Video Surveillance – Personal Data Processing

Daniela-Irina CIREAȘĂ[1]

Abstract
Video surveillance undoubtedly constitutes personal data processing. The legality of this processing is a challenge for Romanian personal data controllers, as the line between legal obligation and the controller's legitimate interest is very fine. Another challenge is correctly establishing the purpose of video surveillance: is it for the physical security of assets and individuals? Is it for employee monitoring? Each of these purposes entails documentation that demonstrates the employer's interest, as well as the methods to respect the principles of personal data processing and ensure their security.

Keywords: *data protection; CCTV; image processing; personal data; video surveillance*.

1. Video Surveillance as a Measure of Physical Security

Video surveillance is governed by two sets of legislation that data controllers must consider: on one hand, the legislation regarding the protection of premises, assets, valuables, and individuals, and on the other hand, the legislation concerning the protection of personal data. The author's opinion is that without consulting and adhering to the provisions of these two distinct legislations, we cannot speak of correct and legal video surveillance.

Regarding the legislation related to the protection of premises, assets, valuables, and individuals, the provisions of Law no. 333 of July 8, 2003, on the protection of premises, assets, valuables, and individuals – republished[2], are applicable. This law applies to "ministries and other specialized bodies of central and local public administration, autonomous regions, national companies and

[1] President of the Association of Privacy and Data Protection Specialists, Romania.
[2] https://legislatie.just.ro/Public/DetaliiDocument/45134

corporations, national research and development institutes, companies regulated by Law no. 31/1990, republished, with subsequent amendments and completions, regardless of the nature of the share capital, as well as other organizations that hold assets or valuables in any form," according to Article 2, paragraph (10) of the aforementioned law.

Government Decision no. 301 of April 11, 2012, approving the Methodological Norms for the Implementation of Law no. 333/2003 on the Protection of Premises, Assets, Valuables, and Individuals, states in Article 2, paragraph (1): "The adoption of security measures for premises, assets, and valuables provided by law is carried out based on a physical security risk analysis." [3]

Therefore, the physical security measures instituted by the units (read: *entities*) provided for in Law no. 333/2003 can only be implemented after conducting a physical security risk analysis. Among the physical security measures is also the installation of a video surveillance system.

In accordance with Ministry of Internal Affairs Instructions no. 9 of February 1, 2013, regarding the conduct of risk analyses for the physical security of the units subject to Law no. 333/2003 on the protection of premises, assets, valuables, and individuals[4]: "The physical security risk assessment constitutes the foundation for adopting the security measures for objectives, assets, and values required by law, which are implemented in the security plan and the alarm system design."

The physical security risk assessment is recorded by the beneficiary unit after it is assumed by its management. Subsequently, within 60 days, the established measures must be implemented. Failure to comply with the measures outlined in the risk assessment constitutes an offense.

Turning to video surveillance, we observe that the aforementioned Methodological Norms distinguish two categories of units: those with minimal requirements and units without minimal requirements. The category of units with minimal requirements includes: public interest units and institutions, banking units, non-banking financial institutions, currency exchange offices, pawnshops, postal service providers, fuel stations, gambling halls, commercial spaces over 500 square meters, utility provider cashiers, cash transaction machines, and cash processing centers. Only for these

[3] https://legislatie.just.ro/Public/DetaliiDocument/138059 articolul 2, alin. 1
[4] https://legislatie.just.ro/Public/DetaliiDocumentAfis/239390

units is the obligation to install video surveillance systems mentioned, such as in public institutions "on access routes, hallways, and other high-risk areas."

We conclude that, for the areas strictly indicated by legislation, the legal basis for processing personal data through these systems is the legal obligation. If such a unit, subject to minimal requirements, decides to install the system in areas other than those strictly mentioned by law, it should identify another legal basis for data processing. Furthermore, the decision to install CCTV in additional areas should be made following a physical risk assessment.

2. Video surveillance as a means of processing personal data

According to Article 4, paragraph 1 of the European Regulation 2016/679 of the European Parliament and Council of April 27, 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)[5] "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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 that person.

Guideline 3/2019 on the processing of personal data through video means[6] states that "Video surveillance changes in many ways the way professionals from the private and public sectors interact in private or public spaces, with purposes such as enhancing security, analyzing the public, providing personalized advertising, etc. Video surveillance has become particularly effective through the extensive use of intelligent video analytics. These techniques can be more invasive (for example, complex biometric technologies) or less invasive (for example, simple counting algorithms). Maintaining anonymity and protecting privacy are becoming increasingly difficult in general." It is also stated that "Video surveillance is not inherently necessary when other means exist to achieve the primary purpose," thus placing the

[5] https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&qid=1736411428622
[6] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_ro

responsibility on the personal data controller to choose the least intrusive means to achieve their goals.

The systematic automated monitoring of a specific space through optical or audio-visual means, primarily for the protection of property or to safeguard the life and health of individuals, has become an important phenomenon in modern times. This activity involves collecting and storing information in the form of images or audio-visual data about all individuals who enter the monitored space and can be identified based on appearance or other specific elements. The identity of these individuals can be determined based on these details. Additionally, further processing of personal data regarding the presence and behavior of individuals in the given space is possible. The potential risk of abusive use of this data increases with the size of the monitored area and the number of people who frequent that space. This is reflected in the General Data Protection Regulation (GDPR) in Article 35, paragraph (3), letter (c), which requires conducting a data protection impact assessment in the case of large-scale systematic monitoring of a publicly accessible area, as well as in Article 37, paragraph (1), letter (b), which mandates controllers to appoint a data protection officer if the processing operation, by its nature, requires periodic and systematic monitoring of the data subjects.

However, there is an exception provided by the GDPR, namely the processing of personal data for personal or household purposes.

The Court of Justice of the European Union has considered the so-called “derogation for household activities” to be “interpreted as referring only to activities carried out within the private or family life of individuals, which is clearly not the case for the processing of personal data consisting of publishing on the internet, so that this data becomes accessible to an indefinite number of people.”[7]. Moreover, if a video surveillance system, insofar as it involves continuous recording and storage of personal data and covers, “even partially, a public space and is, as such, directed outside the private sphere of the person processing the data in this manner, it cannot be considered an exclusively personal or household activity within the meaning of Article 3, paragraph (2), second indent of Directive 95/46.”[8].

[7] Curtea de Justiție a Uniunii Europene, Hotărârea în cauza C-101/01, Bodil Lindqvist, 6 noiembrie 2003, punctul 47

[8] Curtea de Justiție a Uniunii Europene, Hotărârea în cauza C-212/13, František Ryneš/Úřad pro ochranu osobních údajů, 11 decembrie 2014, punctul 33

Therefore, in most cases of video surveillance, we are dealing with the processing of personal data and, clearly, a personal data controller, as defined by the GDPR, with the corresponding obligations.

Regarding the legal basis for processing personal data through video surveillance, the EDPB Guideline 3/2019 on the processing of personal data through video means specifies that "In principle, any of the legal grounds provided in Article 6, paragraph (1) can constitute a legal basis for processing data derived from video surveillance. For example, Article 6, paragraph (1), letter (c) applies in situations where national legislation requires the implementation of video surveillance. However, the provisions most likely to be used in practice are:

- Article 6, paragraph (1), letter (f) (legitimate interest);
- Article 6, paragraph (1), letter (e) (necessity of performing a task that serves a public interest or is based on the exercise of public authority)."[9]

As previously mentioned, in Romanian legislation regarding physical security, there are certain units classified under minimal requirements for which the installation of a video surveillance system is mandatory in specific areas strictly outlined by law. For all other units, as well as for units subject to minimal requirements if they decide to install a video surveillance system in areas other than those specified by law, the controller must determine the legal basis for processing: legitimate interest or public interest. Since public interest is not a legal basis that private controllers can invoke when they are not performing a task in the public interest, we conclude that for these controllers, the only legal basis for processing data can be legitimate interest.

However, legitimate interest is not enough to be identified and declared; it must be demonstrated by fulfilling three cumulative conditions:

- Legality of legitimate interest
- Necessity of processing
- A balance test between the legitimate interest of the controller and the fundamental rights and freedoms of the data subjects.

These cumulative conditions must be documented through the Legitimate Interest Assessment, the conclusions of which may indicate that the risks to the rights and freedoms of the data subjects (especially when the data subject is a child and/or, I would add, an employee) outweigh the legitimate interest of the controller, and therefore the controller cannot carry out that specific personal data processing.

[9] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_ro, pct 16

In the case of a real and dangerous situation, the purpose of protecting property against burglary, theft, or vandalism may constitute a legitimate interest for video surveillance. The legitimate interest must genuinely exist and be a current issue (i.e., it must not be fictional or speculative). Before surveillance begins, there must have been a real danger situation - such as damage or serious incidents occurring in the past. Considering the accountability principle, it would be advisable for controllers to document relevant incidents (date, method, financial loss) and any associated criminal accusations. These documented incidents can serve as solid proof of the existence of a legitimate interest. This documentation is done through a physical risk assessment, prepared according to physical security legislation, and subsequently becomes part of the Legitimate Interest Assessment to demonstrate the necessity of processing.

Regarding the necessity of processing and adherence to the data minimization principle, personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.[10]

Before installing a video surveillance system, the controller must always critically assess whether this measure is, firstly, appropriate for achieving the desired objective and, secondly, adequate and necessary for its purposes. Video surveillance measures should only be selected if the processing purpose cannot reasonably be achieved by other means that are less intrusive to the rights and fundamental freedoms of the data subject[11].

In a situation where a controller wishes to prevent property crimes, instead of installing a video surveillance system, they could take alternative security measures, such as fencing the property, establishing regular security personnel patrols, using doormen, ensuring better lighting, installing secure locks, anti-burglary windows and doors, or applying anti-graffiti plaster or film on the walls. These measures can be just as effective against burglary, theft, and vandalism as video surveillance systems. The controller must assess on a case-by-case basis whether such measures can be a reasonable solution[12].

[10] RGPD, art. 5, alin 1, lit. C)
[11] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_ro, pct. 24
[12] *Ibidem*, pct. 25

3. Video surveillance of the employees

In addition to the provisions of the GDPR, the Romanian legislator has intervened with legal provisions regarding the monitoring of employees through video surveillance systems for the purpose of achieving the legitimate interests pursued by the employer, establishing, through Article 5 of Law 190/2018 on measures for the implementation of Regulation (EU) 2016/679 of the European Parliament and Council of April 27, 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), certain conditions for employers to be able to monitor their employees using such means[13].

When the employer uses monitoring systems through video surveillance at the workplace, the processing of personal data of employees for the purpose of achieving the legitimate interests pursued by the employer is permitted only if:

a) The legitimate interests pursued by the employer are well justified and outweigh the interests or rights and freedoms of the data subjects, with the balance test documented in the Legitimate Interest Assessment;
b) The employer has provided prior, complete, and explicit information to employees, in accordance with the provisions of Article 13 of the GDPR;
c) The employer has consulted the trade union or, where applicable, the employee representatives before introducing the monitoring systems;
d) Other, less intrusive forms and methods to achieve the employer's objective have not previously proven effective (this history also being documented in the Legitimate Interest Assessment); and
e) The duration of storage of personal data is proportional to the purpose of processing, but not longer than 30 days, except in cases explicitly regulated by law or where there are well-justified reasons.

Be aware, as in practice, the video surveillance system has been installed for the (declared) purpose of physical security of property and individuals, but in some cases, it is also used for monitoring employees. Changing or adding a new purpose to the existing one must be preceded by informing the data subjects.

[13] https://legislatie.just.ro/Public/DetaliiDocument/203151

It should be noted that employees are considered by the GDPR as part of the category of vulnerable persons in relation to their employer, as there is a clear imbalance of power between the two parties in the individual employment contract.

Therefore, if the controller chooses to monitor employees through video surveillance (but also other electronic communication means, including GPS monitoring), they must base this decision on a Legitimate Interest Assessment. If, through the Physical Risk Assessment, the authorized evaluator has determined the installation of a video camera in the access area of the controller's premises for the purpose of ensuring the physical security of the space, but the controller uses the camera to monitor how many times employees go out for a smoke, how long they stay during their cigarette break, what time they arrive, what time they leave, etc., then the purpose of the video surveillance changes, and the controller should ensure compliance with all the conditions set out in Article 5 of Law 190/2018.

4. Data Protection Impact Assessment (DPIA)

The GDPR requires data controllers, in certain situations, to conduct a Data Protection Impact Assessment (DPIA). The ANSPDCP, through Decision no. 174/2018, established that a DPIA is mandatory in the case of:

"c) Processing personal data for the purpose of large-scale systematic monitoring of a publicly accessible area, such as video surveillance in shopping malls, stadiums, markets, parks, or similar spaces;

d) Large-scale processing of personal data of vulnerable individuals, particularly minors and employees, through automated means of monitoring and/or systematic recording of behavior, including for advertising, marketing, and publicity activities."

The Guideline on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" under Regulation 2016/679, issued by the Article 29 Working Party, provides examples of cases where the assessment is mandatory: "Using a camera system to monitor driving behavior on highways. The controller intends to use an intelligent video analysis system to identify vehicles and automatically recognize license plates." or "A company systematically monitors its employees' activity, including monitoring employees' workstations, internet activity, etc."

The DPIA is conducted before personal data processing begins, and the responsibility for preparing it rests with the controller, with the advice of the Data Protection Officer if one has been designated.

The GDPR sets the minimum requirements for a DPIA (Art. 35 (7) and Recitals 84 and 90):

- "A description of the envisaged processing operations and the purposes of the processing";
- "An assessment of the necessity and proportionality of the processing";
- "An assessment of the risks to the rights and freedoms of the data subjects";
- "The measures envisaged to:
  - Address the risks;
  - Demonstrate compliance with the provisions of this Regulation."

Consultation with the supervisory authority is necessary whenever the data controller cannot identify sufficient measures to mitigate the risks to an acceptable level (i.e., the residual risks are still high).

5. Processing of special data through video surveillance

Video surveillance systems typically collect large amounts of personal data, which can reveal highly personal information and even special categories of data. The GDPR classifies as special data those that reveal racial or ethnic origin, political opinions, religious beliefs or philosophical convictions, or membership in trade unions, as well as the processing of genetic data, biometric data for the unique identification of a natural person, health data, or data concerning a person's sexual life or sexual orientation.

To process such data, the controller must identify, in addition to the legal basis for processing data under Article 6 of the GDPR, the fulfillment of an additional condition under Article 9, paragraph 2 of the GDPR.

Political opinions could be inferred, for example, from images showing identifiable data subjects participating in an event, taking part in a strike, etc. This situation would fall under the scope of Article 9.

The installation of a video camera by a hospital to monitor a patient's health condition would be considered processing of special categories of personal data (Article 9).

For example, Article 9, paragraph (2), letter (c) ("[…] processing is necessary for the protection of the vital interests of the data subject or of another natural person […]") could – theoretically and exceptionally – be used, but the data controller should justify the processing by the absolute necessity of protecting the vital interests of

a person and demonstrate that this " […] data subject is physically or legally incapable of giving their consent." Furthermore, the data controller would not be permitted to use the system for any other reason[14].

It is important to note here that it is unlikely that any exception listed in Article 9 would be applicable to justify the processing of special categories of data through video surveillance. More specifically, data controllers processing such data in the context of video surveillance cannot rely on Article 9, paragraph (2), letter (e), which allows the processing of personal data that are clearly made public by the data subject. The mere fact of entering the camera's field of view does not imply that the data subject intends to make public the special categories of data concerning themselves[15].

6. Technical and organizational measures to secure the processing of personal data through the video surveillance system

Technical measures

System security means the physical security of all components of the system and the integrity of the system, i.e., protection against intentional and unintentional interference with its normal operation and resilience against these interferences, as well as access control. Data security means confidentiality (data is accessible only to those granted access), integrity (prevention of data loss or manipulation), and availability (data can be accessed when necessary).

Physical security is an essential part of data protection and the first line of defense, as it protects the components of the video surveillance system from theft, vandalism, natural disasters, man-made disasters, and accidental damage (e.g., power surges, extreme temperatures, and spilled coffee). In the case of analog systems, physical security plays a key role in their protection.

System and data security, i.e., protection against intentional and unintentional interference with its normal operation, can include:

[14] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_ro, pct. 69
[15] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_ro, pct. 70

- Protection of the entire video surveillance system infrastructure (including remote cameras, wiring, and power supply) against fraudulent physical manipulation and physical theft;
- Protection of the transmission of recordings against interception through secure communication channels;
- Data encryption;
- Use of hardware and software-based solutions, such as firewall systems, antivirus, or intrusion detection systems, against cyberattacks;
- Detection of malfunctions at the component, software, and interconnection levels;
- Means of restoring availability and access to the system in the event of a physical or technical incident.

Access control means that only authorized individuals can access the system and data, while others cannot. Measures that support physical and logical access control include:

- Ensuring that all areas where video surveillance is carried out and where video recordings are stored are secured against unauthorized access by third parties;
- Positioning monitors (especially when located in open areas, such as a reception) so that only authorized controllers can view them;
- Defining and applying procedures for granting, changing, and revoking physical and logical access;
- Implementing methods and means for authenticating and authorizing users, including, for example, password length and frequency of changes;
- Recording and periodically analyzing user actions (both at the system level and regarding data);
- Continuous monitoring and detection of unsuccessful access attempts, with weak points being identified as soon as possible.

Organizational measures

- Informing the data subjects (individuals captured in images)
- Drafting a video surveillance policy
- Training involved employees
- Establishing responsibilities
- Preparing the Legitimate Interest Assessment (LIA)
- Preparing the Data Protection Impact Assessment (DPIA)
- Signing confidentiality agreements with authorized persons involved

- Limiting the storage of recordings
- Limiting the disclosure of data recorded by the video surveillance system to criminal investigation authorities

Conclusions

The data controller for personal data processed through the video surveillance system must carefully analyze the actual necessity of installing such a system, the intrusion into the private life of the data subjects, the alternative measures that can be taken, the correct determination of the legal basis for personal data processing, and the technical and organizational measures to be implemented to reduce risks to personal data protection.

The controller is responsible for ensuring compliance with national legislation on physical security of property and individuals, as well as with European Union legislation and national legislation on personal data protection, taking into account the recommendations of the EDPB through the issued guidelines, the sanctions imposed by the National Authority for the Supervision of Personal Data Processing (ANSPDCP), as well as the decisions of the CJEU on video surveillance.

References

Autoritatea Națională pentru Supravegherea Prelucrării Datelor cu Caracter Personal. (2018). Decizia nr. 174 din 18 octombrie 2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal.

Comitetul European pentru Protecția Datelor. (2019). Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video (Versiunea 2.0). https://edpb.europa.eu

Grupul de Lucru Articolul 29. (2017). Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă. https://ec.europa.eu

Grupul de Lucru Articolul 29. (2017). Ghid privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat" în sensul Regulamentului 2016/679. https://ec.europa.eu

Guvernul României. (2012). Hotărârea de Guvern nr. 301 din 11 aprilie 2012 pentru aprobarea normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor.

Ministerul Afacerilor Interne. (2013). Instrucțiunile nr. 9 din 1 februarie 2013 privind efectuarea analizelor de risc la securitatea fizică a unităților ce fac obiectul Legii nr. 333/2003.

Parlamentul European și Consiliul Uniunii Europene. (2016). Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor - GDPR).

Parlamentul României. (2003). Legea nr. 333 din 8 iulie 2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor (republicată).

Parlamentul României. (2018). Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016.