

# THE VIDEO SURVEILLANCE MATTER IN THE CASE-LAW OF THE EUROPEAN COURT OF JUSTICE

Cornelia Beatrice Gabriela ENE-DINU\*

## Abstract

*Nowadays, the personal data protection issue is becoming more and more prominent, both in the state institutions and in the private sector. The economic agents and public institutions are required to follow clear rules in what concerns the personal data processing both in terms of the employees and in terms of the individual requesting access to certain goods or services. However, how do we appreciate the concept of personal data protection when balanced with the protection of life, personal property or privacy? This question is becoming more and more present and the answer is absolutely required when we discuss about the video surveillance of living spaces, courtyards and common use space or private parking. Another sensitive aspect interferes when video surveillance involves an area of public space.*

**Keywords:** *personal data protection, monitoring, protection of life, protection of property, video surveillance, legitimate interest, proportionality.*

## 1. Terminological matters

In terms of the personal data processing, the legitimate interest is the most flexible to the processing subject, but the choice of this subject should be appropriate and adjusted to each type of processing. The legitimate interest is an appropriate basis for processing when data subjects reasonably expect that the use of their personal data and the processing thereof have a minimal impact on privacy. If the data controller chooses to process personal data on the basis of the legitimate interest, it must undertake the responsibility to protect the rights and interests of the individuals.

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) provides in article 6 paragraph (1) letter (f) a basis for processing

where: *“Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”*

The concept of legitimate interest referred to in Regulation (EU) 2016/679, entails a wide range of concepts, from personal or third-party interests, commercial interests, as well as social benefits. GDPR specifically mentions the use of data on customers or employees, marketing, fraud prevention, inter-group transfers or IT security as potential legitimate interest. At the same time, it can be stated that there is a legitimate interest when information on potential criminal activities or security threats is disclosed to the authorities. As it could be applied in a wide range of circumstances, it is up to the data controller to balance own legitimate interests and the

---

\* Lecturer, PhD, Faculty of Law, “Nicolae Titulescu” University (e-mail: cdinu@univnt.ro).

need to process personal data against the interests, rights and freedoms of the individual, by taking into account the particular circumstances of the case. To demonstrate a legitimate interest requires to demonstrate that the controller (or a third party) has a certain clear or specific benefit from the processing of the data. It is not sufficient for the processing to be based on vague or generic interests, its purpose and the desired result must be precisely identified. Although any purpose can be relevant, this purpose must be “legitimate”. Any unethical or illegal interest is not a legitimate interest.

The “necessary processing” is another concept the European legislation in the field of the personal data processing operates with, a relevant concept in this study. This concept of “necessary processing” applies to situations where the use of personal data is made for the purpose of the identified legitimate interests. This does not mean that it must be absolutely essential, but it must be a pursued and proportionate way of achieving the goal. It must be analyzed on a case-by-case basis whether the processing is proportionate and appropriate to achieve its purposes and whether there is a less intrusive alternative, so that the purpose to be achieved by other reasonable means, without processing the data in this way. A very clear difference must be made between the processing which is necessary for the established purpose and the processing which is necessary only due to the method chosen to pursue that purpose. In the background of certain legitimate interests, it may be argued that certain non-essential matters of processing are required in order to achieve the purposes. However, this is valid only if the specific purpose behind these features is clearly identified and the processing is not disguised behind a business

purpose that could be achieved in another way. The processing must be necessary for the specific purpose. If we cannot demonstrate that the processing really helps to achieve the legitimate interest, then we cannot discuss the concept of “necessary processing”. Furthermore, if the processing is not a reasonable way of achieving the targeted purpose, the concept of legitimate interest does not apply.

## **2. The ECOJ practice relevant in the field of the video surveillance**

**2.1.** Firstly, we will try to analyze a ECOJ Judgment<sup>1</sup> on the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space. It should be noted that the case was settled by the Court before the entry into force of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC but it is of practical importance in terms of the way in which the Court analyzed and interpreted concepts applicable in the field of personal data protection, also regulated in the current normative act. The circumstances of the case are extremely common in practice, so that it is useful to know the opinion of the ECOJ in this area.

The subject of the case is the request for a preliminary ruling under article 267 TFEU filed by the Supreme Administrative Court (Czech Republic) concerning the interpretation of article 3 paragraph (2) of

<sup>1</sup> ECOJ, Judgment of the Court (Fourth Chamber) Case C-212/13.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995<sup>2</sup> on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article 3 of the aforementioned directive provides the following: “(1) This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. (2) This Directive shall not apply to the processing of personal data: - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law; - by a natural person in the course of a purely personal or household activity”<sup>3</sup>. The issue analyzed by the Court is also regulated by Regulation (EU) 2016/679 in art. 2 para. 2 letter c

In the aforementioned case, Mr. R. installed and used a camera system located under the eaves of his family home. The

system allowed only a visual recording, which was stored on recording equipment in the form of a continuous loop, that is to say, on a hard disk drive. As soon as it reached full capacity, the device would record over the existing recording, erasing the old material. No monitor was installed on the recording equipment, so the images could not be studied in real time. Only Mr. R had direct access to the system and the data. The surveillance system recorded the entrance to his home, the public footpath and the entrance to the house opposite. Given these circumstances, Mr. R. was sanctioned by the Office for personal data protection for infringing Law no. 101/2000, since as a data controller, he had used a camera system to collect, without their consent, the personal data of persons moving along the street or entering the house opposite. It was also noted that the data subjects had not been informed on the processing of such data and that Mr. R. had failed to fulfill the obligation to notify the authority on the respective processing.

The question referred to the Court by the national court was whether the operation of a camera system installed on a family home for the purposes of the protection of the property, health and life of the owners of the home can be classified as the processing

---

<sup>2</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 was repealed by Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

<sup>3</sup> Currently, the material scope of the GDPR regulations are included in art. 2 of Regulation (EU) 2016/679 which provides the following:” (1) This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. (2) This Regulation does not apply to the processing of personal data: a) in the course of an activity which falls outside the scope of Union law; b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; c) by a natural person in the course of a purely personal or household activity; d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. (3) For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98. (4) This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.”

of personal data “by a natural person in the course of a purely personal or household activity” for the purposes of art. 3 para. (2) of Directive 95/46 [...], even though such a system also monitors a public space. In its considerations, the court notes that there should be established whether the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, amounts to the processing of data in the course of a purely personal or household activity, for the purposes of the provisions of art. 3 para. 2 second indent of Directive 95/46.

The first aspect analyzed by the Court entails the fact that the image of a person recorded by a camera constitutes personal data within the meaning of art. 2 letter (a) of Directive 95/46, inasmuch as it makes it possible to identify the person concerned. Secondly, the Court notes that, as can be seen, in particular from recitals (15) and (16)<sup>4</sup> of Directive 95/46, video surveillance falls, in principle, within the scope of that directive in so far as it constitutes automatic processing. The Court notes that according to settled case-law, the protection of the fundamental right to private life guaranteed under Article 7 of the Charter of Fundamental Rights of the European Union, requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. The Court rules that a personal

data processing falls under the scope of the derogation referred to in art. 3 para. (2) second indent of the Directive only if the respective processing is carried out exclusively in the personal or domestic scope of the person performing it.

On the other side, it is noted that that video surveillance such as that at issue in the main proceedings covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely ‘personal or household’ activity for the purposes of art. 3 para. (2) second indent of Directive 95/46.

Notwithstanding, the Court concludes that the application of the provisions of art. 7 letter (f), with art. 11 para. (2) and with art. 13 para. (1) letter (d) and (g) of the directive enables, where appropriate, to take into account the legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself.

Despite the fact that Directive no. 95/46 was repealed by Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, the judgment ruled by the Court decides on an important and sensitive issue in the field of personal data processing, respectively that of the video surveillance and the significance that video surveillance has on individuals’ privacy in the sense that in case a video surveillance system is installed in an individual’s home for the purposes of protecting life and property, to

---

<sup>4</sup> Recitals (15) and (16) of Directive 95/46 provide the following: (15) whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question; (16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defense, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law.

the extent that the images collected are outside their own space, such a processing can be considered as a processing of data in the course of a purely personal or household activity. This interpretation also appears in the domestic legislation by means of Decision no. 52 of 31 May 2012<sup>5</sup> of the National Authority for the Supervision of Personal Data Processing.

**2.2.** Another important aspect in the field of the video surveillance of household was decided by the Court<sup>6</sup>.

Therefore, in October 2018, Bucharest Tribunal decided to suspend the proceedings for the litigation between TK, on the one side, and Asociația de Proprietari (Association of co-owners) and to refer a request for a preliminary ruling to the ECOJ, under article 267 TFEU. The ECOJ answered to the request of Bucharest Tribunal by means of Judgment of 11 December 2019, thus establishing a new reference case in the field of data protection when discussing about video surveillance.

In fact, the request has been made in proceedings between TK and the Asociația de Proprietari bloc M5A-Scara A (Association of co-owners of building M5A, staircase A, concerning TK's application for an order that the association takes out of operation the building's video surveillance system and remove the cameras installed in the common parts of the building. TK lives in an apartment which he owns, located in building M5A. At the request of certain co-owners of that building, the association of co-owners adopted, at a general assembly held on 7 April 2016, a decision approving the installation of video surveillance cameras in that building. In implementation

of that decision, three video surveillance cameras were installed in the common parts of building M5A. The first camera was pointed towards the front of the building, whereas the second and third cameras were installed, respectively, in the ground-floor hallway and in the building's elevator. TK objected to that video surveillance system being installed on the ground that it constituted an infringement of the right to respect for privacy. TK brought an action before Bucharest Tribunal requesting that the association of co-owners be ordered to remove the three cameras and to take them out of operation definitively, failing which a penalty payment would be imposed. TK argued before the referring court that the video surveillance system at issue infringed EU primary and secondary law, in particular the right to respect for private life both under EU and national law. He also stated that the association of co-owners had taken on the task of data controller for personal data without having followed the registration procedure in that regard provided for by law. The association of co-owners stated that the decision to install a video surveillance system had been taken in order to monitor as effectively as possible who enters and leaves the building, since the elevator had been vandalized on many occasions and there had been burglaries and thefts in several apartments and the common parts. The association also stated that other measures which it had taken previously, namely the installation of an intercom/magnetic card entry system, had not prevented repeat offences of the same nature being committed.

<sup>5</sup> Decision 52/2012 of the ANSPDCP (National Authority for the Supervision of Personal Data Processing) provides the following: Art. 3 The processing of personal data by means of the use of the video surveillance systems is performed under the observance of the general rules referred to in art. 4 of Law no. 677/2001, as further amended and supplemented, especially of the principle of proportionality of purpose. Art. 4 Video surveillance can be performed mainly for the following purposes: .....c) to ensure the security and protection of persons, goods and valuables, of real estates and public utility installations, as well as of the enclosures affected by them.

<sup>6</sup> Judgment of the Court of 11 December 2019 in case C-708/18.

Bucharest Tribunal decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

- “Are Articles 8 and 52 of the Charter and Article 7 letter (f) of Directive 95/46 to be interpreted as precluding provisions of national law such as those at issue in the main proceedings, namely Article 5(2) of [Law No 677/2001], and Article 6 of [Decision No 52/2012 of the ANSPDCP], in accordance with which video surveillance may be used to ensure the safety and protection of individuals, property and valuables and for the pursuit of legitimate interests, without the data subject’s consent?”

- “Are Articles 8 and 52 of the Charter to be interpreted as meaning that the limitation of rights and freedoms which results from video surveillance is in accordance with the principle of proportionality, satisfies the requirement of being ‘necessary’ and “meets objectives of general interest or the need to protect the rights and freedoms of others”, where the controller is able to take other measures to protect the legitimate interest in question?”

- “Is Article 7 letter (f) of Directive 95/46 to be interpreted as meaning that the “legitimate interests” of the controller must be proven, present and effective at the time of the data processing?”

- “Is art. 6 para. (1) letter (e) of Directive 95/46 to be interpreted as meaning that data processing (video surveillance) is excessive or inappropriate where the controller is able to take other measures to protect the legitimate interest in question?”<sup>7</sup>

In relation to these questions, the Court ruled that art. 6 para. (1) letter (e) and art. 7 letter (f) of Directive 95/46/CE of the European Parliament and of the Council of

24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, read in the light of art. 7 and 8 of the Charter of Fundamental Rights of the European Union, must be interpreted as not contradicting national provisions which authorize the installation of a system of video surveillance, such as the system at issue in the main proceedings, installed in the common parts of a residential building, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the data subject’s consent, if the processing of the personal data performed by means of the video surveillance system in question fulfills the conditions provided by the aforementioned art. 7 letter (f), an aspect the verification of which is incumbent on the referring court.

Art. 7 letter (f) of Directive 95/46 lays down three cumulative conditions so that the processing of personal data is lawful, namely, **first**, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; **second**, the need to process personal data for the purposes of the legitimate interests pursued; and **third**, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence<sup>8</sup>.

**As regards first condition**, art. 7 letter (f) of Directive 95/46 does not require the data subject’s consent. Such consent, as a condition to which the processing of personal data is made subject, appears, however, only in article 7 letter (a) of that directive. In the present case, the objective which the controller essentially seeks to achieve when he or she installs a video surveillance system such as that at issue in the main proceedings, namely protecting the

<sup>7</sup> Item 27 of Judgment of the Court of 11 December 2019 in case C-708/18.

<sup>8</sup> In this respect, see Judgment of 4 May 2017, Rīgas satiksme, C-13/16, EU:C:2017:336, item 28.

property, health and life of the co-owners of a building, is likely to be characterized as a 'legitimate interest', within the meaning of article 7 letter (f) of Directive 95/46.

**As regards second condition**, relating to the need to process personal data for the purposes of the legitimate interests pursued, the Court has pointed out that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. That condition requires the referring court to ascertain that the legitimate data processing interests pursued by the video surveillance at issue in the main proceedings — which consist, in essence, in ensuring the security of property and individuals and preventing crime — cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter.

In this respect, the condition relating to the need for processing must be examined in conjunction with the 'data minimization' principle enshrined in art. 6 para. (1) letter (c) of Directive 95/46, in accordance with which personal data must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'.

The proportionality of the data processing by a video surveillance device must be assessed by taking into account the specific methods of installing and operating that device, which must limit the effect thereof on the rights and freedoms of data subjects while ensuring the effectiveness of the video surveillance system at issue. Therefore, the condition relating to the need for processing implies that the controller must examine, for example, whether it is

sufficient that the video surveillance operates only at night or outside normal working hours, and block or obscure the images taken in areas where surveillance is unnecessary.

Lastly, as regards **the third condition** laid down in art. 7 letter (f) of Directive 95/46, relating to the existence of fundamental rights and freedoms of the data subject whose data require protection, which might override the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, the assessment of that condition requires a balancing of the opposing rights and interests concerned which depends on the individual circumstances of the particular case in question, and in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter.

In this context, the Court has held<sup>9</sup> that art. 7 letter (f) of Directive 95/46 precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case.

Thus, Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case<sup>10</sup>.

### 3. Conclusions

In the light of the analysis of the case-law of the ECOJ in the field of video surveillance in private spaces, we can conclude that it can be performed without violating the rules on personal data

<sup>9</sup> Item 53 of the Judgment of the Court of 11 December 2019 in case C-708/18.

<sup>10</sup> In this respect, see Judgment of 19 October 2016, Breyer, C-582/14, EU:C:2016:779, item 62.

protection if certain conditions required by the legislation in force are met and if these general rules are appreciated in relation to each particular case.

From the perspective of the conditions that must be analyzed when the video surveillance of private space is discussed, it is necessary to identify the way in which the image of a person recorded by a video camera represents a personal data, insofar as it allows the identification of the data subject. Another aspect concerns the identification of the processing performed by surveillance insofar as it is an automatic processing.

Another aspect that should be identified and analyzed in this field is that the derogation from the protection of personal data made by video surveillance is carried out within the limits of what is strictly necessary. In this respect, a derogation “within the limits of what is strictly necessary” is deemed to be carried out exclusively in the personal or household scope of the person performing it.

An important conclusion emerges from the analysis of the case-law of the ECOJ in the situation of the partial extension of video surveillance to public space, an activity that apparently cannot be considered as an exclusively “personal or household” activity. Notwithstanding, the Court held that, in such situations, the surveillance can be performed if the legitimate interests of the controller, consisting, among others, in the protection of the property, health and life of the controller and his family, are taken into account.

In what concerns the concept of “legitimate interest”, this may be used as a basis for processing if the purpose essentially pursued by the data controller when establishing a video surveillance system is the protection of the property, health and life of the co-owners of a

building. In this context, it is necessary to verify whether the data processing legitimate interest pursued by video surveillance, which consists essentially in ensuring the security of property and persons and in preventing the commission of criminal offences, cannot be reasonably achieved, with the same efficiency, by other means that would be less intrusive for the fundamental rights and freedoms of the data subjects, in particular the right to privacy and to the protection of personal data. From this perspective, it should be noted that the need for processing must be assessed together with the “data minimization” principle, according to which personal data must be adequate, relevant and not excessive in relation to the purpose for which they are collected and further processed.

For every situation in which video surveillance of private spaces is used, in particular of common use spaces within residential areas, it is necessary to balance the opposing rights and interests in question, depending on the specific circumstances of the respective case, in which the importance of the data subject must be taken into account. In this field, the opposing rights and interests take into account the existence of the fundamental rights and freedoms of the data subject, on the one hand, and the legitimate interest pursued by the data controller or third parties to whom the data are communicated, on the other hand. Given that this balancing of the opposing rights and interests in question may differ from one particular case to another, the Court opposes a Member State to establish general rules definitively determining the result of the balancing of opposing rights and interests, without enabling the analysis of specific elements generating a different result depending on the special circumstances of a specific case.



### References

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Decision no. 52/2012 of 31 May 2012 of the National Authority for the Supervision of Personal Data Processing
- ECOJ, Fourth Chamber, Judgment of 11 December 2014, Rines, C-212/13
- ECOJ, Second Chamber, Judgment of 19 October 2016, Breyer v. Germany, C-582/14
- ECOJ, Second Chamber, Judgment of May 4 2017, Rīgas satiksme, C-13/16
- ECOJ, Third Chamber, Judgment of 11 December 2019, TK v Asociația de Proprietari bloc M5A-Scara A, C-708/18