VIDEO SURVEILLANCE: STANDPOINT OF THE EU AND NATIONAL LEGISLATION ON DATA PROTECTION

Claudia CLIZA[*]
Sandra OLANESCU[**]
Alexandru OLANESCU[***]

Abstract

Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 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 ("GDPR") entails a series of major changes in the field personal data protection.

The new developments mainly concern the introduction of data protection controller, of specific rights of data subject, such as: the right to be forgotten and the right to data portability, as well as special provisions on minors.

Notwithstanding, certain items seem at first sight to be left untreated by G.D.P.R., which is not true! GDPR applies to all data processing operations, even if not all of these are expressly regulated. One of these personal data modalities is represented by the video surveillance. Despite not expressly regulated by G.DP.R., this is one of the most commonly used means of personal data processing.

The particular importance of this subject is given by the potential issues that may occur when the captured images clearly disclose the identity of a person, so that they lead to the unique identification of the data subject. In this case, the issue that arises is whether the processed data would somehow fall under the scope of special data, such as biometric data.

Keywords: *data protection, data subjects, video surveillance, identity, special categories of data.*

1. Introduction

1.1. Data Protection Legislation

Changing the legislation regarding the personal data protection emerged as a necessity taking into consideration the exchange of personal data determined by day by day technology evolution.

The current possibility that every individual has I what concerns the publishing of personal data information imposed a framework regulation within the Member States to protect as much as possible the interest of the individual.

At European Union (the "*EU*") level, the personal data protection was governed by Directive 95/46/EC of the European Parliament and of the Council of October 14th, 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

Taking into consideration the increase in cross-border flows of personal data, at EU level the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.2. What is the G.D.P.R.?

G.D.P.R. means Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

G.D.P.R. was adopted on April 27th, 2016, being published on May 4th, 2016. G.D.P.R. entered into force on May 24th, 2016 and it shall become applicable for all Member States as of May 25th 2018.

G.D.P.R. is a legally binding act. It shall apply directly, in its entirety, in all Member States.

1.3. Who does the G.D.P.R. affect?

The G.D.P.R. applies to both organisations/entities located within the European Union (the "*E,U.*") and organisations/entities located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects[1].

Moreover, the G.D.P.R. applies to all companies processing and holding the personal data of data subjects residing in the E.U., regardless of the location of the company.

[*] Lecturer, PhD, Faculty of Law, "Nicolae Titulescu" University of Bucharest (e-mail: claudia@cliza.ro);

[**] Master's Degree in International and EU Law, Faculty of Law, "Nicolae Titulescu" University of Bucharest (e-mail: sandra.olanescu@cliza.ro);

[***] Master's Degree in International and EU Law, Faculty of Law, "Nicolae Titulescu" University of Bucharest (e-mail: alexandru.olanescu@cliza.ro);

[1] See https://www.eugdpr.org/gdpr-faqs.html;

1.3. National Legislation

In Romania, the applicable legal provisions on Data Protection are comprised in Law no. 677/2001 on for protection of persons with regard to the processing of personal dataa and the free movement of such data ("*Law No. 677/2001*").

As of May 25th, 2018, the provisions of such national legislation shall be repealed and the G.D.P.R. shall fully apply in all E.U. Member States, including Romania.

Nonetheless, it may be held that the current national legal provisions on data protection may also apply after the G.D.P.R. becomes applicable, but only as a recommendation and only to the extent that the GDPR does not provide for such a situation or does not provide a provision contrary to the repealed national legislation.

2. Video Surveillance from G.D.P.R.'s perspective

2.1.Short considerations from the perspective of the ECHR

As regards the recent case law of the European Court of Human Rights (the "ECHR"), there are several key-cases that enable us to determine how the Court assesses the breach of human rights via video surveillance, as well as the requirements that have to be met in order to value one's legitimate interest more than the protection of the right to privacy (Art. 8 of the European Convention on Human Rights - Right to respect for private and family life).

Hence, the following cases shall be deemed as eloquent:

- **Case Köpke v. Germany** – October 5th, 2010 (decision as to the admissibility)
  - The applicant – cashier in a supermarket was dismissed without notice for theft;
  - A private detective agency carried out covert video surveillance whereby the theft was found;
  - The dismissal decision was unsuccessfully contested before the competent domestic courts;
  - The European Court of Human Rights (the "Court") dismissed the applicant's claim as inadmissible under article 8 of the Convention, given the following:

a) the domestic authorities achieved a fair balance between the employee's right to respect for her private life, the employer's interest in the protection of its property rights and the public interest in the proper administration of justice;
b) the contested measure was limited in time (two weeks) and covered only the area around the cash desk– this area being accessible to the public.
c) the visual data obtained were processed by a limited number of persons working for the detective agency and by staff members of the applicant's employer. The data was used only for the purposes of the termination of the employment relationships, including the proceedings the applicant brought in this respect in the labor courts;

The Court: the overlap with the applicant's private life was limited to what was necessary to achieve the scope pursued by the video surveillance. Notwithstanding, the Court noted that, in this case, the competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life are made possible by new, more and more sophisticated technologies".

- Case Antović & Mirković v. Muntenegru – November 28th, 2017
  - The applicants – two professors of the School of Mathematics of the University of Montenegro, after video surveillance had been installed in areas where they taught;
  - They stated that they had had no effective control over the information collected and that the surveillance had been unlawful;
  - The domestic courts rejected the compensation claim, finding that the question of private life had not been at issue as the auditoriums where they taught were public areas;
  - The Court found that there had been a violation of Article 8 of the Convention, the video surveillance in this case being unlawful **on the following grounds:**

a) the Court noted that it had previously found that private life might include professional activities, as in case of the applicants;
b) the evidence showed that surveillance had violated the provisions of domestic law – the domestic courts had never even considered any legal justification for the surveillance because they had decided from the outset that there had been no invasion of privacy.

The Court: private life might include professional activities, as in case of the applicants. The video surveillance of the classroom represented an interference with the applicants' right to private life".

- Case López Ribalda & others v. Spain – January 9th, 2018
  - Applicants: employees of a Spanish supermarket chain, suspected of theft;
  - Contested video materials – the ground of the applicants' dismissal;
  - The domestic courts accepted the video materials as evidence and confirmed the dismissal decisions;
  - The Court found that there had been a violation of article 8 of the Convention, given that:

a) the domestic courts failed to strike a fair balance between the rights available in this case, respectively the applicants' right to private life and the employer's property right;
b) under Spanish data protection legislation, the applicants should have been informed that they were under surveillance, but they had not been;
c) the employer's rights could have been safeguarded

by other means and it could have provided the applicants at the least with general information on the surveillance;

d) Notwithstanding, the Court found that there had been no violation of article 6 § 1 (the right to a fair trial) of the Convention. The Court found that the proceedings as whole had been fair because the video material was not the only evidence the domestic courts had relied on when upholding the dismissal decisions and the applicants had been able to challenge the recordings in court.

The Court: there was not a fair balance between the rights available in this case (the employees' right to private life/the employer's property right); the applicants should have been informed that they were under surveillance; the employer's rights could have been safeguarded by other means".

To conclude with, the Court determines whether the video surveillance of employees violates their right to privacy, according to the following criteria:

1. Prior notification of supervised employees;
2. Grounds justifying the application of the surveillance measure (scope);
3. Proportionality between the measure adopted and the aim pursued;
4. Level of intrusion and use of data obtained through surveillance (e.g., data retention time).

2.2. G.DP.R. – how does it apply on Video Surveillance

Apparently, the GDPR does not contain an express regulation on video surveillance. However, this is a false representation, as the G.D.P.R. does not expressly regulate every circumstance or situation governed by its provisions.

In order ti understand its scope, it is necessary to define the key-elements that the G.D.P.R. sets forth. Some of these are the following (G.D.P.R., Art. 4):

1. "personal data" = any information relating to an identified or identifiable natural person ("data subject");

- any information = subjective or objective information; information in term of its content; information format; regardless the modality of capture, storage or presentation (i.e. including images, audio or video recordings, etc, etc.);
- identified natural person = a person who differentiates himself into a particular group of persons from the other members of the group;
- identifiable natural person* = a person who can be identified, directly or indirectly, in particular by reference to an identifier (i.e. a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person);

2. "controller" = means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

- (!) he / she shall be held liable for the following: (a) how the processor is chosen; (b) to ensure the CONTROL on the processing operations performed by the processor (as a general rule, by inserting minimum clauses in the contract);

3. "processor" = means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- (!) he/she shall be held liable for the following: (a) THE FAILURE TO MEET THE OBLIGATIONS incumbent on him/her under GDPR; (b) THE FAILURE TO MEET THE INSTRUCTIONS of the controller.

The controller and the processor shall be held JOINTLY liable before the data subject!

2.2.1. Principles relating to processing of personal data (G.D.P.R., Art. 5)

1. Lawfulness, fairness and transparency (the existence of the GROUND of the processing and the NOTIFICATION[2] made available to data subject);
2. Limitations as to the scope (establishing the purpose BEFORE the processing);
3. Data minimization (i.e. only NECESSARY data is processed);
4. Accuracy (in relation to processed data – it has to be UPDATED and ACCURATE);
5. Storage limitations (the data is erased when it is no longer NECESSARY);
6. Integrity and confidentiality (LIMITATION AND SECURITY OF THE ACCESS to processed data);
7. Accountability (existence and storage of justifying DOCUMENTS on conformity).

2.2.2. The main elements to be established/identified in relation to every processing

For every type of data processing, there has to be a **scope** well established by the personal data processing. G.D.P.R. does not limit this scope, the controller is the one who exclusively establishes it.

The scope of the processing must be found in the relationship between the controller and the data subject.

Another main element provided and established by G.D.P.R.. as opposed to the scope, **the ground** is expressly and restrictively provided by GDPR, in Art. 6). This may be one or more of the following:

1. Legal obligation;
2. Execution of an agreement (the stages of the execution of an agreement – negotiation, conclusion, execution, etc.);
3. Legitimate interest – the performance of an assessment is required (it is not expressly indicated, but can be derived from art. 6(1) letter f)

[2] The information must, in order to be valid, present the following features: (i) be made in a concise, transparent, intelligible and easily accessible form; (2) using clear and simple language, especially for any information specifically addressed to a child; (iii) free of charge;

and para. 47 - preamble) – Legitimate Interest Assessment;(„LIA"). This assessment can entail the answer to the following questions:

- Is there any legitimate interest in the processing? The answer to this question can be given by taking into account the following elements: it complies with lato sensu law; it is sufficiently specific/specified; it is real and present.
- Is the processing required? (i.e. is there another way to reach the identified interest?). the so-called "Balancing Test" is used in this respect – the assessment of the opportunity to establish the legitimate interest as the ground for such processing. The conclusion of this test shall be the importance and nature of the identified legitimate interest > fundamental rights and freedoms of the data subjects (otherwise, there is NO LEGITIMACY for processing)

The peculiarity of the legitimate interest as the ground of processing is that it entails the right of opposition of the data subject and the information must mention this (GDPR, art. 21).

1. **Consent** (when there is a legal obligation[3]; when NO other ground can be used[4]);
2. **The protection of vital interests of data subject/other natural persons;**
3. **The performance of a task that is in the public interest or which results from the exercise of the public authority** by the controller.

Another essential element, the importance of which is crucial in establishing a violation of G.D.P.R., from the perspective of the national supervisory authority, is the **storage period**. This must be predetermined/identifiable and limited to what required. A processing longer than necessary and unjustified is a violation of G.D.P.R.

2.2.3. GDPR and video surveillance – what is the connection?

Why is it important for surveillance camera users to acknowledge the GDPR impact? The answer is a natural one: surveillance cameras capture data!

In this respect, it is particularly important to know **data classification** (according to WP29[5]). Therefore, data is classified as follows:

I. Data provided directly by the data subject;
II. Observed data;
III. Derived data.

Given the aforementioned classification and the type of data processing by video surveillance means, the data obtained by video surveillance is observed data.

Further on, we have to identify the capacity of the person performing the processing by video surveillance means and/or equipment. Therefore, the supervision can be performed by the **controller**, if he/she is the one who effectively processes the data (i.e. video recordings); or by the **processor**, if the controller entrusts the processing to the processor (i.e. the conclusion of an agreement with a security service provider).

As in case of any type of personal data processing, the processing by video surveillance equipment requires the **assessment of its main elements**, therefore:

1. in terms of the ground, the following can be identified as potential grounds of personal data processing:

a) legitimate interest – the analysis of the legitimacy of the identified interest is required;
b) legal obligation – Law no. 333/2003: art. 2 and the Methodological regulations for the application thereof (!) video surveillance is mandatory in the following cases: public units and institutions; credit institutions which fall in the category of banks; trading companies the scope of business of which is the foreign exchange; pawn shops, metal or gemstone jewelry shops or weapons and ammunition shops; mail service providers; fuel marketing stations; commercial properties with areas larger than 500 sq.m., gambling facilities; the cashiers of utility suppliers; cash dispensers; cash processing centers.
c) execution of an agreement (in case of the processor – security service provider).

2. from the perspective of the person performing the processing, the assessment of the processing operation must be viewed and analyzed distinctly, depending on the controller and processor. Therefore, from the perspective:

of the CONTROLLER

The scope can be defined as the security of persons and goods.

The ground can be either a legal obligation or the legitimate interest.

Storage term: as a general rule, 30 days/the deadline established by the law.

of the PROCESSOR

The scope can be defined as the security of persons and goods.

The ground is, as a general rule, the execution of an agreement.

The storage term is the deadline established in the agreement by the controller/deadline established by the law (as a general rule, 30 days).

[3] *E.g.* GDPR – art. 8, 9, 22 (1) – the processing of sensitive data regarding children; fully automated decisions with significant effect; Law no. 504/2006 (the storage of information on terminal – cookies); Law no. 356/2004 (marketing by phone and e-mail, except the existent customers);

[4] Especially if the assessment of the legitimate interest shows that the interest of the data subject prevails;

[5] Article 29 Working Party on Data Protection (WP29) - Handbook on the Right to Data Portability, p. 10, available on: https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf. A se vedea și: Avizul nr. 4/2007 privind conceptul de date cu caracter personal, disponibil pe: https://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwirhvOSxPbZAhVSI1AKHTExDxgQFggoMAA&url=http%3A%2F%2Fwww.dataprotection.ro%2Fservlet%2FViewDocument%3Fid%3D288&usg=AOvVaw3hbKD20dAykEhu6bjHoXnu;

(!) The processor is bound to appoint a Data Protection Officer ("DPO")[6], on the following grounds:

- his/her main activities consist in processing operations which,
- by their nature, scopes and/or purposes, require periodic and systematic monitoring of data subjects on a large scale.

3. The approach of video surveillance performed by the Member States from the GDPR perspective

For a better understanding of the way the Member States approached the issue of the implementation of the regulations of G.D.P.R. which leaves at their discretion the regulation of certain areas, it is important to analyze various measures and perspectives that some of them have already applied.

1. Bavaria – Germany

– June 6th, 2016 – The Data Protection Authority of Bavaria ("Bavarian ***DPA***") issued a short guide on the conformity of video surveillance with GDPR.

"GDPR does not contain guidelines on regulatory requirements for video surveillance. The legitimacy of video surveillance measures falls under the scope of art. 6 paragraph (1) letter (f) of GDPR, according to which the processing is lawful if «the 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 Bavarian DPA identified the following criteria for the compliance with GDPR, namely:

- Study of impact on private life – the controller performs a study of impact before the processing, especially in what concerns the area accessible to the public – GDPR, preamble 91, art. 35;
- Documentation of the study of impact – the controller shall keep the required documentation in order to prove the conformity with the legal requirements on the performance of the study of impact - GDPR, art. 5 para. (2);
- The storage of sufficient evidence on the processing operations – GDPR, art. 30 GDPR. According to Bavarian DPA, this includes especially the obligation to indicate every camera, the scope, reason for which the surveillance system is necessary and proportionate, any risk for the data subjects and the measures envisaged/taken in order to approach risks.
- Consultation before processing – the consultation of the authority is necessary before the processing, if the study of impact indicates that the processing would result in a high risk in the absence of the measures adopted by the controller in order to mitigate the risk – GDPR, art. 36[7].

2. Belgium

– March 8th, 2018 – a draft amendment to "Surveillance camera law" of March 21st, 2007 was adopted, which is to become effective as of May 25th, 2018.

This draft provides mainly the following:

- Surveillance cameras located on public roads: security agencies will be able to watch real-time images of these cameras, installed in open spaces;
- Surveillance camera located in closed and publicly accessible spaces (i.e. a store), can be accompanied by a public display where the images can be watched, located near the camera to reinforce its preventive effect;
- Surveillance cameras used to monitor compliance with municipal parking regulations and tolls: the compliance with all municipal regulations falling within its scope shall be checked;
- The use of mobile surveillance cameras (portable cameras, mobile phones, drones, etc.) shall be authorized in a closed space in three cases exclusively:
- the use by police officers of their competencies under the private security law (article 142 of private security law);
- in closed spaces or parts thereof, where nobody should be present (unoccupied place, industrial place at night, shop outside the working hours, etc.);
- the use by a natural person for personal and household purposes in a closed place that is not accessible to public (owner of a large private property).
- The use of "smart surveillance cameras": they are classified as follows:
- cameras which are not connected to personal data files (cameras that detect sounds, movements, etc.): such cameras shall be authorized;
- cameras connected to personal data files (recognition of number plates, faces, etc.) – only ANPR cameras (with number plate recognition capabilities) and the personal data file is required to be processed according to the legislation regarding the respect for private life;
- The obligation to inform the authorities: two amendments occur:
- the use of surveillance cameras shall be notified only to the police, as well as to the Data Protection Authority. This statement must be updated, a new online notification application is to be implemented;
- the persons liable for the processing of this type of data shall keep a register of image processing activities (in electronic format or not) which entails information established by the royal decree and shall be made available to the Data Protection Authority and police departments, upon request. On the other hand, the citizen who wants to install a surveillance camera

[6] GDPR, art. 37 (1) - the designation of the DPO is also mandatory for public authorities / bodies (except courts) and where the principal activities of the operator / proxy are to process large-scale special categories of data;

[7] Source: https://www.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf

within his/her house for personal and internal purposes shall not be bound to make a statement, to fill in a register or to use a pictogram (which does not mean that he/she can film people without their consent). Furthermore, when a person installs a surveillance camera in accordance with surveillance camera law, but also uses this camera for other purposes which are regulated by other laws, the legislation on video surveillance shall prevail if different provisions which are not compatible apply[8].

3. Great Britain

- March 14th, 2018 – The Commissioner for video surveillance announced the adoption of a national strategy on video surveillance for England and Wales.

Scope of the Strategy: the provision of guidelines in the field of surveillance cameras in order to enable system controllers to understand good and best practices and their legal obligations (such as those provided by Freedoms Protection Law, Data Protection Law and Private Security Industry Law).

Vision of the Strategy: "to make sure that the public is confident that any use of camera surveillance systems in a public place helps in protecting them and keeping them safe, while complying with the individual right to private life".

- to exist proportionality with a legitimate purpose and transparency proving the fulfillment of good and best practices and relevant legal obligations.

Object of the Strategy: The sector of surveillance cameras includes CCTV, body worn video, automatic recognition of number plates, vehicle borne cameras and unmanned aerial vehicles (*i.e.* drones). Indicative estimates of the number of CCTV cameras are available (closed-circuit video surveillance), yet these only cover part of surveillance camera coverage and capability.

Compliance with the security legislation: The strategy complies with the obligations to keep Great Britain safe from the threat of terrorism and to mitigate and prevent crime and to make sure that people feel safe in their homes and communities.

Challenges: cyber security incidents,

Strategic goals:

1. Enable certification against a range of recognisable standards for the whole spectrum of the industry (manufacturers, installers, designers, system controllers) in delivering surveillance camera solutions;
2. Establish an early warning system to horizon scan for technological developments with implications for the scope and capability of surveillance cameras;
3. Make information freely available to the public about the operation of surveillance camera systems;
4. The police pro-actively share relevant information about their own operation of surveillance camera systems and use of data;
5. Local authorities pro-actively share information about their operation of surveillance cameras and use of data;
6. Enablers and incentives are in place to encourage the voluntary adoption of the Surveillance Camera Code;
7. Surveillance camera systems associated with protection of critical national infrastructure are operated in compliance with the SC Code;
8. Organisations involved in the manufacture, planning, design, installation, maintenance and monitoring of surveillance camera systems are able to demonstrate that they understand and follow good and best practice and legal obligations;
9. Make information freely available about training requirements and provision for all those who operate, or support the operation of, surveillance camera systems and those who use the data for crime prevention/detection or public safety purposes;
10. Establish and make greater synergies between regulators and those with audit and oversight responsibilities in connection with surveillance cameras;
11. Develop a well-publicised digital portal housing information about surveillance camera regulation, how to achieve compliance and what individual's rights are[9].

4. Conclusions

Video Surveillance is one of the most popular type of personal data processing methods when it comes to ensuring protection of individuals and property.

Thus, it is paramount that controllers and processors comply with the provisions of the G.D.P.R. when using such data processing method, as this might be one of the key-issues with which national authorities shall begin when investigating possible breaches of the legislation on data protection.

On the other hand, it is as much as important that data processing subjects are well informed on their right to refuse this type of personal data processing before any recording is made, as well as eventual actions that they may take against an illegal processing of video or images exposing their person.

To conclude with, video surveillance as a data processing method should be assessed very carefully by any company/entity /institution or organization that has the capacity of controller or processor, in order to be fully compliant with the provisions of the G.D.P.R.

[8] Source: http://www.lachambre.be/flwb/pdf/54/2855/54K2855001.pdf;

[9] Source: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/608818/NSCS_Strategy_post_consultation.pdf.

References

- 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) – the G.D.P.R. - available on: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines, available on: https://edps.europa.eu/sites/edp/files/publication/12-02-13_report_cctv_en.pdf
- European Data Protection Supervisor Guidelines, available on: https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en