UNIONE POLIZIA LOCALE ITALIANA

LORENZO TAMOS

REATI E PRIVACY

GUIDA ALLE NORME 5.2020

GUIDA ALLE NORME N.5.2020
del 12 maggio 2020

Direzione e coordinamento editoriale:
Massimiliano Mancini, segretario generale UPLI

Guida senza periodicità a uso interno dell'associazione.

UPLI-Unione Polizia Locale Italiana
Associazione di categoria senza scopo di lucro
c.f. 97984710588
www.unionepolizialocaleitaliana.it
facebook.com/UnionePoliziaLocaleItaliana

PRIVACY E POLIZIA

La nuova normativa europea sulla privacy, nonostante dovrebbe essere ben consolidata essendo prossima al traguardo dei quattro anni dall'entrata in vigore, è ancora poco conosciuta soprattutto in Italia, dove in molti casi si lesina in eccessiva tolleranza nell'applicazione e in altri casi si presta ad applicazioni particolarmente negative da essere pretestuose.

Ancora oggi si violano deliberatamente le più basilari prescrizioni della normativa del DGPR, così alcune amministrazioni pubbliche, a tutt'oggi, non hanno nemmeno provveduto alla nomina del responsabile alla protezione dei dati-DPO oppure non hanno fornito l'informativa sulla privacy o fanno ancora riferimento a moduli predefiniti ai sensi delle precedenti norme abrogate, tutto ciò nella falsa convinzione che gli enti pubblici in genere e le forze di polizia ancor di più (non si sa per quale ragionevole motivo) siano legibus solutibus, al di sopra delle norme che invece vincolano uniformemente tutti i cittadini europei e tutte le istituzioni nel territorio comunitario.

Viceversa si assiste spesso a immotivati rifiuti da parte della pubblica amministrazione di fornire dati, contenuti, documenti adducendo ragioni di tutela dei dati personali, senza il minimo riferimento alla norma di legge, utilizzando in sostanza la normativa sulla privacy come pretesto per limitare la trasparenza o per coprire le inefficienze.

Uno dei casi che conferma questa impressione generale è il trattamento dei dati personali da parte delle forze di polizia.

C'è una generale convinzione che l'attività di polizia, per il suo ruolo nell'ambito della sicurezza dello Stato e dei cittadini, goda di una generale inapplicabilità delle norme della privacy.

Ma non è affatto così!

Massimiliano Mancini,
Direttore Guida alla Norma UPLI.

LORENZO TAMOS
Avvocato specializzato in diritto amministrativo e privacy

REATI E PRIVACY

www.unionepolizialocaleitaliana.it/2020-g5/

INDICE

INTRODUZIONE

Questa breve guida vuole introdurre il tema del trattamento dei c.d. “dati personali di reato” quando e se non d’acchito rientranti nell'ambito di applicazione del **Decreto legislativo 18 maggio 2018 n.51**[1] che, in Italia, ha recepito la **Direttiva 2016/680 UE**[2] poiché, ad esempio, non attinenti a dati personali di un individuo contenuti in una sentenza penale di condanna quale ipotesi di trattamento pacificamente riferibile all'ambito applicativo (soggettivo e materiale) della normativa nazionale d'attuazione della succitata Direttiva nota ai più come “Direttiva di Polizia”.

Invero, per quanto qui rileva, gli ultimi aggiornamenti della normativa europea in materia di trattamento dei dati personali hanno avuto almeno un triplice non trascurabile effetto:

- hanno ampliato il concetto di c.d. dato personale di reato;
- hanno esteso il novero dei soggetti tenuti, individualmente e/o con le forze dell’ordine istituzionali, all’applicazione delle disposizioni interne di recepimento della Direttiva UE 2016/680 UE;
- hanno introdotto un nuovo e più specifico metodo di trattamento che, se non osservato in concreto, può comportare gravi responsabilità.

---

[1] Decreto legislativo 18 maggio 2018 n.51, *Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*. Disponibile all’indirizzo: https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg.

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

UNA "COPERTA" NORMATIVA APPARENTEMENTE CORTA?

Al riguardo pare ad oggi sussistere una sorta di inconsapevole trascuratezza dottrinale ed una certa frettolosità nell'interpretare la normativa di riferimento con riguardo ad un **tema** che, invece, **meriterebbe grande attenzione tecnica**, **scientifica ed istituzionale** se non altro per l'ampia manifestazione concreta che lo stesso quotidianamente ha e potrebbe sempre più avere.

Usando il linguaggio colloquiale che viene sollecitato dalla normativa europea sul trattamento dei dati personali, la questione critica **si potrebbe spiegare nel seguente modo**: «*se è facile comprendere che chi ruba, o tenta di rubare, compie un fatto umano previsto dalla legge penale come reato, le cose si complicano molto qualora ci si trovi a trattare i dati personali dell'autore del furto, o di chi è solo sospettato essere tale, al di fuori delle classiche ipotesi dell'arresto in flagranza, della denuncia alle forze di polizia da parte della vittima o da chi abbia assistito direttamente alla commissione del delitto*».

E la stessa complicazione potrebbe sussistere anche rispetto al fatto umano di colui che, sempre ad esempio, semplicemente rischi di provocare delle lesioni gravi ad altri, ovvero rispetto al caso di chi solo tenti di danneggiare dei beni materiali altrui senza riuscirvi.

Eppure, in tutte le accennate ipotesi che consentono l'identificazione sia di chi abbia davvero rotto il naso ad un individuo, o danneggiato la proprietà di altri, e sia di chi sia stato solo sospettato (o tacciato) di averlo fatto, vi sarebbe sempre da attentamente considerare **un tipo di trattamento di dati personali delicato e speciale**, poiché (in base alla

ratio legis euro unitaria) in grado di ripercuotersi in negativo, gravemente e a lungo, sulla persona fisica a cui quei dati personali, afferenti a simili gravi fatti umani (accertati, creduti o sospettati), si potrebbero riferire.

I profili di potenziale **criticità** che nascono da queste situazioni, almeno dall'angolo visuale del possibile **trattamento dei dati** che esse comportano, sono molti e significativi, soprattutto in ragione delle diffuse vicende umane quotidiane rispetto alle quali tali dati personali si rendono trattabili sia dalle autorità istituzionali competenti, sia da parte di cittadini ovvero variegati organismi privati[3].

Come noto agli "addetti ai lavori" tale tipo di trattamento di dati, sebbene non rientrante tra le categorie dei c.d. dati particolari *ex* art.9 del GDPR (Reg.UE n.2016/679[4]), è disciplinato e protetto da **una serie di cautele e regole** che non si ritrovano solo nell'art.10 del medesimo regolamento generale, bensì, soprattutto, nella citata Dir.UE n.2016/680, nelle normative nazionali di recepimento della stessa[5] e pure in quelle regolamentari di specificazione delle legislazioni adottate da ogni singolo Stato membro dell'Unione.

---

[3] La trascuratezza riscontrata relativamente a questo tema è stata evidenziata nel corso di un importante convegno pubblico tenutosi a Milano, il 25/06/2019, presso le strutture della Regione Lombardia, ove, difatti, è stato discusso il "*trattamento dati personali nelle pratiche della sicurezza urbana partecipata*" (meglio conosciuta nei paesi anglosassoni con il termine di *neighbourhood watch*), e rispetto al quale sono stati spiegati alcuni profili giuridici della detta questione, con particolare riguardo a ciò che si potrebbe ritenere attinente al sempre più diffuso trattamento "**atipico dei dati personali di reato**".

[4] Regolamento del Parlamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pubblicato in G.U.U.E del 04/05/2016.

[5] Cfr. art.7 del Dlgs n. 51/2018, secondo cui «Il trattamento di dati di cui all'articolo 9 del regolamento UE è autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato».

Ciò detto per, in primo luogo, sottolineare che – oggi senza dubbio – anche i fatti umani **costituenti o valutabili come reato** possono rappresentare delicati dati personali riferibili a persone fisiche e, quindi, essere una parte significativa di quel diritto fondamentale di protezione dell'uomo previsto dall'art.8 della Carta dei Diritti Fondamentale dell'Unione Europea (nota anche come Carta di Nizza)[6], nonché dall'art.16, paragrafo 2, del TFUE (Trattato sul funzionamento dell'Unione Europea)[7].

L'aspetto centrale della questione afferente a tale tipo di delicato trattamento è, dunque, quello di capire non solo **quando ci si trovi** effettivamente **ad avere a che fare con un c.d. "dato di reato"** ma anche **quale normativa** (primaria e secondaria) applicare esattamente al corretto trattamento di tale tipologia di dati anche in relazione a fattispecie concrete che non siano quelle "tipiche" degli operatori di polizia istituzionali o professionali, ovvero di chi svolge una funzione di carattere giuridico (un avvocato, un investigatore munito di licenzia prefettizia, un magistrato).

Orbene, senza pretesa di (poter) approfondire qui l'intero argomento rispetto ad ogni possibile prospettiva che lo stesso pone, basti osservare che l'art.10 del GDPR stabilisce che «*Il trattamento dei dati personali relativi alle condanne penali **e ai reati** o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1* [id est: le c.d. basi legittimanti il trattamento]*, deve avvenire **soltanto sotto il controllo dell'autorità pubblica** o se il trattamento **è autorizzato dal***

---

[6] Cfr. art.8, Carta di Nizza, secondo cui «ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge //».

[7] Cfr. art.16, paragrafo 2, TFUE, secondo cui «Il Parlamento europeo e il Consiglio // stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte // degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione».

diritto *dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati*».

Tale norma del GDPR è abbastanza chiara con riguardo alle prescrizioni che la stessa pone rispetto all'indicazione più generica (e forse maggiormente conosciuta) sul "quando e come" si possono trattare i dati personali di reato al di fuori dell'ambito di applicazione del DLgs.51/2028, ossia:

A) o sotto il controllo dell'autorità pubblica;

B) ovvero perché esiste una norma che autorizzi a farlo e che indica bene il modo in cui proteggere i dati durante il relativo trattamento.

Orbene, se tale disposizione del GDPR risulta "facilmente utilizzabile" rispetto ad alcuni casi pratici, ad esempio quando un privato denuncia alle forze dell'ordine l'autore riconoscibile di una aggressione, **non lo è più** in altri contesti meno immediatamente delineabili sotto il profilo di fatto: ad esempio ove si comunichi la targa di un autoveicolo alle forze dell'ordine in quanto si ha il **mero sospetto** che appartenga ad un soggetto che si ritiene possa commettere un furto, ovvero perché **si pensa** che un individuo identificabile abbia già commesso un atto criminoso utilizzando quel veicolo.

È evidente che nelle sopra descritte ipotesi il trattamento dei dati che scaturisce dalle segnalazioni non ha affatto lo stesso fondamento: il primo trattamento, difatti, si baserebbe su un **fatto** (l'aggressione subita), il secondo si baserebbe su una mera **valutazione** soggettiva (il sospetto di un accadimento) e tuttavia (in base alla normativa in materia di trattamento dati), a discapito della notevole differenza di fondamento su cui poggiano i descritti trattamenti, le due situazioni sono in pratica da porre **sullo stesso piano normativo** e, quindi, da ricondurre alle medesime disposizioni onde **non sbagliare di centrare la normativa** da applicare nel

caso concreto andando a porre in essere una grave violazione.

Al detto proposito v'è difatti da ricordare che (anche) in base all'art.7, paragrafo 1, della Dir.UE n.2016/680[8], nonché, per quanto riguarda l'Italia, all'art.4, comma 1, del Dlgs 51/2018, sia le **mere valutazioni** soggettive che i **veri e propri fatti** accertati possono costituire entrambi **"dati personali di reato"** e, quindi, come tali, da trattare[9] sulla base della stessa confacente normativa e con il medesimo livello di protezione ivi imposto.

Del resto, anche le recenti Linee Guida n.3/2019 sulla c.d. videosorveglianza (video-audio ripresa), per come elaborate dal Comitato Europeo per la Protezione dei Dati[10], sono piuttosto chiare solo in relazione a certi aspetti dalle stesse trattati in forma di esempi.

Tali linee guida, invero, ci indicano che, un conto è lecitamente trasmettere il filmato di un soggetto riconoscibile e ripreso nel mentre commette un reato alle forze dell'ordine o al proprio avvocato, altra cosa, illecita, è appostare il medesimo filmato in rete, ovvero inoltrarselo tra privati cittadini (poiché, in tale ultimo caso, il c.d. "*balance test*" da effettuare tra diritti contrastanti e libertà individuali contrapposte, prevarrebbe a favore della protezione dei dati personali del soggetto ripreso).

Eppure, anche rispetto alle ipotesi che vengono prese in considerazione dalle autorevoli linee guida a cui si è fatto

---

[8] Cfr. art.7, paragrafo 1, Dir.UE n.2016/680, secondo cui «Gli Stati membri dispongono che i dati personali fondati su fatti siano differenziati, nella misura del possibile, da quelli fondati su valutazioni personali».

[9] Cfr. art.4, comma 1, Dlgs n.51/2018, in base al quale «il titolare del trattamento // distingue i dati personali in relazione alle diverse categorie di interessati previste dalla legge e i dati fondati su fatti da quelli fondati su valutazioni //».

[10] Cfr. Linee guida n.3/2019 sul trattamento dei dati attraverso videocamere, adottate dall'EDPB in data 29/01/2020.

cenno, non si riscontrano mai i necessari approfondimenti sui molti casi incerti basati su **semplici valutazioni** (percezioni) personali di privati cittadini, ovvero afferenti all'esercizio di funzioni che non siano quelle ordinarie delle forze dell'ordine ma quelle attribuite ad altri soggetti che eseguono un servizio para-pubblicistico, ovvero sono incarichi di pubblico servizio senza nulla avere direttamente a che vedere con l'ambito operativo delle attività di polizia ma a cui la normativa pur tuttavia si riferisce laddove la stessa, difatti, include tra il novero delle Autorità Competenti tenute ad osservarla anche «***qualsiasi altro organismo o entità incaricata dagli ordinamenti interni*** *...di esercitare l'autorità pubblica e i poteri pubblici //*» (cfr. punto 2, lettera g, dell'art. 2 del Dlgs 51/2018).

LO SCENARIO NORMATIVO

Ebbene, se nella **previgente normativa** domestica sussisteva una maggiore specificità lessicale e i riferimenti normativi avevano una più definita delimitazione applicativa (se non altro terminologica) con riferimento particolare al concetto di **"dato personale giudiziario"** e **"ambito applicativo di polizia"**, oggi, certamente, non è più così o, almeno, non è più sostenibile che lo sia ancora.

In buona sostanza (ed in via di regola generale) se sino al 2016 si poteva ancora sostenere (non sempre a ragione) che il dato personale afferente ai reati era esclusivamente quello c.d. "giudiziario" e l'ambito di trattamento era solo quello riservato alle forze dell'ordine per l'attuazione delle finalità (dirette o indirette) di polizia.

Attualmente, tale **tesi interpretativa non pare essere più "predicabile"** sia sotto il profilo normativo, sia avuto riguardo

al modo pratico in cui i dati di reato sono (sempre più) utilizzati anche da parte di chi non è *tout court* autorità pubblica o autorità competente (e nemmeno un agente di polizia, un qualificato professionista, o un giurista iscritto in un albo professionale).

È quindi opportuno indicare alcuni dei molti spunti normativa che si potrebbero analizzare al suddetto proposito.

L'art.4 del DIgs.n.196/2003, **ante novella 2018**, ad esempio, alla sua lettera e) indicava quali "dati giudiziari", quei «dati personali idonei a rivelare provvedimenti di cui all'art.3, co. 1, lett. da a) ad o) e da r) a u), del DPR n.313/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt 60 e 61 del cpp» e, all'art. 22, il medesimo decreto forniva i «principi applicabili al trattamento di dati sensibili e giudiziari» ivi specificando che «i soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari».

Il non ancora effettivamente abrogato DPR n. 15/2018 (G.U. n.61 del 14-03-2018) in materia di «//trattamento dei dati effettuato per le finalità di polizia, da organi, uffici e comandi di polizia» era/è molto esplicito nell'individuare il proprio ambito applicativo soggettivo.

Così come l'autorizzazione generale n. 7/2016 (del 15/12/2016 n. 5803630) che, invero, si riferiva e si riferisce, esplicitamente, al trattamento dei dati giudiziari (sebbene) da parte di privati, enti pubblici economici e soggetti pubblici, parla espressamente di «*dati giudiziari*» e così via.

I CONFINI APPLICATIVI NORMATIVI PREVIGENTI CI SONO ANCORA?

Oggi, alla luce del Regolamento Generale e della Dir. UE n. 2016/680, tale delimitazione terminologica ed applicativa pare assottigliarsi molto sino a quasi scomparire del tutto.

Il considerando n. 91 e l'art. 10 del GDPR confermano, ad esempio, che (a certe condizioni) i dati afferenti ai dati di reato possono essere trattati anche da chi non è autorità pubblica (ossia da parte dei privati ben oltre i limiti del trattamento c.d. “domestico” che, come tale è escluso dall’applicazione della normativa).

L'art. 1, parag. 1 della Dir. UE n. 2016/680 parla di «*reati o esecuzioni di sanzioni penali*» in tal modo rafforzando **il significato “umanistico” e materiale da attribuire al concetto di dato di reato**, rendendolo del tutto **indipendente**, in termini di riferimento applicativo della normativa, **da un accertamento da parte di una autorità o dalla valutazione**, seppur preliminare, di un ente o forza dell’ordine istituzionale (ivi, invero, specificando "*reati* "*o*" “s*anzioni*").

Il considerando n. 12 della detta Direttiva (DPDPG) si riferisce alle attività di polizia e delle altre autorità preposte anche qualora **non vi sia previa conoscenza della rilevanza penale di un fatto** e «*ad altre autorità incaricate dell'applicazione della legge*» a prevenzione e tutela degli interessi della società tanto da, quindi, ulteriormente scollegare il detto concetto di dato di reato sia dall'accertamento giudiziale (ed anzi, addirittura, dalla previa conoscenza della rilevanza penalistica dello stesso), sia da quelle autorità istituzionali che, a vari livelli, possono contribuire ad accertarlo, ovvero a **preliminarmente valutarlo**.

Il considerando n. 13 della Direttiva si riferisce al reato quale «*concetto autonomo*» del diritto dell'Unione Europea e, oltretutto, sia gli artt. 6 e 7 della stessa, che l'art. 4 del Dlgs n. 51/2018, pongono la eloquente distinzione tra categorie di interessati al trattamento di dati di reato (rei; potenziali rei; vittime; persone informate) e tra dati afferenti a reati fondati su fatti e dati basati su valutazioni personali ivi ponendo un obbligo di distinzione tra gli uni e gli altri.

Ed ancora, l'art. 3, parag. 7, lett. b, della citata Direttiva, nonché l'art. 2, parag. 1, lett g 2 del Dlgs n.51/2018, com e visto, si riferiscono alle “autorità competenti” anche rispetto a «*qualsiasi altro organismo o entità incaricato dagli ordinamenti interni di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagini, accertamento e perseguimento di reati//*» con ciò, pertanto, erodendo definitivamente "l'egemonia" nel possibile trattamento di “dati di reato” che si poteva in tale materia attribuire alle (sole) forze di polizia o autorità pubbliche intese in senso meramente istituzionale.

TRATTARE I DATI PERSONALI DI REATO

Detto questo, a tal punto, occorre una sintesi esemplificativa che dovrebbe permettere di ancor meglio centrare l'argomento in parola e le delicate, sempre più estese e trascurate criticità che lo stesso porta con sé.

Invero, se rimane indubbio che le forze dell'ordine italiane oggi applicano il menzionato Dlgs n. 51/2018 nel mentre eseguono, ad esempio, l'identificazione o l'arresto di una persona per porre in esecuzione un ordine giudiziario relativo alla commissione di un reato, da un altro angolo visuale esiste un ampio (sempre più vasto, in realtà) ambito di

trattamento "atipico" di **"dati di reato"** (nel senso giuridico-umanistico del termine) che sfugge a tale pacifica ipotesi applicativa e che non costituisce affatto un mero esercizio di teorica scolastica, o di fantasia.

E poiché per reato, come accennato, si può e si deve in generale intendere "*un fatto umano antigiuridico a cui un ordinamento ricollega una sanzione penale*" ecco che, allora, niente esclude che anche chi non fa parte delle forze dell'ordine (o non sia un operatore professionale del diritto o un investigatore) si trovi spesso a poter trattare (comunicare, diffondere, appostare) dati di reato concernenti persone fisiche identificate o identificabili.

Al riguardo non pare possibile sbrigativamente "licenziare" l'argomento sostenendo che il dato di reato consisterebbe solo in quel dato "assistito/caratterizzato" da una sentenza penale di condanna, ovvero che sia tale solo se trattato da parte dell'autorità.

Questa visione sarebbe davvero limitata, limitativa e, peraltro, nemmeno corrispondente al contenuto e significato (letterale e comprensibile) della normativa europea che, notoriamente, andrebbe in ogni caso interpretata estensivamente e non in modo restrittivo ovvero, ancor peggio, "miope".

Sovviene al proposito il "**caso *František Ryneš***" (richiamato anche dalle menzionate Linee Guida n. 3/2019 dell'EDPB), ove la Corte di Giustizia UE si è occupata dei dati raccolti da un proprietario di una abitazione che aveva ripreso con il sistema di sorveglianza domestico (CCTV) l'immagine riconoscibile (e, poi, difatti, identificata) di chi gli stava mandando in frantumi alcune finestre.

La CGUE ha stabilito che la videosorveglianza con registrazione e conservazione di tali dati personali costituisce

trattamento automatico di dati (sentenza C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, del 11/12/2014).

Ma ciò che occorre chiedersi per quanto riguarda il tema in argomento è se il suddetto trattamento (indubbiamente) di dati costituisca oggi, anche, un **“trattamento di dati personali di reato”?**

A questa domanda si dovrebbe rispondere di sì poiché, a sommesso avviso di chi scrive, un simile caso di trattamento costituisce in primo luogo la video-ripresa di un fatto umano (riconducibile a persone identificabili) antigiuridico, contrastato e precettato dalla legge penale a cui il/un legislatore ricollega (o può ricollegare) come conseguenza una pena, ovvero una sanzione.

Ma si pensi anche al caso in cui un negoziante video-riprenda una persona che, a viso scoperto, sia intenta a scassinargli il negozio prima di fuggire e che, poi, tale filmato, venga trasmesso al proprietario dell'esercizio commerciale adiacente per permettergli di capire se si fosse trattato del medesimo ladro che il mese prima lo aveva derubato ed era stato solo parzialmente immortalato di spalle (anche) dalle telecamere installate in tale secondo negozio.

Si tratta di esempi reali, il cui **accadimento concreto è molto meno raro di quello che si potrebbe immaginare**.

Anzi, oggi, sono fattispecie da considerarsi diffusissime in tutta Europa e, non a caso, riprese anche nelle citate linee guida n. 3/2019 (adottate in data 29/01/2020) del Comitato Europeo Per la Protezione dei dati (ex art. 68 del GDPR) riguardanti la “video-audio ripresa”.

LE LINEE GUIDA EDPB N. 3/2019 CI POSSONO AIUTARE?

Si tratta di Linee guida che, oltre a riprendere alcuni argomenti già resi oggetto del Provvedimento del Garante Italiano in data 08/04/2010[11], contengono vari spunti sull'argomento, spesso interessanti, altre volte curiosi, altre ancora solo accennati, ma che, in ogni caso, fanno capire come il tema relativo al trattamento **"atipico"** dei "dati di reato" da parte di chi non è, o non è *tout court* «*autorità competente*» (*ex* Dlgs n. 51/2018) o «*autorità pubblica*» (*ex* art. 10 GDPR), sia sempre più meritevole di attenzione e, soprattutto, necessiti di specifici approfondimenti giuridici *ad hoc* e, forse, di più esaustive prescrizioni appositamente dedicate ad esso (senza qui voler mettere in discussione i responsabilizzanti principi del "*case by case*" che caratterizzano tutta la normativa europea in materia di trattamento dati personali).

Le dette Linee guida n. 3/2019, ad esempio, al parag. 4.2, si occupano (in modo apparentemente "sbrigativo") della «*divulgazione di filmati alle forze dell'ordine*» ivi indicando e spiegando con due esempi quanto segue.

La divulgazione come "trattamento dati" è definita all'articolo 4, paragrafo 2, GDPR, come trasmissione (ad es. comunicazione individuale), diffusione (ad esempio, la pubblicazione online) o la messa a disposizione in altro modo.

---

[11] Cfr. Provvedimento del Garante Privacy in data 08/04/2010, pubblicato nella G.U. n. 99 del 29/04/2010 (senza qui dimenticare il precedente provvedimento generale dell'aprile 2004 che, per quanto compatibile, non è da ritenersi per nulla abrogato).

I terzi sono definiti all'articolo 4, paragrafo 10, GDPR (inoltre, il WP Group 29 ha adottato delle specifiche linee guida al riguardo).

Ad ogni modo, qualsiasi divulgazione di filmati contenenti dati personali deve avere una specifica base giuridica (Articolo 6, paragrafo 4, GDPR).

Esempio: un titolare che desideri caricare una registrazione su Internet deve fare affidamento su una base giuridica per tale trattamento, ad esempio ottenendo il consenso dell'interessato secondo Articolo 6, paragrafo 1, lettera a), GDPR.

La stessa valutazione deve essere effettuata dal destinatario che, in particolare, dovrà identificare la sua base giuridica ai sensi dell'Articolo 6 (ad esempio la ricezione del materiale).

Esempio: il sistema di videosorveglianza posto su una barriera all'ingresso di un parcheggio è stata installata con lo scopo di risolvere eventuali richieste di risarcimento danni. Si verifica un danno e la registrazione viene trasferita ad un avvocato per seguirne il caso. In questo caso la finalità della registrazione è il trasferimento del dato personale contenuto nella registrazione.

Laddove nella medesima situazione, però, la registrazione venisse pubblicata online per puro divertimento, in questo caso la finalità sarebbe diversa e non sarebbe compatibile con la finalità iniziale. Inoltre, sarebbe problematico identificare una base giuridica per tale trattamento (pubblicazione) e si potrebbe immaginare il consenso dell'interessato».

Ben chiare spiegazioni esemplificative queste, che, tuttavia, **lambiscono ma non toccano il vero problema** e, quindi, non permettono nemmeno di porsi nell'ottica di

cominciare ad affrontare la sottesa attuale tematica (e, anzi, a loro volta, fanno sorgere diversi interrogativi ad esempio relativamente alle indicate pubblicazioni *on line* di dati [di reato?] basate sul consenso).

E ciò parrebbe vero soprattutto se tali "sbrigativi" accenni si volessero utilizzare per interpretare correttamente la normativa di complessivo riferimento, tenendo conto della attuale assai vasta realtà con cui, di fatto[12], ogni giorno i c.d. "dati personali di reato" vengono direttamente o indirettamente trattati da parte di una sempre più amplia platea di soggetti pubblici e privati in tutta l'Unione Europea.

[12] Realtà in cui, come detto, sono diventate numerosissime le persone che, quotidianamente, praticano ad esempio la sicurezza urbana partecipata con le forze dell'ordine locali in attuazione di un modello europeo finalizzato alla prevenzione dei reati nei quartieri residenziali (anche) mediante il trattamento "atipico" di quantità sempre più importanti di dati di reato riferibili a persone fisiche: e ciò, va ripetuto, si verifica al di là dei casi già pacificamente soggetti all'applicazione della Dir. UE n. 2016/680, ovvero, per meglio dire, delle normative nazionali di recepimento della stessa (Dlgs n. 51/2018). A fronte di questo fenomeno (sociale non più trascurabile) occorrerebbe, quindi, una celere, approfondita e condivisa analisi costruttiva (in primo luogo giuridica, prima ancora che sociologica o, persino, "criminologica") di tale realtà europea composta, ad oggi, da milioni di persone che si dedicano volontaristicamente alle necessarie (nobili) pratiche conosciute in Italia con il nome di Controllo del Vicinato.