CENTRAL EUROPEAN ACADEMY

LAW REVIEW

CENTRAL EUROPEAN ACADEMY

LAW REVIEW

VOLUME **II**

2024 | № **1**

RIGHTS | CONSTITUTIONAL | SPACE ACTIVITY | SUSTAINAB
GOVERNMENTS | EUROPEAN CHARTER | FRAMEWORK REGU
E LAW | IMPACTS | LEGAL SYSTEM | CIVIL RIGHTS | CONSTIT
RACT | FINANCIAL AUTONOMY | SELF-GOVERNMENTS | EUR
DICTION | DEVELOPMENT | CIVIL RIGHTS | CONSTITUTIONA

CEA
PUBLISHING

Central European Academy Law Review (Print)
HU ISSN 3057-8396 (Print) HU ISSN 3057-8442 (Online) DOI prefix: 10.62733

Publisher:
Central European Academic Publishing
1122 Budapest (Hungary), Városmajor St. 12.
E-mail: publishing@centraleuropeanacademy.hu
Prof. Dr. Barzó Tímea, Director-General

TABLE OF CONTENTS

FLAGSHIP STUDIES

Ana PANEVA*

The Advantages, Risks, and Rules of Installing Video Surveillance in Workplaces

ABSTRACT: *The monitoring of employees is an issue closely related to the right to privacy, protection of personal data, and dignity. The development of modern technology has brought many benefits, but also risks – to which special attention should be paid, especially with the installation of video surveillance systems. The data collected during video surveillance is usually images relating to an identified person, or a person who can be identified – directly or indirectly – to monitor behaviour. As video monitoring spreads, people's freedom of movement and behaviour, and their privacy, are therefore reduced. Video surveillance is used for various purposes, but mostly for security - where guarantees must be taken to avoid any misuse for completely different and individual purposes (e.g. for marketing; to monitor the work of employees, etc.). This paper provides an analysis of the rules and regulations in Macedonian legislation. Special attention is paid to the procedure and circumstances under which it is possible to install permanent video surveillance to control work activity.*
KEYWORDS: *video surveillance, workplace, data protection, procedure.*

1.
Introduction

In our increasingly digitised and interconnected world, the intersection of modern technology and the right to privacy has become a matter of concern. The rapid development of advanced technologies has ushered in a new era of convenience, efficiency, and security – but it has also raised crucial questions regarding the protection of personal data and individual dignity. One significant concern in this scenario is the intricate matter of employee monitoring. This issue revolves around a delicate balance between the necessity of maintaining workplace security and the fundamental rights of individuals regarding privacy, personal data protection, and human dignity.

* PhD candidate, Teaching Assistant, Faculty of Law, Goce Delcev University, Stip, North Macedonia.

http://doi.org/10.62733/2024.1.281-296

One aspect of this challenge involves the use of video surveillance systems. These systems have become pervasive in various environments, offering valuable tools for security and asset protection. However, with this increasing prevalence comes the potential for encroachment upon the individual rights of those being observed. The data captured through video surveillance invariably comprises images of identified individuals – or those who can be indirectly or directly identified – providing a comprehensive record of their actions and behaviour. As these surveillance systems expand their reach, there is a corresponding reduction in the privacy and freedom of movement of those under their surveillance.

Video surveillance is used for a variety of purposes, but mostly for security, where guarantees must be taken to avoid any misuse for completely different and for individual purposes (e.g., for marketing; to monitor the efficiency of employees' performance, etc.). As such, it is imperative to establish clear legal guidelines and regulations to safeguard the rights and freedoms of individuals, while upholding the legitimate objectives of surveillance.

This paper embarks on an in-depth examination of the rules and regulations within North Macedonian legislation. It delves into the specificities of the procedure, and the circumstances under which the installation of permanent video surveillance systems is permissible. This paper aims to clarify the complex legal system that governs the intersection of technology and individual rights, with a specific emphasis on the legal framework in Macedonia.

In the following, the paper will delve into the complexities of video surveillance, examining the challenges of balancing security with personal privacy; it will assess the existing legal safeguards and their effectiveness in achieving a fair equilibrium. Ultimately, this paper aims to contribute to the ongoing discourse on surveillance, privacy, and the protection of personal data – offering insights into how North Macedonian legislation addresses the challenges and complexities posed by video surveillance.

2.
The Legal Framework of the Right to Privacy

One of the most important aspects of moral integrity is a person's privacy, and it is therefore necessary to enjoy legal protection. Hence, the right to privacy is one of the most basic human rights, among a wider group of civil-political rights.

However, modern understandings of privacy were only formed after World War II.[1] In 1947 the United Nations (UN) created the Human Rights Commission

1 Neuwirth, 2007, p. 1.

and prepared the Universal Declaration of Human Rights (UDHR),[2] which has a fundamental significance in building legal frameworks in the field of human rights and freedoms. This declaration, accepted on December 10, 1948, by the UN General Assembly, became the first universal legal document of worldwide significance that deals exclusively with human rights and freedoms. The right to privacy is enshrined as one of the 30 articles of the declaration, with Article 12 emphasising: "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

The right to privacy in the International Covenant on Civil and Political Rights[3] of 1966 is based on the principle of the UDHR and refers to the right of every person to be protected from arbitrary and unlawful interference with his private life, family, home, or correspondence.[4] In addition, if the person believes that his right to privacy has been violated, he has the right to legal protection and can turn to the competent judicial authorities for the determination of damages and the protection of his rights.

The European Convention for the Protection of Human Rights[5] is also an important international document in which the right to privacy can find its foundations. The European Convention – one of the most important international agreements for the protection of human rights in Europe – has been accepted by the Council of Europe and aims to protect and ensure the fundamental rights and freedoms of the signatory states.[6] The protection of privacy is declared in Article 8 of this convention and reads:

> *"Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary for a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

2 The Universal Declaration of Human Rights was adopted and published in Resolution 217 A(III), of December 10, 1948, by the United Nations General Assembly.

3 International Covenant on Civil and Political Rights was adopted and open for signature and ratification or accession by resolution of UN General Assembly 2200 A(XXI) of December 16, 1966. Entered into force on the 23rd. March 1976.

4 Article 17 International Covenant on Civil and Political Rights.

5 Convention for the Protection of Human Rights and Fundamental Freedoms. Rome, 4.XI.1950.

6 Under the strong influence of the Universal Declaration of Human Rights Council of Europe in 1950 (on November 4 in Rome) adopted a Convention for the Protection of Human and Fundamental Rights Freedoms. The convention is the first and basic document of The Council of Europe for the Protection of Human Rights and Freedoms.

The primary purpose of Article 8 is to protect against arbitrary interferences with private and family life, home, and correspondence.[7] However, member states also have positive obligations to ensure that Article 8 rights are respected even between private parties. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals themselves. The right to privacy can only be limited on the basis of a legitimate purpose. Article 8 paragraph 2 of the convention lists such legitimate goals: national security, public security, economic well-being, protection of health and morals, and protection of the rights and freedoms of other citizens.

Later, the Convention for the Protection of Persons with Regard to Automatic Processing of Personal Data[8] was adopted, in order to extend the protection of the basic rights and freedoms of individuals, and especially the right to privacy. This convention provides specific instructions for the legal processing of personal data (the processing is required to be legal, proportionate, and justified by a legitimate purpose), which allows under certain circumstances and limitations the protection of the right to privacy, in order to respect the rights and freedoms of other persons.

The right to privacy, as defined in international documents, is a universally recognised right that not only binds the international community but also national legislation, creating fertile ground for the formulation and integration of the first mechanisms and norms for the protection of citizens' privacy. Thus the right to privacy, defined as one of the basic human rights in international sources, is not limited only to the international scene. In the constitutions of many countries, including the Constitution of the Republic of North Macedonia,[9] a guarantee is provided for the right to privacy, which confirms it as an important and universal right at the national level. In the constitution as the highest legal act, in the section dedicated to human rights and freedoms, protection of the right to privacy is ensured. Thus, in Article 25, every citizen is guaranteed respect and protection of the privacy of his personal and family life, dignity, and reputation.

Going deeper into the very content and concept of the right to privacy, it is clearly a complex right with no universally accepted definition. However, in the broadest sense, it represents the right of every individual to live, develop, and realise himself as a person without illegal interference from the state and other natural and legal persons. This right, in specific cases, also requires an active role by the state in creating conditions for its realisation, and providing protection in case of its violation.

7 Guide on article 8 of the European Convention on Human Rights, Rights to respect for private and family life, home and correspondence, 31 August 2022.

8 The law on the ratification of the Convention for the protection of individuals with Regard to Automatic Processing of Personal Data (Official Journal – International Agreements 7/2005).

9 Constitution of the Republic of North Macedonia (The decision to promulgate the constitution, 17.11.1991).

3.
The Right to Privacy in Working Relationships

The right to privacy is a broad concept that includes the protection of individual freedom and the relationship between the individual and society.[10] Hence, in each legal system and country the content of this right may be defined in different ways, but its essence remains unchanged. The right to privacy – like other civil-political rights – aims to protect the private sphere of individuals in relation to the state, but with the development of working life and the fact that people spend considerable time at the workplace, a serious question arises about protection of employees privacy. Today, labour relations are intertwined with the right to privacy where workers are exposed to various aspects of surveillance, monitoring, and data collection in the workplace. In this context, balancing workers' right to privacy with employers' need to ensure efficient work and job security becomes a challenge.

To ensure that workers' privacy is protected, many states have enacted laws governing the collection and use of workers' personal information, as well as workplace surveillance and monitoring procedures. In the Macedonian legal system, the Law on Personal Data Protection[11] takes a central place. This law aims to protect the right to privacy and other human rights of all citizens. This law, adapted from European legislation, was adopted in February 2020, and enables the state to monitor progress in the area of personal data protection. It also introduces the standards and principles of the European Union, specifically the General Data Protection Regulation (GDPR).[12] In addition, in 2022 the methodology for harmonising departmental legislation with the Law on Personal Data Protection was adopted. This methodology ensures consistency and compliance with the law in the various sectors and departments of the state. Although this law does not specifically regulate the right to privacy of employees as such, these provisions are appropriately applied to workers when it comes to protecting the right to privacy and personal data. It is evident that employers automatically or semi-automatically collect various information about their employees in the

10 Jernej, 2005, p. 44.

11 The Law on Personal Data Protection (Official Gazette of the Republic of North Macedonia No. 42/20, 294/21), in the following text LPDP.

12 As technology advanced and the internet was developed, the European Union (EU) recognised the necessity for contemporary data protection measures. Subsequently, Europe's data protection authority announced the need for a comprehensive approach to personal data protection within the EU. This initiative led to the revision of the 1995 directive. The General Data Protection Regulation (GDPR) was implemented in 2016 after receiving approval from the European Parliament, and starting from May 25, 2018, all organisations were mandated to ensure compliance with its provisions.

course of employment, effectively processing personal data.[13] Consequently, employers are obligated to adhere to legal requirements for data processing according to the LPDP: processing must be lawful (based on written consent or another legitimate and authorised basis); the processing method should be legal; and data should be proportionate and up to date.

The Law on Labour Relations[14] sets the foundations of labour relations, however the legislator did not recognise the need for a more detailed regulation of the issue related to the right to privacy of workers. The need for a more detailed regulation of this issue is often untouched, and the law only briefly mentions it in a few provisions. The first, Article 43, sets an obligation for the employer to protect and respect the personality and dignity of the employee, as goods from the sphere of private life. The second provision, Article 44, establishes the rules for the collection, processing, use, and delivery of workers' personal data. This limits the collection and use of the employee's personal data only if it is determined by law, or if it is necessary for the exercise of rights and obligations from the employment relationship or in connection with the employment relationship. However, these provisions represent principles rather than clear practical guidelines, therefore the issue of protection of the right to privacy of workers remains outside the scope of the Law on Labour Relations. Therefore, the key regulation for analysis when it comes to this issue in the Macedonian legal system is the Law on Personal Data Protection.

Employee privacy rights are rules that limit the extent to which an employer can search an employee's property or person, monitor their activities or conversations, or obtain information about their personal life, especially in the workplace.[15] The nature and extent of protection of these rights have become increasingly important in recent years, especially with the development of the internet and social media.

In this area, three aspects of the employees' right to privacy can be distinguished, from where their protection can be threatened. The first refers to the protection of personal data, which is the most frequently discussed aspect in the legal field, as well as in the theory of labour law.[16] In addition, the privacy of employees can be defined by factors related to their private life, especially in the context of establishing and terminating the employment relationship. Finally, the danger to the privacy of the employees increases in the sphere of the surveillance carried out by the employer during the work process.[17] The greatest danger to the privacy of employees arises

13 Danilović, 2017, p. 170.
14 Law on Labor Relations of the Republic of Macedonia (Official Gazette No. 62/2005; 106/2008; 161/2008; 114/2009; 130/2009; 149/2009; 50/2010; 52/2010; 124/2010; 47/ 2011; 11/2012; 39/2012; 13/2013; 25/2013; 170/2013; 187/2013; 113/2014; 20/2015; 33/2015; 72/2015; 129/2015 and 27/2016).
15 Employee Privacy Rights: Everything You Need to Know.
16 Jašarević, 2016, pp. 263-282.
17 Jovanović and Božičić, 2018, p. 861.

from the unequal relationship between the employee and the employer. One of the basic elements of the working relationship is subordination, that is, the existence of an imbalance of positions in the context of working relationships. Specifically, that would mean the performance of work tasks by the employee under the authority of the employer. More precisely, during the exercise of managerial powers, the most possible danger is the violation of the employee's privacy. With the development of technology, the violation of the right to privacy becomes an essential concern in the workplace, because it provides the employer with various options for managing and monitoring the work process. However, one form of surveillance attracts particular attention, and that is video surveillance.[18] By using video surveillance, employers control the work process and workers in real-time. This can be considered an effective method of monitoring, but it can also be a potential violation of employee privacy, especially if not applied with appropriate restrictions and legal frameworks.

4.
Video Surveillance

In today's fast-paced corporate world – where the need for safety, productivity, and workplace compliance is paramount – video surveillance has emerged as a powerful tool for employers. The implementation of video surveillance systems in the workplace is becoming more and more common, promising increased security, optimisation of operational processes, and protection of valuable assets. However, this also raises significant questions about privacy, ethics, and the delicate balance between protecting organisational interests and respecting the rights and dignity of employees.

The establishment of video surveillance in the workplace is mainly justified from the aspect of security – to detect and prevent potential security risks, and to sanction persons who threaten both the public and private aspects of security. This system was initially introduced in the public sector in the 1960s,[19] and was extended to the private sphere in the form of business premises, where it reached its full momentum during the 1990s.[20] Bringing this type of surveillance into the workplace raises questions about its expediency and impact on workers.

The introduction of video surveillance creates a complex situation where legitimate employer interests – such as ensuring a safe working environment and protecting property – conflict with the employee's right to privacy. In situations where these

18 Ibid.
19 Žarkoviћ, 2015, p. 170.
20 Potokar and Androić, 2016, p. 150.

two valid interests collide, and it becomes evident that workplace video surveillance can infringe upon an employee's private life,[21] restrictions on the employer's supervisory authority become necessary to safeguard employees' privacy rights.

It is crucial to address several significant principles according to European legislation. Firstly, to establish spatial and temporal constraints in the operation of video surveillance. Concerning the workplace, the use of video surveillance has no place within the employer's premises where the work process is not directly conducted. When it comes to time limits, video surveillance should be reserved exclusively for the duration of the employee's working hours. This further implies that continuous video surveillance within the work process is inappropriate. Such limitations are not only in line with safeguarding employees' right to privacy, but also relate to the adverse effects of constant exposure to surveillance on employees' mental well-being.[22]

Transparency also represents a fundamental component of permissible video surveillance. This means that employees must receive written notifications prior to its establishment.[23]

The issue of secret video surveillance in the work process is particularly sensitive. Its presence inherently suspends the principle of transparency. It is generally prohibited, but exceptions exist in specific, exceptional cases, primarily related to situations where there is reasonable suspicion of criminal activity.[24] Before covert recording is carried out, a privacy impact assessment should be carried out to ensure that it is necessary and proportionate to the discovery of criminal activities in the workplace. Where covert video surveillance is installed to monitor criminal activity, then it cannot be used for other purposes (for example, to monitor the work of employees). It is clear that a decision on reasonable suspicion of criminal activity cannot be left to the employer alone. Employees have a right to privacy, which can be limited if justified and proportionate to the intended goal. The jurisprudence of the European Court of Human Rights introduces the concept of 'reasonably expected privacy' to assess the admissibility of employer interference with employees' private lives, considering the interests of both parties.[25]

When it comes to secret video surveillance in the workplace, it is clear that the decision on its permissibility will depend on the circumstances of each specific case. This is also the conclusion reached by the European Court, which grappled with

21 This position will be taken by the European Court in the case *Köpke v. Germany (dec.)* - 420/07.
22 Jovanović and Božičić, 2018, p. 864.
23 More about the specific conditions for the introduction of video surveillance in the member states of the European Union in: Hendrickx, 2001, pp. 110-111.
24 Jovanović and Božičić, 2018, p. 865.
25 Danilović, 2017, p. 176.

this issue in the case of Köpke v Germany.[26] In this case, the court highlighted that in a scenario where the legitimate interests of the employer and the rights of the employee are in conflict, 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.

In practice, the introduction of video surveillance requires a thorough legal analysis to achieve a balance between employer interests and employee rights. Once this analysis demonstrates the appropriate equilibrium, internal policies, procedures, and notifications should be established to inform employees of all aspects related to the processing of personal data through surveillance applications.

Only after completing these steps and ensuring a proper balance between employer interests and employee rights should the employer consider implementing video surveillance.

5.
Video Surveillance Installation Under the Macedonian Legal Framework

As previously mentioned, in the Macedonian legal system the issue of video surveillance in the workplace is not specifically regulated by the Law on Labour Relations. Also, there is no separate legal act dedicated exclusively to this topic. However, personal data protection and workplace video surveillance are regulated by the Personal Data Protection Law. This law ensures the rights of persons to whom personal data refers, and sets provisions for the collection, processing, and protection of this data. In the employment relationship, the employer processes the personal data of the employees to fulfil various purposes. In that relationship the employer has the role of a controller with all his powers and obligations, and the employee has the role of a subject of personal data with all their rights. The Law on Personal Data Protection contains provisions that are important for the installation of video surveillance and work at the workplace. The provisions of this law define rules for the processing of personal data, including cases where video surveillance is used for control and security. In the following, aspects regarding the establishment of video surveillance systems at the workplace will be considered in accordance with the legal regulations.

26 *Köpke v. Germany (dec.)* - 420/07. The applicant, a supermarket cashier, was dismissed without notice for theft, following a covert video surveillance operation carried out by her employer with the help of a private detective agency. She unsuccessfully challenged her dismissal before the labor courts.

5.1. Analysis or Periodic Evaluation of the Objective(s)

Before starting the process for establishing a video surveillance system, the controller – i.e. a natural or legal person, a state authority, a legal person established by the state for the exercise of public powers, an agency, or another body, which independently or jointly together with others determines the goals and the method of personal data processing – is obliged to perform an analysis of the goal – i.e. the goals for which the video surveillance is established.[27] The analysis contains the reasons for setting up video surveillance with an explanation of the need to fulfil the goal, as well as a description of movable and immovable objects, i.e. the space that will be protected by video surveillance.

The analysis must also contain the opinion of the personal data protection officer.[28] Based on the prepared analysis and the opinion received from the personal data protection officer, the responsible person decides upon the establishment of a video surveillance system in a separate document.

The controller is obliged to perform a periodic assessment of the results achieved by the video surveillance system every two years. These especially regard the further need to use a video surveillance system, the purpose or objectives of video surveillance, and possible technical solutions for replacing the video surveillance system. From the performed evaluation, the controller must make a report, which is an integral part of the documentation for the establishment of video surveillance.[29]

5.2. Defining the Objectives for the Establishment of Video Surveillance

According to the legal provisions, the controller can perform video surveillance on official or business premises if it is necessary to protect the life and health of people; to protect property; protect the life and health of employees due to the nature of the work; or to provide control over entry and exit from official or business premises, for security purposes.[30] The controller can perform video surveillance only on the premises that are necessary to achieve specific goals. For example, if the goal is to protect property or control access from official or business premises, video surveillance should be limited to the entrance of the building, and not to internal parts such as kitchens, offices, corridors, meeting rooms, etc. When setting up video surveillance at the entrance or exit from the facility (the company/state institution), the controller

27 Article 92, paragraph 1, LPDP.
28 Rulebook on the content and form of the act on the method of performing video surveillance (RSM Official Journal, no. 122 of 12.5.2020), article 7 paragraph 3.
29 Article 92, paragraph 3, LPDP.
30 Article 90, paragraph 1, LPDP.

should make sure that cameras are directed only to the property of the company/state institution – i.e., that they are not directed onto public areas, neighbouring facilities, etc. When setting up video surveillance, it is essential to protect the right to privacy of all persons, employees, customers, parties, and other subjects of personal data. Precisely for this reason, the controllers should be especially careful when directing the cameras and when choosing the locations for video surveillance, to avoid private rooms such as wardrobes, dressing rooms, sanitary units, and other similar rooms.[31] Employees should not be under constant video surveillance. The camera should be placed so that it does not cover the workspace where the employees work. Video surveillance must not be set up for the purpose of control – i.e. for the purpose of monitoring the efficiency of employees.

On the one hand, the establishment of video surveillance by the employer has a legitimate purpose, which is manifested in the need to ensure safety in the work process, but also in the protection of property. However, even in such situations video surveillance should be seen as an emergency measure, which should only be considered if there is no alternative method less invasive to the privacy of employees. Concrete measures that could be effective against break-ins and thefts, as well as video surveillance systems, are the installation of security alarm systems, good lighting, use of porters, many security guards, installation of security locks, protective windows, etc.

To protect the personal data that it collects, processes, and stores, the controller must take appropriate technical and organisational measures and regulate the way video surveillance is performed with a special act to prevent possible unauthorised access to the data.[32] This means that only the controller has the right to monitor in real-time, and in case of an incident review the material. Stored data must be kept locked, with access available only to the controller.

For performing video surveillance, the controller should prepare a special act (regulations, policy, procedure) which will regulate in detail the way of performing video surveillance. This act should describe the system for performing video surveillance, the purpose (i.e. the purposes of personal data processing), categories of personal sub-flows, technical and organisational measures to ensure the security of personal data processing, authorised persons for personal data processing, deadlines for keeping the recordings, the method of reporting and exercising the rights of the subjects of personal data, technical specification of the equipment, as well as a plan of where the video surveillance system is set up.[33]

31 Article 90, paragraph 3, LPDP.

32 Rulebook on the content and form of the act on the method of performing video surveillance (RSM Official Journal, no. 122 of 12.5.2020), Article 9, paragraph 1.

33 The content and form of this act are prescribed by the director of the Agency for the Protection of Personal Data by adopting a separate bylaw.

5.3. Obligation for Transparency and Reporting

The law on the protection of personal data introduces the principle of transparency in the establishment of video surveillance, which means that the subjects of personal data should be informed in detail about when and how their data is processed. This includes detailed information about the locations being filmed and the CCTV reporting – which should be clear, visible, and easily accessible to all stakeholders.[34] The notification should contain information about where the video surveillance is performed, the name/title of the controller who performs the video surveillance, the way in which information can be obtained, and about where and for how long the recordings from the video surveillance system are kept.[35]

The controller is obliged to inform the employees about performing video surveillance on official or business premises.

5.4. Storage Periods and Obligation to Delete

The recordings made during video surveillance are kept until the objectives for which it is carried out are met – not longer than 30 days, unless a longer period is provided by another law. This means that these recordings can be stored for longer than 30 days only if another law provides for a longer period, which includes measures to protect the rights and freedoms of subjects, but no longer than after the fulfilment of the goals.[36] Video recordings can be stored for a longer period than 30 days when it is necessary to realise the controller's legitimate interest in conducting appropriate procedures in accordance with the law – for which the controller establishes internal procedures for the method of storing and deleting the recordings.[37]

Video recordings may not be made available to other people, unless it is necessary in a possible evidentiary procedure. For example, the controller may not make the photos available or sell them to another person.

5.5. The Basic Rights of Employees, or the Subjects of Personal Data

In the act of performing video surveillance, the controller prescribes the method of exercising the rights of the subjects whose data is processed through the video

34 Article 89, paragraph 3, LPDP.
35 Article 89, paragraph 4, LPDP.
36 Article 89, paragraph 8, LPDP.
37 Rulebook on the content and form of the act on the method of performing video surveillance (RSM Official Journal, no. 122 of 12.5.2020), article 11 paragraph 3.

surveillance system, in order to familiarise them with the method of providing transparent information, communication, and the exercise of their rights, information and access to personal data, as well as the exercise of the right to correction and deletion, the right to object, and the automated adoption of individual decisions.[38]

5.5.1. Right of Access

Employees have the right to confirmation from the controller as to whether their personal data is being processed.[39] In the case of real-time monitoring without data storage, the controller may inform them that no personal data is processed after the monitoring is completed. If the data processing is still ongoing during the request – i.e. if the data is stored or continuously processed in any other way – the employee has first access to the recordings and corresponding information. However, there are several limitations to the right of access, such as when identification of the individual is impossible, or the request is unfounded. In such a case, the controller must inform the employee about the same. Also, an indefinite number of individuals may be recorded in the same video surveillance sequence, in which case the controller should take measures to obscure the faces of the individuals who are not the subject of the access request.

5.5.2. Right to Erasure

The employee has the right to ask the controller to delete his personal data, while the controller has the obligation to delete personal data within 30 days from the day of submitting the request for deletion if one of the following conditions is met: personal data is not required for the purposes for which they were collected or processed; whenever consent is withdrawn (and there is no other legal basis for processing); the employee files an objection to the processing; personal data was illegally processed; personal data should be deleted in order to comply with an obligation established by law that applies to the controller; personal data was collected in connection with the offer of information society services, in accordance with the legal provisions.[40]

38 Ibid, article 13, paragraph 1.
39 Article 19, LPDP.
40 Article 21, LPDP.

5.5.3. Right to Object

For video surveillance based on legitimate interest, or for the need to perform a task of public interest, the subject of personal data has the right to object at any time, based on a specific situation. Hence, the controller may not carry out further processing of personal data, unless it proves that there are relevant legitimate interests for processing which prevail over the interests, rights, and freedoms of the subject of personal data, or for the establishment, exercise, or defence of legal claims.[41]

6.
Conclusion

Video surveillance and workplace monitoring are on the rise in Macedonia, reflecting the employer's managerial authority and the employment relationship's subordination dynamics. The powers and rights of the employer, as the owner of the capital, determine the employment relationship as a relationship of subordination. In this regard, the right of the employer to organise and control the work of the workers is recognised, thus exercising legitimate managerial authority. While employers possess the legitimate authority to oversee their workforce, it is essential to define the limits of this supervision – especially concerning video surveillance – which can be the most intrusive form of monitoring and a potential threat to employees' privacy. Legal standards, as presented in this paper, establish the parameters within which this balance should be maintained.

In this regard, it is essential to highlight that the legislative framework in Macedonia, concerning the protection of privacy and personal data, aligns with European legal standards. It is in harmony with the principles established in European legislation. It outlines the necessary steps and legal requirements for the installation of video surveillance, with a strong focus on respecting the basic principles. The primary purpose of the provisions on privacy and protection of personal data, in this sense, is to regulate, limit, and condition the supervision to ensure that when surveillance is already carried out – which is *de facto* an invasion of privacy – that invasion is necessary, legal, fair, transparency and proportionate. The employer must respect the principle of proportionality in relation to the purpose for which the video surveillance is installed.

It is important to note that, in Macedonia, there is still no developed case law that sets the framework and interprets the legislation in this area. This creates a challenge and a longer process of development and establishment of standards for video surveillance and control of workplaces.

41 Article 25, paragraph 1, LPDP.

Bibliography

- Danilović, J. (2017). The right to privacy at work: Annals of the Faculty of Law in Belgrade, year LXV, 2/2017, p.162-182.
- Employee Privacy Rights: Everything You Need to Know, Available at: https://www.upcounsel.com/employee-privacy-rights/ (Accessed: 15 August 2023).
- F. Hendrickx, F. (2001). Protection of workers' personal data in the EU: surveillance and monitoring at work, pp. 110-111.
- Jernej, R., (2005). *The private and the public in the media, Regulation, and Implementation in Slovenia*, published by: Peace Institute, edition: Mediawatch, Available at: http://mediawatch.mirovni-institut.si (Accessed: 5 September 2023).
- Jašarević S. (2016). *New tendencies in the field of personal data protection at work in international and European law, thematic collection Harmonization of Serbian and Hungarian law with the law of the European Union*, book 4, Faculty of Law in Novi Sad, pp. 263-282.
- Jovanović, P., Božičić, D., (2018), *Right employee on privacy as security segment and health at work*. Faculty in Law at University in Novi Sad: Legal tradition and new legal challenges, pp.855-868, doi:10.5937/zrpfns52-20000.
- Neuwirth, K. (2007) *Privacy as a basic human right*, Skopje: Foundation Metamorphosis, (Metamorphosis ICT Guide; No. 3), ISBN 978-9989-2451-7-6.
- Potokar, M., Androić, S., (2016). *Video Surveillance and Corporate Security, Journal of Criminal Justice and Security*, No. 2/2016, p. 150.
- **Žarkoviћ, I., (2015),** *Measuring electronic surveillance of employees and the right to privacy at the workplace*, Science, security, police, no. 3/2015, p.170.

Legal sources

- Case of Köpke v Germany (Application no. 420/07), European Courts of Human Rights, October 2010.
- Constitution of the Republic of North Macedonia (The decision to promulgate the constitution, 17.11.1991).
- The Universal Declaration of Human Rights was adopted and published in Resolution 217 A(III), of December 10, 1948, by the United Nations General Assembly.
- The International Covenant on Civil and Political Rights was adopted and open for signature and ratification or accession by resolution of UN General Assembly 2200 A(XXI) of December 16, 1966. Entered into force on the 23rd. March 1976.
- The Convention for the Protection of Human Rights and Fundamental Freedoms. Rome, 4.XI.1950.

- The General Data Protection Regulation (Official Journal L 119 of the European Union, Volume 59, 4 May 2016).
- The Guide on Article 8 of the European Convention on Human Rights, Rights to respect for private and family life, home and correspondence, 31 August 2022.
- The law on the ratification of the Convention for the protection of individuals with Regard to Automatic Processing of Personal Data (Official Journal – International Agreements 7/2005).
- The Law on Labor Relations of the Republic of Macedonia (Official Gazette No. 62/2005; 106/2008; 161/2008; 114/2009; 130/2009; 149/2009; 50/2010; 52/2010; 124/2010; 47/ 2011; 11/2012; 39/2012; 13/2013; 25/2013; 170/2013; 187/2013; 113/2014; 20/2015; 33/2015; 72/2015; 129/2015 and 27/2016).
- The Law on Personal Data Protection (Official Gazette of the Republic of North Macedonia No. 42/20, 294/21).