, di livello elevatissimo, per la riservatezza dei cittadini.

Per di più con gli ultimi sviluppi tecnologici in ambito Internet of Things, AI e Machine learning la raccolta massiva di dati e informazioni diviene ingrediente essenziale per le politiche degli Enti negli ambiti indicati nel paragrafo seguente.

Principio di finalità

Il monitoraggio del traffico stradale è operazione che può essere impiegata per assolvere diverse finalità di trattamento, che, peraltro, possono presentare tra loro elementi di disomogeneità tali da determinare differenti livelli di criticità e di impatti sulla protezione dei dati personali.
A titolo esemplificativo e non esaustivo il monitoraggio del traffico può assolvere a

- Regolazione del traffico.
- Informazione all'utenza.
- Assistenza alla guida
- Sorveglianza di passaggi a livello
- Sicurezza nelle gallerie e protezione di opere d'arte
- Manutenzione della carreggiata
- Supporto a studi e ricerche

E' onere dell'Ente condurre una valutazione d'impatto su tali utilizzi della videosorveglianza e configurare il trattamento in aderenza al principio di minimizzazione dei dati.

Principio di minimizzazione

Già il Garante per la protezione dei dati personali[5] rappresentava che ciascun sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi; svolgeva un espresso riferimento alle operazioni di monitoraggio del traffico, valutando che fossero sufficienti all'esaudimento delle finalità solo riprese generali che escludessero la possibilità di ingrandire le immagini e rendere identificabili le persone. Sulla scorta di quanto riferito al paragrafo che precede, quindi, l'Ente è tenuta a valutare la

[5] Nel Provvedimento in materia di videosorveglianza dell'8 aprile 2010.

proporzionalità dei dati trattati e le finalità specifiche perseguite dall'Ente, tenuto conto che i sistemi oggi consentono elaborazioni dei dati certamente più strutturate.

Il principio di trasparenza

E' di tutta evidenza che la complessità di un sistema di monitoraggio del traffico varia in rapporto agli obiettivi del monitoraggio stesso, ai metodi o alle tecnologie adoperate, alla catena di misura, trasferimento e trattamento dell'informazione. Con riferimento all'utilizzo di tecnologie di AI e machine learning si raccomanda all'Ente di utilizzare un approccio trasparente, con l'obiettivo di consentire agli utenti di comprendere con quale finalità sono raccolti i dati che li riguardano e con quali modalità verranno utilizzati. Al fine di promuovere studi ed elaborazioni da parte di privati l'Ente potrebbe rendere disponibili al pubblico i dati statistici, di traffico ed eventi necessari alla gestione della viabilità ed infomobilità.
In ogni caso, l'Ente deve dare la maggiore diffusione possibile ai prospetti informativi relativi ai trattamenti di dati personali effettuati a mezzo delle operazioni di monitoraggio del traffico.