Giorgi Khorbaladze[*]

Video Monitoring of an Employee's Work Process/Space

The primary objective of the Law of Georgia "On Personal Data Protection" is to safeguard the rights to privacy, family life, personal space, and the inviolability of communication. Video monitoring constitutes one of the forms of personal data processing. To ensure the protection of an employee's rights as a data subject—particularly the right to personal autonomy—and to lawfully implement video monitoring of the workplace and work processes, it is essential to consider a range of legal aspects established under the Law on Personal Data Protection.

This paper examines the legislative framework governing the implementation of video monitoring in the workplace, alongside the relevant practices of the Personal Data Protection Service, supervisory authorities in European jurisdictions, and the European Court of Human Rights. Additionally, it addresses specific legal considerations pertaining to the video monitoring of employees' workspaces and work processes, as well as the key obligations of Controller to process such data.

Keywords: *Personal data, workspace/process, workplace, video monitoring, data security, impact.*

[*] Master of Law at Ivane Javakhishvili Tbilisi State University. Lawyer of the Office of the President of the Personal Data Protection Service of Georgia.

1. Introduction

The right to respect for private and family life is a fundamental human right enshrined in the Constitution of Georgia. The principle of personal autonomy is regarded as the cornerstone of the right to privacy[1], which is intrinsically linked to the concept of personal data as a critical component of this right. As long as individuals exist, personal data will exist. Consequently, in any democratic state, the protection of an individual's private life, as a supreme value, must be treated as a priority.

Despite the paramount importance of safeguarding private life, both national and international legal frameworks recognize that this right is not absolute. In certain circumstances, restrictions on this right are permissible. Given the inherently competing nature of human rights, it is essential to maintain a fair balance between them, necessitating a case-by-case assessment and analysis by the relevant authority or decision-maker. The right to the protection of personal data is frequently juxtaposed with the right to freedom of speech and expression. To ensure a fair equilibrium between these rights, the adjudicating body or individual must conduct a comprehensive examination of the specific circumstances and assess them in accordance with the principle of proportionality. A restriction imposed by the state on a fundamental right is justified only if it is prescribed by law, serves a legitimate aim, and is necessary in a democratic society.

One of the primary national legislative acts governing the protection of fundamental human rights and freedoms—particularly the rights to privacy, family life, personal space, and the inviolability of communication—is the Law of Georgia "On Personal Data Protection". Among other matters, this law regulates the processing of personal data through video monitoring in various private and public spaces. Given the broad scope of privacy protection, this study aims to examine a specific aspect of video monitoring—namely, the video monitoring of an employed individual's workspace and work process.

Accordingly, this study will analyze the legislative framework governing this issue, elucidate the concept of an employee's workspace and work process, and outline the standard of a reasonable expectation of privacy. Furthermore, the core section of the study will present relevant best practices derived from the Personal Data Protection Service, European Data Protection Supervisory Authorities, and the European Court of Human Rights.

[1] *Case of Pretty v. the United Kingdom*, [2002] ECHR App. No. 2346/02, §61.

2. Legislative Regulation of the Implementation of Video Monitoring

Video monitoring is the processing of visual image data using the technical means located/installed in a public or private space, including video control and/or video recording (except for covert investigative actions)[2].

Unlike the Law "On Personal Data Protection" that was in force on March 1st, 2024, the previous Law of December 28, 2011, did not explicitly include the concept of video monitoring, although it recognized video recording as a form of data processing. With the objective of aligning with European legislation, the new Law of Georgia "On Personal Data Protection" comprehensively regulates matters related to video monitoring, including the legal grounds for conducting video monitoring of an employee's workspace or work process.

Video monitoring constitutes a permissible form of personal data processing if it is conducted for specific purposes, such as the prevention and detection of crime, ensuring public security, protecting the safety of individuals and property, safeguarding minors (including protection from harmful influences), protecting confidential information, conducting examinations or testing, or fulfilling other tasks related to public and/or other legitimate interests. However, the implementation of video monitoring must be an adequate and proportionate means of achieving the intended purpose of data processing[3].

The purpose of implementing video monitoring in an employee's workplace may vary depending on the nature of the work process, the specific characteristics of the workspace, and other relevant factors[4]. In certain cases, based on the nature of the work being performed, the employer may even be obligated[5] to implement video monitoring[6]. Given the diverse and dynamic nature of labor relations, the current legal framework grants the personal data protection supervisory authority the discretion to assess, on a case-by-case basis, the legitimacy of an employer's interest in conducting video monitoring,

[2] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 3, subparagraph "g".
[3] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 10, Paragraph 1.
[4] For example, Article 20, Paragraph 17 of the Law of Georgia on General Education stipulates that video surveillance shall be implemented on the external and internal perimeters of schools for the purpose of ensuring the safety of individuals and protecting minors from harmful influences.
[5] See, for example, Order No. 1143 of the Minister of Internal Affairs of Georgia of August 29, 2007, "On the approval of video surveillance systems and the rules for their installation and operation at gambling and other profitable games (except for promotional draws) and on the external perimeters".
[6] *Takashvili S.,* Personal Data Processing Standards for Video Monitoring of an Employee's Workplace, Law Methods, №8, 2024, 129.

even when such an interest is not explicitly specified in the law but falls within the broader category of "other legitimate interests."

By contrast, the legal framework in force prior to March 1st, 2024, limited the permissible purposes for workplace video surveillance to personal and property security, the protection of confidential information, and the conduct of examinations or testing[7]. Thus, the current regulation under the Law "On Personal Data Protection" provides greater flexibility for assessment, enabling the resolution of complex legal issues in a lawful and equitable manner.

In the field of personal data protection, the Council of Europe Convention No. 108 of January 28, 1981, For the Protection of Individuals with regard to Automatic Processing of Personal Data, along with its modernized version, holds significant importance. The primary international legal instrument governing the processing of personal data is the European Union's General Data Protection Regulation (hereinafter referred to as the "GDPR"). Notably, while neither the aforementioned conventions nor the GDPR establish specific rules for processing personal data through video surveillance, they explicitly state that when processing data by such means, the Controller or Processor must comply with obligations to safeguard the dignity, legitimate interests, and fundamental rights of the data subject.

Accordingly, when assessing the lawfulness of processing an employee's personal data through video monitoring, data protection supervisory authorities (DPAs) rely on national legislation, European conventions, and the relevant provisions of the GDPR, which establish the principles and general rules governing personal data processing.

3. Employee's Workspace/Process

An employee, like an employer, is a party to an employment relationship. An employee is a natural person who, under an employment contract, performs specific work for an employer. Additionally, an employee may also hold the status of a public servant, as defined by the Law of Georgia On Public Service.[8]

[7] Law of Georgia "On Personal Data Protection", 5669-RS, 28/12/2011, Article 12, Paragraph 3.
[8] Organic Law of Georgia "Labor Code of Georgia", 4113-RS, 17/12/2010, Article 3, Paragraph 3. Also, according to Subparagraph "d" of Article 3 of the Law of Georgia "On Public Service", a public servant is a professional

The Law of Georgia On Labor Inspection provides definitions of an employee and their workplace/place of work. According to subparagraphs k and l of Article 3, a workplace is defined as a specific location where an employee directly performs labor activities, whereas a place of work encompasses all workplaces and the surrounding area where an employee or any other individual is present or moves for official purposes and which is directly or indirectly controlled by the employer[9]. A similar definition is found in Resolution No. 341 of the Government of Georgia, dated July 1, 2022, "On Approval of Technical Regulations on Minimum Requirements for Safety and Health Protection in the Workplace". This resolution also distinguishes between open and closed workspaces. However, due to the potential specificity of different workplaces and workspaces, various subordinate normative acts provide differing definitions of similar terms.[10]

With regard to the work process, it pertains directly to the employee's professional activities and may vary in terms of duration, the nature of the work performed, and other relevant factors. The work process may take place not only in enclosed spaces but also in open-air environments, as evidenced by a case examined by the Personal Data Protection Service concerning the legality of data processing for employees in a particular company[11].

According to the circumstances of the case, the company, through a processor, conducted video monitoring of employees working in outdoor spaces using security cameras, citing a high risk of harm to employee health as justification. During the investigation, it was established that these outdoor areas were designated for the execution of the employees' primary official duties and responsibilities. However, due to non-compliance with workplace video monitoring regulations—specifically, the company's failure to develop a written document governing the implementation of video monitoring—the company was found to be in violation of the law under Article 69 of the Law on Personal Data Protection. Accordingly, despite variations in work processes, the law provides equal protection for employees' personal data, ensuring compliance with established data protection standards.

civil servant/public official/civil servant, a person employed under an administrative contract, a person employed under an employment contract.

[9] See Recommendations on the Implementation of Video Monitoring and Audio Monitoring, 2024, 8.

[10] For example, Order No. 104/N of the Minister of Education and Science of Georgia of December 29, 2021, Article 3, Subsection "d".

[11] Decision No. G-1/340/2024 of the President of the Personal Data Protection Service of November 20, 2024.

4. The Standard of Reasonable Expectation of Privacy

The new Law “On the Personal Data Protection” expressly prohibits the implementation of video monitoring in any space where an individual has a reasonable expectation of privacy.[12]

The determination of a reasonable expectation of privacy is not based on the subjective perception of an individual but rather on the perspective of an objective observer or a third party[13]. In the workplace, such an expectation objectively exists in specific spaces, including areas designated for hygiene. Additionally, in cases where the nature of the work requires the presence of changing rooms, the Law on Personal Data Protection categorically prohibits video monitoring in such areas without exception. The implementation of video monitoring in these and similar spaces is deemed to be in violation of generally accepted moral standards. However, given the impossibility of exhaustively listing all such spaces under the Numerus Clausus principle, the legislator introduced the concept of a reasonable expectation of privacy as a guiding standard for assessing the permissibility of video surveillance in different workplace environments.

In addition to the aforementioned cases, an employee may also have a reasonable expectation of privacy in workplace spaces such as kitchens, where employees typically spend time during breaks. This expectation of privacy is equally reasonable in workplaces with day and night shifts, such as medical institutions or security companies, where rest areas are provided for employees[14].

"In certain environments, a person has a legitimate expectation of privacy and respect."[15] As a result, due to the heightened need for privacy in these spaces, the legislator explicitly prohibits video monitoring in such areas without exception. Consequently, Article 69 of the Law “On Personal Data Protection” imposes a stricter penalty in the form of a fine if the person responsible for data processing conducts video monitoring in an area where the data subject has a reasonable expectation of privacy.

[12] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 10, Paragraph 4.
[13] European Data Protection Board (EDPB), Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, Adopted on 29 January 2020, §36.
[14] For example, Order No. 06/n of the Minister of Education, Science, Culture and Sports of Georgia of January 29, 2019, “On the Approval of the Rules and Conditions for Maintaining Security and Public Order in a General Educational Institution,” establishes that video surveillance is prohibited in school restrooms, changing rooms, classrooms, and teacher's rooms.
[15] *Case of Von Hannover v. Germany,* [2004] ECHR App. No. 59320/00, §51.

5. The Importance of the Ultima Ratio Principle in Video Monitoring of an Employee's Workspace/Process

According to Article 10, paragraph 3 of the Law “On Personal Data Protection”, video monitoring of an employee's work process or workspace is only permitted in exceptional cases, where the objectives defined by law cannot be achieved through other means or would require disproportionate effort. The legal and legitimate grounds for implementing video monitoring are outlined in Article 10, paragraph 1 of the law, including purposes such as the protection of personal safety and property, public safety, and others.

However, in order for video monitoring of the work process or workspace to be deemed lawful, the legislator sets higher standards. In addition to having a legitimate purpose, the person responsible for data processing must demonstrate that the intended objective cannot be achieved by alternative means or that using such alternatives would entail disproportionate effort. Therefore, video monitoring of the workplace or work process, as an Ultima Ratio, is permissible only in exceptional circumstances, where no other logical, less intrusive alternative exists that would justify interfering with the right to privacy.

For a practical examination of this issue, it is useful to analyze the legality of video monitoring implemented by a private school as part of a planned inspection conducted by the Personal Data Protection Service[16]. According to the circumstances of the case, video monitoring was carried out in the school's computer science classroom. The school representative explained that the purpose of the video monitoring was to protect property, ensure security, and identify individuals causing damage. Additionally, the monitoring was carried out for testing purposes as part of periodic educational projects.

During the inspection, it was revealed that the school had an agreement on a "Security Rule" with the Ministry of Education, which, among other matters, explicitly stated that video monitoring in classrooms was inadmissible. As a result, aside from the violation of this specific rule, the Service's assessment determined that video monitoring in the computer science classroom was not an adequate or proportionate means of achieving the stated objectives. The protection of property, security prevention, and identification of individuals responsible for damage could have been accomplished through alternative measures, which were already outlined in

[16] Decision No. G-1/342/2024 of the President of the Personal Data Protection Service of November 22, 2024.

contracts with teachers. These contracts included provisions for protecting material assets and the designation of a responsible person/supervisor for the items. Regarding the testing purpose, despite the fact that such an objective is explicitly mentioned in the first paragraph of Article 10 of the Law "on Personal Data Protection", it was determined that the goal of monitoring the testing process could only be effectively achieved by video monitoring the process directly. The video monitoring carried out before and after the testing, however, exceeded the stated purpose. Therefore, in accordance with Article 69 of the Law (regarding violations of video monitoring implementation rules), the school was found to be in violation.

An educational institution is a space where both pupils/students and employees (e.g., teachers, lecturers) are engaged in the learning process. As such, the spaces within these institutions simultaneously serve as workplaces for employees. Therefore, the purpose for implementing video monitoring must justify any interference with personal privacy. The European Court of Human Rights, in the case Antović and Mirković v. Montenegro, clarified that the auditorium is the workplace of lecturers, where they not only teach students but also interact with them and contribute to the development of their social identity. Since the supervision of the learning process was not a purpose expressly permitted by national legislation, and no genuine need to protect the safety of individuals was identified, the Court ruled that the video monitoring of auditoriums violated Article 8 of the European Convention on Human Rights.[17]

The importance of the *Ultima Ratio* principle is clearly demonstrated in another decision by the Personal Data Protection Service[18], in which a college (the controller) implemented video monitoring through cameras located in several auditoriums (including a workshop, sewing room, and integrated laboratory). The controller justified the monitoring of these spaces as a measure to protect expensive equipment and inventory. However, the decision emphasized that the auditorium, by its nature, serves as a learning space for students and a work space for teachers, where interactions extend beyond academic topics to include personal and general matters.

While the protection of property is considered a legitimate goal, the decision highlighted that there were alternative means to achieve this goal. Specifically, the college conducted an annual inventory, and the contracts with teachers included provisions making them responsible for the material property of the college. The same objective could have been achieved by

[17] *Case of Antović and mirković v. Montenegro*, [2017] ECHR App. No. 70838/13, §44, §55-§60.
[18] Decision No. G-1/346/2024 of the President of the Personal Data Protection Service of November 26, 2024.

designating a responsible person for the items, storing valuable inventory in secure spaces, and keeping records of their use and return. Consequently, video monitoring was deemed neither a necessary nor an adequate means of achieving the college's objective. Since video monitoring was not the only feasible means to achieve the stated goal, there was no legal basis for the installation of a video monitoring system. As a result, the college was instructed to discontinue video monitoring in the classrooms.

This special regulation regarding the admissibility of video monitoring in an employee's workspace or process arises from the need to protect the right to privacy, as well as the potential "dilutive effect"[19] it may have on other fundamental rights (such as the freedom of assembly). Therefore, in addition to the existence of a legitimate interest, video monitoring must also be an adequate and proportionate means of achieving the goal of processing employee data.

6. Main Obligations of the Data Controller and Processor

6.1. Obligation to Inform

Once the employer establishes a legal basis for implementing video monitoring in the workplace, as stipulated by the Law on Personal Data Protection, they, as the data controller or processor, shall be subject to several obligations. In accordance with Article 10, Paragraph 8 of the Law on Personal Data Protection, the data controller processor is required to place a clearly visible warning sign indicating the ongoing video monitoring[20]. Furthermore, in the case specified under Paragraph 3 of the same Article, the employer must additionally provide the employee with written notification detailing the specific purpose(s) of the video monitoring. Compliance with these requirements shall be deemed sufficient to ensure that the data subject is informed of the processing of their personal data.

Accordingly, the law unequivocally establishes that the processing of an employee’s personal data (visual images) through video monitoring is

[19] Recommendations on the Implementation of Video Monitoring and Audio Monitoring, 2024, 8.

[20] A warning sign about the ongoing video monitoring must contain an appropriate inscription, an easily understandable image about the ongoing video monitoring, and the name and contact details of the controller.

prohibited in a manner that prevents the data subject from being aware of such processing. Recognizing the significance of safeguarding the principle of transparency, the legislation imposes an even higher standard of information disclosure in cases where video monitoring is conducted in the employee's workplace or during work processes. In addition to the requirement to place a visible warning sign, the employer, as the data controller or processor, is further obligated to provide employees with written notification specifying the exact purpose(s) of the video monitoring. Consequently, failure to conduct data processing in adherence to the principle of transparency may lead to a situation where the employer's legitimate interest (e.g., ensuring the security of company property) is transformed into an unwarranted and unlawful objective[21].

The decision of the European Court of Human Rights in López Ribalda and Others v. Spain[22] holds significant importance in the context of an employer's failure to fulfill the obligation to inform an employee. According to the factual circumstances of the case, the applicants were employed as cashiers and consultants in a supermarket in Barcelona. In March 2009, the supermarket administration became aware of financial losses and, in an effort to identify the cause, decided to install video surveillance cameras. Some of the installed cameras were concealed, with their field of view directed towards the cashiers. While the company informed employees about the installation of visible cameras and placed a warning sign, it failed to notify them of the hidden cameras.

Over the course of several months, the employment relationship with 14 employees, including the applicants, was terminated due to the theft of company property. The Chamber of the European Court of Human Rights determined that Article 8 of the European Convention on Human Rights had been violated, as the employees were not fully informed about the surveillance, and a fair balance was not maintained between the right to respect for private life and the employer's interests. The respondent state appealed the decision to the Grand Chamber.

In its ruling, the Grand Chamber acknowledged that the supermarket was an open space and that transactions at the cash register were not of a private nature. However, it also recognized that the surveillance took place in the employees' workplace, raising the issue of a reasonable expectation of privacy. The Court noted that such an expectation is significantly diminished in areas

[21] *Article 29 Data Protection Working Party*, Opinion 2/2017 on Data Processing at Work, Adopted on 8 June 2017, 9.
[22] *Case of López Ribalda and others v. Spain*, [2019] ECHR App. No. 1874/13; 8567/13.

where official duties are performed in public, particularly in direct interaction with customers. Nevertheless, given that the surveillance lasted only ten days and that access to the recordings was restricted to a limited number of individuals, the interference with the employees' private life was deemed to be of low severity. Furthermore, the Court emphasized that if the employees had been informed about the surveillance, the employer's objective—identifying the cause of the theft—would not have been achieved.

The European Court of Human Rights underscored the paramount importance of informing employees and ruled that conducting covert video surveillance based on mere suspicion of misconduct was not justified. However, the Court also recognized that where there is a reasonable suspicion of employee misconduct resulting in significant financial damage, the employer may be justified in implementing such measures despite the general obligation to inform, provided that the actions are necessary to prevent the disruption of the company's operations. Accordingly, the interference with the right to privacy was ultimately deemed justified in this specific case.

The European Court of Human Rights did not establish a violation of the right to private life in another case with circumstances similar to those outlined in the aforementioned decision. This case concerned the covert video surveillance of an employee (a cashier) by the employer. The Court recognized the employer's objective—to safeguard its property and detect instances of theft—as a legitimate and substantial interest. Furthermore, it determined that this objective could not have been effectively achieved through other equally efficient means.[23]

Furthermore, the guidance issued by the UK Data Protection Authority ("ICO") on the lawful monitoring of employees stipulates that, in exceptional circumstances—such as for the prevention or detection of criminal offenses—covert video surveillance in the workplace may be permissible. However, such monitoring must be conducted strictly by authorized personnel, with due consideration given to the limited duration and scope of surveillance[24]. Additionally, a data protection impact assessment must be carried out[25]. Notwithstanding the stated purpose, covert video surveillance remains strictly prohibited in areas where employees have a reasonable expectation of privacy[26], such as restrooms, changing rooms, and similar locations.

[23] *Case of Köpke v. Germany*, [2010] ECHR, App. No. 420/07.

[24] *EDPS*, Video-Surveillance Guidelines, Brussels, 17 March 2010, 31-32 <https://www.edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf> [16.12.2024].

[25] Workplace Monitoring: What Are Your Employees' Rights? <https://gdprinformer.com/gdpr-articles/workplace-monitoring-rights> [15.12.2024].

[26] Workplace Monitoring: What Are Your Employees' Rights? <https://gdprinformer.com/gdpr-articles/workplace-monitoring-rights> [15.12.2024].

Pursuant to the Law “on Personal Data Protection”, video monitoring of an employee’s workspace or work process may be conducted for the purpose of detecting a crime. However, the law does not provide for the possibility of covert video surveillance by the data controller or processor. Instead, it unequivocally establishes the obligation to inform employees in writing as data subjects. Covert video monitoring in the workplace constitutes a serious intrusion into private life and carries the inherent risk of unlawfully obtaining other types of information related to employees’ private lives[27].

Accordingly, in light of the precedential interpretations provided by the European Court of Human Rights in the aforementioned decisions—where covert video surveillance in the workplace was deemed permissible only in exceptional circumstances—it is advisable that such measures be undertaken not by the data controller or processor, but rather by law enforcement authorities, particularly when conducted for the purpose of detecting criminal offenses

The significance of properly informing the data subject is further highlighted by the consistent practice established by the Personal Data Protection Service[28], which dictates that non-functional video cameras in the workplace are not permissible. Specifically, if a video camera is installed but not operational, the employer is obligated to either remove the camera or conduct video monitoring in accordance with the procedures established by law, which prioritize the protection and respect of private life. In such cases, the employee is not informed that their visual image is not being processed as personal data. As a result, the employee may mistakenly believe that their personal data is being processed, which could lead to an unreasonable alteration of their behavior due to perceived surveillance.

By fulfilling the obligation to inform, the principle of transparency in data processing is upheld, and personal data will be processed lawfully, provided that the employee has full awareness that their workspace or process is indeed subject to video monitoring.

[27] It may lead to liability under the Criminal Code (e.g., infringement of information reflecting private life or personal data (Criminal Code, No. 2287, Article 157).

[28] Decision No. G-1/342/2024 of the President of the Personal Data Protection Service of November 22, 2024, 18.

6.2. Obligation to Develop a Written Document

In addition to the obligation to inform the data subject, it is imperative that the data controller or processor, in accordance with the principles set forth in Article 4 of the Law on Personal Data Protection, formally document the purpose and scope of video monitoring, the duration of such monitoring, the storage period of the video recordings, as well as the procedures and conditions for accessing, storing, and destroying the recordings. Furthermore, the mechanisms for safeguarding the rights of the data subject must also be established.

Beyond ensuring transparency in the data processing process through video monitoring, the employer is further obligated to: collect or obtain personal data solely for specific, clearly defined, and legitimate purposes[29]; and process the data only for the duration and to the extent necessary to fulfill the legitimate purpose[30]. These principles form the foundation of the employer's duty to clearly outline in writing the critical aspects related to video monitoring. Although the regulatory provision does not explicitly require the provision of this written documentation to the data subject, Articles 24 and 25 of the Law “on Personal Data Protection” nevertheless impose the obligation to inform the data subject about such matters, regardless of whether the data is collected directly from the data subject.

In addition to the above, one of the guidelines issued by the United Kingdom Data Protection Supervisory Authority (“ICO”) emphasizes that, when monitoring employees for the purpose of protecting personal data, it is essential for the employer to assess the need for a data protection impact assessment. If there is a likelihood of processing special categories of data in this process, the employer is required to conduct an impact assessment[31].

The data controller is obligated to create a written document when carrying out an impact assessment in accordance with the procedure approved by Order No. 21 of the President of the Personal Data Protection Service, dated 28 February 2024. As per the same order, a high probability of creating a threat to the fundamental rights and freedoms of employees as a result of data

[29] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 4, Paragraph 1, Subparagraph "b".

[30] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 4, Paragraph 1, Subparagraphs: "c"; "e".

[31] *ICO*, Guideline on Monitoring of Workers by Employers, 2023, p. 20; 35 <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf> [20.12.2024].

processing using new technologies, data categories, volumes, purposes, and means of data processing may arise when two cumulative conditions are met. Specifically, if, for example, profiling leads to an assessment of the quality of work performed by employees, or if systematic and large-scale monitoring of employee behavior or condition (including physical/health condition) is conducted[32]. Therefore, the employer must assess the need for a data protection impact assessment in accordance with the procedure outlined in the aforementioned order, and, should the specified conditions be met, the employer will be obliged to develop an impact assessment document.

6.3. Obligations Regarding Data Security

Another key obligation of the data controller/processor is to ensure data security. As a fundamental principle, data security requires that the controller/processor implement appropriate technical and organizational measures to protect the data against unauthorized or unlawful processing, accidental loss, destruction, and/or damage[33]. This principle forms the basis for the requirement in Article 10(5) of the Personal Data Protection Law, which mandates that the video monitoring system and video recordings be safeguarded against unauthorized access and use. The controller is obligated to ensure that each instance of access to the video recordings is recorded (referred to as "logging"), including the time of access and the username, thus enabling the identification of the person accessing the data.

The importance of the obligation to establish security measures was highlighted by the French data protection supervisory authority in one of its decisions, where it was emphasized that the employee video surveillance system should be secured with a sufficiently strong password, and access should be restricted to a limited number of individuals[34]. The controller/processor is required to regularly check the functionality of the

[32] Order No. 21 of the President of the Personal Data Protection Service of February 28, 2024, Article 5, subparagraphs "a" and "b".
[33] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 4, Paragraph 1, Subparagraph "f".
[34] CNIL, Employee monitoring: CNIL Fined AMAZON FRANCE LOGISTIQUE €32 Million, <https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million> [10.12.2024].

video surveillance system and take appropriate action in response to instances of unauthorized access to the system.[35]

The Latvian Personal Data Protection Supervisory Authority reviewed a case concerning the video surveillance of employees' workspaces using "CCTV" cameras installed at the workplace. According to the facts of the case, a company employee shared a video recording with the data subject through various communication platforms, despite the company's internal regulations explicitly prohibiting employees from accessing and sharing video recordings. The supervisory authority clarified that the company had implemented technical and organizational measures to ensure data security. Therefore, the company, as the data controller, could not be held liable for the actions of an employee who intentionally violated the data security protocols established by the company.[36]

Article 27 of the Law on Personal Data Protection specifically addresses data security matters. In particular, paragraphs 1 and 2 of this article stipulate that the data controller is obligated to implement appropriate technical and organizational measures to ensure that data is processed in compliance with this Law and to be able to demonstrate such compliance. Furthermore, both the data controller and the processor are required to adopt organizational and technical measures that are appropriate to the potential and inherent risks of data processing, thereby ensuring the protection of data against loss, unlawful processing, including destruction, deletion, alteration, disclosure, or unauthorized use.

The significance of data security protection is further reinforced by the consistent practice established by the Personal Data Protection Service, which holds that, to establish non-compliance with data security requirements, it is not necessary to have an unlawful disclosure of data. It is sufficient if "the data controller fails to consider the risks associated with data processing and creates a risk of unlawful data processing through their actions or inaction."[37].

Finally, in conjunction with other obligations established by law, data security protection is critical in that, without adequate measures, there are risks of unauthorized access, disclosure, public exposure, and dissemination of personal data. Even in the event of such risks, the lack of proper data security creates the grounds for the imposition of administrative liability.

[35] <https://pdps.ge/ka/content/978/5263/ra-unda-vicodeT-videomonitoringis-Sesaxeb> [11.12.2024].
[36] World Practice, Personal Data Protection Service, 2024, September, 4.
[37] Decision No. G-1/340/2024 of the President of the Personal Data Protection Service of November 20, 2024.

7. Conclusion

The data subject's official, professional activities are an inherent and integral part of their private life. "In the course of their professional life, most individuals have a unique opportunity to develop their relationship with the outside world.[38]" Therefore, the protection of personal data, as a crucial aspect of the right to privacy, must be guaranteed in the workplace of an employed person.

This paper examines the legislative regulation of the workplace/process of an employed individual, clarifies the standard of reasonable expectation of privacy, the principle of Ultima Ratio, and outlines the obligations of the employer as the data controller/ processor. In addition to theoretical considerations, the paper evaluates the practices and significant clarifications provided by the Personal Data Protection Authority, supervisory authorities of European countries, and the European Court of Human Rights.

The study revealed that the Law on Personal Data Protection establishes high standards for safeguarding the rights of an employee as a data subject and permits video monitoring of the work process/space only in exceptional circumstances. Furthermore, it was determined that in areas of the workplace where an individual has a reasonable expectation of privacy, video monitoring is prohibited, regardless of the legitimate purpose the employer may have.

The Law on Personal Data Protection specifically protects the personal data of employees, and in this context, which is permissible only under certain conditions, it imposes numerous obligations on the employer as the data controller/processor. Persistent failure to adhere to these obligations, particularly in terms of data security protection, where there is merely a risk of personal data security breaches, constitutes an administrative offense and provides grounds for imposing administrative liability.

[38] Case of Bărbulescu v. Romania, [2017] ECHR App. No. 61496/08, §61.

Bibliography:

1. Organic Law of Georgia "Labor Code of Georgia," No. 4113-RS, 17 December 2010.
2. Law of Georgia "On Personal Data Protection," No. 3144-XIMs-XMP, 14 June 2023.
3. Law of Georgia "On Public Service," No. 4346-Ic, 27 October 2015.
4. Law of Georgia "On Labor Inspection," No. 7178-Ic, 29 September 2020.
5. Law of Georgia "On General Education," No. SSM-1330, 8 April 2005.
6. Order No. 21 of the President of the Personal Data Protection Service of 28 February 2024.
7. Order No. 104/n of the Minister of Education and Science of Georgia of 29 December 2021.
8. Order No. 06/n of the Minister of Education, Science, Culture and Sports of Georgia of 29 January 2019.
9. Order No. 1143 of the Minister of Internal Affairs of Georgia of 29 August 2007, "On the Approval of Video Surveillance Systems and the Rules for Their Installation and Operation in Places of Gambling and Other Profitable Games (Except for Promotional Draws) and on the External Perimeter."
10. 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 Aata, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.
11. Resolution No. 341 of the Government of Georgia of 1 July 2022, "On the Approval of Technical Regulations on Minimum Requirements for Safety and Health Protection in the Workplace."
12. Article 29 Data Protection Working Party, Opinion 2/2017 on Data Processing at Work, 2017, 9.
13. CNIL, Employee Monitoring: Fined AMAZON FRANCE LOGISTIQUE €32 Million, <https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million> [10.12.2024].
14. EDPB, Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, 2020, §36.
15. EDPS, Video-Surveillance Guidelines, Brussels, 17 March 2010, 31-32 <https://www.edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf> [16.12.2024].
16. ICO, Guideline on the Monitoring of Workers by Employers, 20-35 <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-

resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf> [20.12.2024].
17. Recommendations on the Implementation of Video Monitoring and Audio Monitoring, Personal Data Protection Service, 2024, 8.
18. *Takashvili S.,* Personal Data Processing Standard for Video Monitoring of an Employee's Workplace, Law Methods, No. 8, 2024, 129.
19. World Practice, Personal Data Protection Service, October 2023, 7–8.
20. World Practice, Personal Data Protection Service, September 2024, 4.
21. Workplace Monitoring: What Are Your Employees' Rights? <https://gdprinformer.com/gdpr-articles/workplace-monitoring-rights> [15.12.2024].
22. Decision No. G-1/346/2024 of the President of the Personal Data Protection Service of 26 November 2024.
23. Decision No. G-1/342/2024 of the President of the Personal Data Protection Service of 22 November 2024.
24. Decision No. G-1/340/2024 of the President of the Personal Data Protection Service of 20 November 2024.
25. *López Ribalda and others v. Spain*, [2019] ECHR, №1874/13; №8567/13.
26. *Antović and Mirković v. Montenegro*, [2017] ECHR, №70838/13, §44, §55-§60.
27. *Bărbulescu v. Romania*, [2017] ECHR, №61496/08, §61.
28. *Köpke v. Germany*, [2010] ECHR, №420/07.
29. *Von Hannover v. Germany*, [2004] ECHR, №59320/00, §51.
30. *Pretty v. the United Kingdom*, [2002] ECHR, №2346/02, §61.