La videosorveglianza nei condomini e la tutela della privacy secondo il diritto UE

di Francesco Santolini

Title: Video surveillance in residential buildings and data protection according to EU law

Keywords: Video surveillance; Data protection; Dir. 95/46/EC and GDPR.

1. – Con sentenza dell'11 dicembre 2019, la Terza Sezione della Corte di giustizia dell'Unione europea si è espressa circa la compatibilità con la normativa europea in materia di trattamento dei dati personali di una legislazione nazionale che, per finalità di sicurezza degli abitanti, permette l'installazione di un sistema di videosorveglianza nelle parti comuni di un immobile ad uso abitativo anche senza il consenso di alcuni condomini.

Nello specifico, oggetto della domanda di pronuncia pregiudiziale era l'interpretazione della direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Come premesso dai giudici di Lussemburgo, la sentenza, tenuto conto della data dei fatti oggetto della controversia, concerne una normativa attualmente abrogata e sostituita, a far data dal 25 maggio 2018, dal regolamento UE 2016/679 del Parlamento europeo e del Consiglio, più noto come General Data Protection Regulation (GDPR). Interessante sarà quindi esaminare quanto la pronuncia mantenga elementi di rilevanza anche nell'attuale contesto normativo.

Da tenere presente, ai fini di una migliore comprensione di quanto segue, che nella direttiva 95/46/CE si utilizzava la locuzione «responsabile del trattamento» per definire chi «determina le finalità e gli strumenti del trattamento dei dati personali», denominato nel GDPR «titolare del trattamento».

2. – Il caso che ha originato il rinvio pregiudiziale è il seguente. In un immobile sito in una città della Romania la «associazione dei comproprietari» ha deliberato, nell'aprile 2016, l'installazione di telecamere di sorveglianza, che poco tempo dopo, sono state posizionate in vari punti dell'edificio in cui maggiore era il passaggio di persone.

TK, proprietario di uno degli appartamenti e ivi residente, si è opposto all'introduzione della videosorveglianza nel palazzo, sostenendo che essa violasse il diritto al rispetto della vita privata. Dal momento che, nonostante i ripetuti solleciti e finanche il riconoscimento scritto dell'illegittimità dell'installazione da parte dell'assemblea stessa che l'aveva deliberata, il sistema continuava a funzionare, TK ha

ISSN: 2037-6677

adito il Tribunale superiore di Bucarest, affinché ingiungesse la rimozione definitiva delle telecamere.

Dinanzi al giudice di merito, l'attore ha dedotto la violazione sia del diritto al rispetto della vita privata, sancito dal diritto primario e dal diritto derivato dell'UE, sia della normativa nazionale in materia e ha inoltre lamentato l'assunzione, da parte dell'associazione dei comproprietari, della funzione di responsabile del trattamento dei dati personali senza aver seguito l'iter previsto dalla legge.

La parte convenuta ha in primo luogo dato conto del fatto che si era deciso di installare un sistema di sorveglianza per controllare il più efficacemente possibile le entrate e le uscite dall'immobile, a seguito di numerosi atti vandalici nei confronti degli spazi comuni e di furti nelle private abitazioni, e tenuto altresì conto che altre misure, meno invasive, in precedenza adottate non erano riuscite a impedire la commissione degli atti illeciti. Ha inoltre presentato in giudizio documentazione atta a dimostrare la disinstallazione delle videocamere e l'avvenuta cancellazione delle immagini registrate, nonché di aver nel frattempo completato le procedure necessarie per poter assumere le funzioni di responsabile del trattamento dei dati personali.

Il giudice del rinvio ha in primo luogo rilevato che la legge nazionale (l. 677/2001), approvata in attuazione della direttiva 95/46/CE, in via generale prevede che un trattamento di dati personali, come la registrazione di immagini mediante un sistema di videosorveglianza, possa avvenire solo con il consenso esplicito e inequivocabile delle persone interessate. La stessa legge contiene però delle eccezioni, tra le quali il caso in cui il trattamento dei dati sia necessario per la tutela della vita, dell'integrità fisica o della salute delle persone interessate o di altri, ribadita tra l'altro pure dall'Autorità garante della protezione dei dati personali rumena in una propria decisione. Altra disposizione considerata è l'art. 52, par. 1 della Carta dei diritti fondamentali dell'UE, che sancisce la necessità di un rapporto di proporzionalità tra le finalità che consentono di limitare i diritti e i mezzi utilizzati allo scopo.

Il Tribunale superiore di Bucarest, avendo osservato che il sistema di videosorveglianza oggetto della controversia non appariva avere obiettivi differenti da quelli dichiarati dall'associazione dei comproprietari, cioè la tutela della vita, dell'integrità fisica e della salute dei comproprietari stessi, ha deciso di sollevare varie questioni pregiudiziali di interpretazione aventi ad oggetto disposizioni della direttiva (artt. 6, par. 1 e 7, lett. f) e della Carta dei diritti fondamentali (artt. 8 e 52) pertinenti con il caso di specie, onde verificare la compatibilità con esse della normativa nazionale.

3. – La Corte di giustizia, effettuata una ricognizione delle varie disposizioni normative di diritto primario e derivato delle quali è stata chiesta la corretta interpretazione, ha in primo luogo affermato che con le questioni poste, da esaminare congiuntamente, il giudice del rinvio ha in sostanza chiesto se gli artt. 6, par. 1, lett. c) (che stabilisce che i dati personali debbono essere «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati») e 7, lett. f) (che prescrive che il trattamento dei dati personali può essere effettuato quando «è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1») della direttiva 95/46/CE, letti alla luce degli artt. 7 (che sancisce il diritto al rispetto della vita privata e familiare) e 8 (concernente la protezione dei dati personali) della CDF dell'UE, siano da interpretare in senso ostativo a «disposizioni nazionali, le quali autorizzino la messa in opera di un sistema di videosorveglianza, come il sistema controverso nel procedimento principale, installato nelle parti comuni di un immobile ad uso abitativo, al fine di perseguire legittimi interessi consistenti nell'assicurare la sicurezza e la tutela delle persone e dei beni, senza il consenso delle persone interessate».

I giudici di Lussemburgo hanno quindi proceduto a fornire al giudice del rinvio i criteri per inquadrare normativamente i fatti oggetto della controversia, ricordando che, ai sensi dell'art. 3, par. 1 della direttiva 95/46/CE e come risulta dalla propria giurisprudenza (Corte giust. UE, sent. 11 dicembre 2014, Ryneš, C-212/13, pt. 25) un sistema di videosorveglianza mediante telecamere costituisce un trattamento di dati personali automatizzato, e quindi ricade nel campo di applicazione della direttiva, qualora permetta di registrare e stoccare dati personali, quali per esempio immagini che consentano di identificare persone.

La Corte ha poi rammentato che qualsiasi trattamento di dati personali per essere considerato legittimo deve sia essere conforme ai principi relativi alla qualità dei dati, di cui all'art. 6 della direttiva, sia rientrare in uno dei casi, previsti in modo esaustivo e tassativo dall'art. 7 della direttiva, per cui è legittimo trattare dati personali (cfr. da ultimo Corte giust. UE, sent. 13 maggio 2014, Google Spain e Google, C-131/12, pt. 71), senza che vi sia possibilità per gli Stati membri di estendere la portata di detti principi o aggiungerne di nuovi (Corte giust. UE, sent. 19 ottobre 2016, Breyer, C-582/14, pt. 57).

Con riferimento alla normativa applicabile alla fattispecie controversa, la Corte ha rilevato che un trattamento dati è lecito, in conformità al principio di cui alla lett. f) dell'art. 7 della direttiva, quando esso i) persegue un interesse legittimo del responsabile del trattamento o dei terzi a cui vengono comunicati i dati, ii) è necessario per la realizzazione di detto interesse e iii) su quest'ultimo non prevalgono diritti e libertà delle persone interessate dalla protezione dei dati (cfr. anche Corte giust. UE, sent. 04 maggio 2017, Rīgas satiksme, C-13/16, pt. 28), senza che occorra il consenso della persona interessata.

Entrando in modo più specifico nel caso da cui è scaturito il rinvio, i giudici di Lussemburgo hanno ritenuto qualificabile come legittimo interesse l'obiettivo – di protezione dei beni, della vita e della salute dei comproprietari – perseguito dall'associazione degli stessi, responsabile del trattamento, e che quindi sia soddisfatta la prima condizione prevista dall'art. 7, lett. f) della direttiva (cfr. anche Corte giust. UE, sent. Ryneš cit., pt. 34). In risposta a una delle questioni poste dal giudice del rinvio, hanno poi rilevato che, come anche fatto valere da alcuni Governi nazionali e dalla Commissione, il legittimo interesse deve essere esistente e attuale al momento del trattamento, senza però spingersi fino a richiedere che in passato sia già stato arrecato un pregiudizio alla sicurezza dei beni e delle persone, e che, nel caso di specie, le pregresse vicende di furti e atti vandalici soddisfano il requisito richiesto.

Con riferimento alla seconda condizione, la Corte ha ricordato che le deroghe e le restrizioni al principio della tutela dei dati personali debbono avvenire nei limiti dello stretto necessario (cfr. da ultimo Corte giust. UE, sent. Rīgas satiksme cit., pt. 30) e che, pertanto, il giudice del rinvio deve verificare che gli obiettivi legittimamente perseguiti mediante la videosorveglianza non possano essere raggiunti con mezzi altrettanto efficaci ma meno pregiudizievoli per i diritti al rispetto della vita privata e alla tutela dei dati personali; inoltre occorre considerare il criterio di stretta necessità unitamente a quello della minimizzazione dei dati, di cui all'art. 6, par. 1, lett. c) della direttiva, secondo il quale i dati personali devono essere «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o vengono successivamente trattati». Relativamente al caso di specie, appaiono rispettati i due elementi, perché da un lato misure di sicurezza meno invasive precedentemente messe in atto si erano rivelate insufficienti e dall'altro la videosorveglianza è limitata ad alcune parti comuni e agli accessi dell'immobile; si è però evidenziata la necessità che il responsabile del trattamento imposti secondo i parametri citati le concrete modalità di funzionamento dei dispositivi di videosorveglianza.

Circa la terza condizione prevista dalla lett. f) dell'art. 7 della direttiva, i giudici di Lussemburgo hanno rammentato la necessità che sulla base delle circostanze concrete venga fatta una ponderazione degli opposti diritti e interessi in gioco, senza

ISSN: 2037-6677

che sia possibile stabilire a priori l'esclusione generalizzata di alcune categorie di dati dal trattamento (Corte giust. UE, sent. Breyer cit., pt. 62). Da una parte occorre tener conto della gravità del pregiudizio ai diritti e alle libertà delle persone interessate – per la cui valutazione si devono considerare la natura dei dati personali, le tipologie del trattamento, con specifico riferimento al numero di soggetti che possono avere accesso e alle concrete modalità dello stesso e le ragionevoli aspettative dell'interessato in merito alla possibilità o meno che abbia luogo un trattamento – e dall'altra l'importanza dei legittimi interessi perseguiti mediante il trattamento.

4. – In conclusione, la Corte di giustizia ha affermato che «l'articolo 6, paragrafo 1, lettera c), e l'articolo 7, lettera f), della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, letti alla luce degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, devono essere interpretati nel senso che essi non ostano a disposizioni nazionali, le quali autorizzino la messa in opera di un sistema di videosorveglianza, come il sistema controverso nel procedimento principale installato nelle parti comuni di un immobile ad uso abitativo, al fine di perseguire legittimi interessi consistenti nel garantire la sicurezza e la tutela delle persone e dei beni, senza il consenso delle persone interessate, qualora il trattamento di dati personali effettuato mediante il sistema di videosorveglianza in parola soddisfi le condizioni enunciate nel succitato articolo 7, lettera f), aspetto questo la cui verifica incombe al giudice del rinvio».

5. – Come già evidenziato da altri autori, la tematica della tutela dei dati personali ha assunto nell'Unione europea una portata strategica (cfr., per esempio, A. Correra, Dati personali: un cantiere aperto e in continua evoluzione, in questa Rivista, 1/2018, 211 ss.). Già a partire dagli anni '90 l'UE ha regolamentato i vari aspetti della materia mediante fonti di diritto derivato (tra cui si ricordano, oltre alla già menzionata direttiva 95/46/CE sulla protezione dei dati; il regolamento CE n. 45/2001 sul trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari; la direttiva 2002/58/CE sull'e-privacy, modificata nel 2009; la direttiva 2006/24/CE sulla conservazione dei dati, dichiarata successivamente invalida) e, come visto sopra, finanche introducendo nella Carta dei diritti fondamentali, all'art. 8, il diritto alla protezione dei dati di carattere personale. Contestualmente, la crescente richiesta di protezione dei dati combinata con un'evoluzione tecnologica sempre più pervasiva ha indotto la Corte a pronunciarsi ripetutamente sull'argomento, giungendo a più di dieci sentenze nel biennio 2014-2015. Da ultimo il 27 aprile 2016 sono stati approvati due atti normativi, entrambi del Parlamento europeo e del Consiglio: il già noto e citato regolamento UE 2016/679, entrato in vigore nel maggio 2018, che ha abrogato la direttiva 95/46/CE, e la direttiva UE 2016/680, relativa al trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (che ha abrogato la decisione quadro 2008/977/GAI del Consiglio).

Tra le altre cose, i giudici di Lussemburgo molto spesso, come nella sentenza in esame, mettono in stretta connessione il diritto alla protezione dei dati personali (art. 8 CDFUE) con quello al rispetto della propria vita privata e familiare (art. 7 CDFUE).

La tematica della videosorveglianza è, inoltre, quanto mai attuale, non solo in ambito strettamente UE: non può non citarsi, sia pure senza addentrarsi ad esaminarla, la sentenza della Corte europea dei diritti dell'uomo del 17 ottobre 2019 (ricorsi n. 1874/13 e 8567/13, Lopez Ribalda e altri c. Spagna) in merito alle riprese sul luogo di lavoro, la quale, nonostante riguardi una fattispecie differente da quella che oggi qui si commenta, contiene degli utili spunti. La pronuncia – che si inserisce nel nutrito filone

giurisprudenziale riguardante la compatibilità dei controlli a distanza, mediante l'utilizzo della tecnologia, sui lavoratori con l'art. 8 della CEDU, che sancisce il diritto al rispetto della vita privata e familiare (ex multis: sentt. Corte EDU 9 gennaio 2018, López Ribalda c. Spagna n. 1; 18 novembre 2017, Antović e Mirković c. Montenegro; 5 settembre 2017, Bărbulescu c. Romania; 5 ottobre 2010, Köpke c. Germania) – è significativa nella parte in cui ribadisce varie esigenze: che si operi un bilanciamento degli interessi concorrenti, nel caso di specie il diritto al rispetto della vita privata dei lavoratori e la possibilità, per il datore di lavoro, di proteggere i propri beni e l'efficienza dell'azienda; che i mezzi approntati siano proporzionati e appropriati rispetto agli obiettivi perseguiti; che vengano ben circoscritte le modalità di effettuazione della videosorveglianza e della successiva fruizione delle immagini registrate.

Inoltre, giova osservare, in una prospettiva più ampia, che la fattispecie oggetto della sentenza in esame non riguarda esclusivamente la protezione dei dati personali e della vita privata, ma concerne la sempre avvertita esigenza di bilanciamento tra riservatezza e sicurezza, entrambi interessi meritevoli di tutela ma spesso confliggenti.

Si può quindi a ragione sostenere che la pronuncia della Corte di giustizia si occupi di questioni di significativa importanza e rilevanza nel momento presente.

6. – Si evidenzia che i principi relativi in generale al trattamento dei dati personali e quelli concernenti nello specifico la sua liceità elencati nella direttiva sono stati trasfusi anche nel GDPR e, quindi, i ragionamenti svolti nella sentenza in esame preservano una loro attualità anche sotto la vigenza della nuova normativa. Nonostante la sentenza non abbia trattato tale aspetto, essendosi occupata solo delle questioni relative alla legittimazione del trattamento, occorre ricordare che, ovviamente, anche per la videosorveglianza si applicano le disposizioni circa l'informativa da fornire agli interessati e i diritti degli stessi.

Esaminando nello specifico i profili giuridici rilevanti, la Corte di giustizia ha ribadito in modo molto chiaro e preciso, come risulta dall'esposizione di cui sopra, con quali modalità sia possibile installare nei condomini un sistema di videosorveglianza nel rispetto delle disposizioni UE in materia di tutela dei dati personali, le quali vanno lette anche alla luce del diritto al rispetto della vita privata. In particolare, l'attenzione si è focalizzata sulla corretta interpretazione della condizione di cui all'art. 7, lett. f) della direttiva 95/46/CE, che, ricordiamo, prescrive – analogamente a quanto attualmente stabilito dall'art. 6, par. 1, lett. f) del GDPR – che il trattamento dei dati personali può essere effettuato quando «è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1».

Per ritenere lecita la videosorveglianza nelle parti comuni dei condomini si è confermata la necessità di verificare nel concreto la contemporanea sussistenza di tre elementi: la legittimità dell'interesse perseguito da chi mette in atto il trattamento, la circostanza che i legittimi interessi di cui sopra non possano essere realizzati con misure meno invasive, l'adeguato contemperamento degli interessi prefissati con i diritti degli altri soggetti coinvolti, tenuto conto di tutte le circostanze del caso.

L'intervento della Corte, tra l'altro su una fattispecie fattuale piuttosto diffusa nel vivere quotidiano dei cittadini europei, è quanto mai utile – e ancor di più in un contesto normativo come quello antecedente al GDPR e oggetto della sentenza, in cui in ogni Stato vigeva una differente normativa nazionale di recepimento della direttiva – per assicurare in modo uniforme la corretta interpretazione e attuazione da parte degli operatori del diritto delle disposizioni sovranazionali e garantire i diritti fondamentali su cui esse si fondano.

ISSN: 2037-6677

7. – Ai fini di una più completa analisi della materia e in continuità sia sostanziale sia cronologica con quanto disposto dalla sentenza, è di qualche utilità dar conto di profili che nel momento attuale stanno interessando i cittadini e gli Stati dell'Unione europea.

In primo luogo, occorre focalizzarsi su alcune novità del GDPR: l'introduzione del principio c.d. di «accountability» o «responsabilizzazione» che grava sul titolare del trattamento, che, ai sensi dell'art. 5, par. 2, è competente per il rispetto dei principi applicabili al trattamento e deve essere in grado di comprovarlo, cioè di dare evidenza dell'efficacia delle misure adottate; i principi di «data protection by design e by default» di cui all'art. 25; l'obbligo, contenuto nell'art. 35, di effettuare una «valutazione d'impatto sulla protezione dei dati» quando il trattamento prevede l'uso di nuove tecnologie e può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità; una formulazione della disposizione riguardante la sicurezza del trattamento (art. 32) maggiormente estensiva e articolata rispetto a quella analoga contenuta nella direttiva (art. 17).

Tutti questi argomenti sono rilevanti per l'installazione di un sistema di videosorveglianza e andranno nel futuro tenuti in adeguata considerazione.

In secondo luogo, entrando ancor più nello specifico, troveranno applicazione le «Guidelines 3/2019 on processing of personal data through video devices». Esse, dopo essere state approvate in una prima versione il 10 luglio 2019 e sottoposte a consultazione pubblica fino al successivo 9 settembre, il 29 gennaio scorso sono state adottate in via definitiva dal Comitato europeo per la protezione dei dati, il quale, come noto, è un organismo dell'Unione, dotato di personalità giuridica, istituito e disciplinato dal capo VII, sezione 3 (artt. 68-76) del GDPR, è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti e ha il compito di garantire l'applicazione coerente del regolamento, attraverso attività di monitoraggio, consulenza, adozione di linee guida, raccomandazioni e migliori prassi, redazione di pareri e relazioni annuali.

Le linee guida costituiscono il primo documento europeo che applica i principi del GDPR al trattamento dei dati effettuati tramite riprese video. Esse tengono conto del fatto che l'installazione di sistemi di videosorveglianza può essere utile per soddisfare esigenze di sicurezza ma anche comportare che i dati raccolti vengano utilizzati per differenti e meno gradite finalità (per esempio, controllo dei lavoratori, marketing) e che tali rischi sono amplificati dall'evoluzione tecnologica. Non c'è dubbio che emergano significativi problemi di tutela della privacy e della vita privata, i quali rendono opportuno avvalersi della videosorveglianza in via residuale, solo se non esistono altri mezzi per raggiungere lo scopo.

Le linee guida prevedono circostanze nelle quali non trova applicazione il GDPR: situazioni in cui la videosorveglianza, per le sue caratteristiche, non consente l'identificazione dei soggetti (telecamere finte o riprese effettuate a eccessiva distanza o con modalità particolari) e i casi di c.d. «esenzione domestica» («household exception»), cioè video realizzati in ambito familiare e fruibili solo in quel contesto, senza diffusione a un numero indeterminato di persone, o riguardanti solo la propria proprietà privata, senza estensione neanche parziale a spazi pubblici o di altri privati.

Per quanto riguarda la legittimazione al trattamento dei dati, non è sufficiente che ci si riferisca genericamente a esigenze di sicurezza, ma occorre indicare precisamente quale delle condizioni di liceità del trattamento di cui all'art. 6, par. 1 del GDPR sussista, tenendo a mente che il consenso dell'interessato può essere invocato solo in casi eccezionali e comunque deve essere prestato in modo libero ed esplicito. Il legittimo interesse, che risulta essere la situazione maggiormente ricorrente nella prassi, deve essere sempre reale e attuale. Prima dell'installazione, è obbligatorio dimostrare che il sistema di videosorveglianza sia idoneo a raggiungere l'obiettivo perseguito e a ciò necessario, potendo essere scelto solo se detto scopo non può ragionevolmente essere realizzato con altri mezzi meno restrittivi dei diritti e delle

libertà individuali. Comunque la videosorveglianza deve limitarsi, dal punto di vista spazio-temporale, al minimo indispensabile.

Le linee guida affermano inoltre l'obbligatorietà di un bilanciamento tra gli interessi coinvolti, per esempio tra la protezione di persone e beni da una parte e i diritti dei soggetti i cui dati vengono trattati dall'altra. Il bilanciamento deve avvenire caso per caso e non in astratto e tener conto di vari elementi: la tipologia e il quantitativo dei dati trattati, la portata spazio-temporale, la natura e le finalità del trattamento, la ragionevole prevedibilità di essere ripresi in quelle circostanze.

Qualsiasi diffusione ad altri soggetti delle videoriprese effettuate necessita di una propria legittimazione ai sensi dell'art. 6 del GDPR, con alcune agevolazioni nel caso in cui lo scopo perseguito sia il medesimo. L'accesso da parte delle forze di pubblica sicurezza generalmente ha un suo autonomo fondamento giustificativo ai sensi dell'art. 6, par. 1, lett. c) del GDPR.

Se la videoregistrazione comporta il trattamento di dati sensibili trova applicazione l'art. 9 GDPR.

Le linee guida prevedono poi in capo agli interessati i diritti di accesso, cancellazione e opposizione; stabiliscono obblighi di trasparenza e informazione, compresa la disciplina dei segnali di avvertimento e delle ulteriori informazioni da rendere disponibili, ai sensi degli artt. 12 e seguenti del GDPR; impongono una conservazione delle immagini registrate limitatamente al tempo strettamente necessario alle finalità perseguite, prevedendo la necessità di motivazione nel caso si ecceda le 72 ore e indicando, a titolo esemplificativo, per le riprese introdotte per fronteggiare atti di vandalismo o furti nei confronti di proprietà di dimensioni contenute, una durata di 24 ore, salvo situazioni eccezionali. Infine, le linee guida evidenziano l'esigenza di adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, come previsto dall'art. 32 del GDPR, di rispettare i principi di «data protection by design e by default» di cui all'art. 25 del GDPR e di procedere alla valutazione d'impatto sulla protezione dei dati («data protection impact assessment») quando ricorrono le condizioni e secondo le modalità di cui all'art. 35 del GDPR.

Questa breve esposizione delle novità nel frattempo intervenute sull'argomento è utile sia a riprova dell'avvertita necessità di una regolamentazione uniforme su tutto il territorio dell'Unione della materia della videosorveglianza che tenga in adeguata considerazione le esigenze di tutela della privacy sia a dimostrare l'attualità delle considerazioni svolte dalla Corte di giustizia al proposito. Come già evidenziato, l'Unione europea tramite i suoi organi, legislativi e giurisdizionali, è da tempo impegnata a garantire la protezione dei dati personali, che costituisce un vero e proprio diritto dei cittadini, e ad approntare e incrementare gli strumenti più idonei allo scopo, quanto mai necessari in un mondo interconnesso in cui la tecnologia è sempre più pervasiva. Nello stesso tempo, nel concreto vivere quotidiano è costantemente necessario un contemperamento tra questo importante diritto e altri diritti e interessi, parimenti meritevoli di tutela, come delinato nella sentenza in esame.

Francesco Santolini
Dip.to di Giurisprudenza
Università degli Studi di Genova
fra.santolini@gmail.com