Tomasz MIROSŁAWSKI*

Between Casuistry and Vagueness – A Comparative Legal Analysis of Employer Surveillance of Employee Tasks under Polish and Czech Legislation

ABSTRACT: *The new phase of economic development has brought many benefits to the countries of Central and Eastern Europe, yet rapid technological advancements also present inherent risks. While modern technologies have made it significantly easier for employers to fulfil their control entitlements and more efficiently protect their property, they concurrently pose threats towards employee privacy and dignity. The employee cannot be objectified and treated as a tool of the employer, and nor can his or her work be treated as a mere market commodity. The employer must respect the employee's dignity and right to privacy, and should not infringe it by excessive surveillance. The relationship – which can also be classified as a conflict between the interests of the employer and the privacy of the employee – underscores the necessity of striking a certain balance between the two. Legal measures regulating workplace surveillance serve this purpose, albeit with variations across different countries. This article aims to analyse models of employee tasks surveillance in two countries in the Central and Eastern European region: the Czech Republic and Poland. Despite the similar paths followed by the labour law systems of both countries, the regulations concerning employee tasks surveillance exhibit significant divergence. The Polish model of workplace surveillance can be described as detailed yet narrow, while the Czech one can be referred to as open guidance, and sometimes even as a puzzle. Therefore, the focal point of the research is to compare the differences between these models. To achieve this, an exhaustive analysis was conducted of the doctrine, jurisprudence and provisions of legal acts regulating the issue of employee surveillance in both countries.*

KEYWORDS: *privacy in the workplace, surveillance of employee tasks, monitoring of employees, labour law, GDPR, right to privacy*

* PhD Candidate at the Ferenc Deák Doctoral School of the Faculty of Law of the University of Miskolc, Intern at the Central European Academy in Budapest, e-mail address: tomasz.miroslawski@centraleuropeanacademy.hu, doi: ://orcid.org/0000-0002-7758-7415.

http://doi.org/10.62733/2024.1.191-216

1.
Introduction

Recent years have brought increased economic development to the countries of Central and Eastern Europe. Convergence between CEE and Western European countries has improved, and their national labour markets have strengthened[1]

This new phase of economic development is associated with rapid technological progress,[2] driven in part by foreign investment. Multinational companies, while investing in the CEE region, are also introducing new technological solutions, most often affecting the areas of management and employee surveillance.[3] These activities also provide inspiration for domestic employers, thus creating new trends in the terms and conditions of employment.

New technologies and their widespread availability enable employers to supervise employees with much greater ease than before. Such forms of employee surveillance as visual monitoring, covert monitoring, monitoring of employees' business email, checking of the visited websites and computer activity during working hours, GPS monitoring, interception of employees' telephone calls and recording of keystrokes allow the employer at relatively low cost to assert its interests. These interests include protecting the employer's property from personal use (or misuse); controlling the correct performance of the tasks entrusted to the employee; preventing crime; ensuring good quality of services and products; preventing the disclosure of company secrets; and securing the employer's reputation.[4] To a certain extent, these motives for employee surveillance are understandable and justified. However, as a result of the pursuit of profit, among many employers there is a visible tendency to objectify employees by exposing them to excessive surveillance measures.[5] This, in turn, may cause the infringement of employees' privacy and can lead to increased stress and distrust towards the employer, the consequence of which can be a reluctance to cooperate[6] and an increased desire to resist.[7] On the other hand, more detailed surveillance of employees is happening not without reason. The increasing digitalisation

1 Polster, 2021, pp. 74-79.
2 Instytut Analiz Rynku Pracy (Institute for Labour Market Analysis), 2020, p. 3 .
3 An example of such an action can be the automated system of worker performance reviews introduced in Amazon's distribution centre in Poznań (POZ1). The system combines the elements of employee evaluation and surveillance, collects vast amounts of personal data throughout the working day and uses algorithms to measure two indicators during process of work: productivity and quality of work. – See more in: Rozmysłowicz and Krzyżaniak, 2023.
4 Dąbrowska, 2019, p. 12.
5 Góral, 2016, p. 56.
6 Chang, Liu, Lin, 2015, p. 96.
7 Ball, 2021, p. 37.

of workplaces has resulted in the fact that the fulfilment of employees' tasks often demands access to computers and the internet. This, in turn, carries the risk that employees will use these technologies in ways that are not work-related, e.g. for online shopping, entertainment, social networking, etc. This phenomenon is known as 'cyberloafing',[8] and is becoming more prevalent in Central and Eastern Europe, as can be seen in the example of a group of employees described by Štefko as the 'Facebook fired'.[9] [10]

In light of the above, there are increasing calls for the need to establish a balance between the interests of the employer and the rights of the employee in the context of workplace surveillance. The balance can be achieved by appropriate legal measures. However, it is extremely difficult to do so because the law cannot keep up with the swift development of technology. This article intends to contribute to the ongoing discussion between labour law scholars and parties to labour relationships in Central and Eastern Europe. Its aim is to analyse and compare Polish and Czech legislation on surveillance in the workplace, with a special focus on the surveillance of employees' tasks.

The system of labour law in both countries has followed a similar path, consisting of three main periods. The first was the period of law characteristic of the communist bloc and the so-called 'socialist labour relations'.[11] The second period was that of systemic transformation and the beginnings of the primacy of neo-liberalism in the economic sphere, which left its mark on the labour law systems of the region at the time.[12] The last period, which continues to this day, commenced in 2004 when Poland and the Czech Republic joined the European Union and began the process of adapting labour law to the standards of the community. However, the harmonisation of the labour law system, the increase in employee protection standards, and the obligation to implement the principles set by GDPR[13] – in the context of employees' data collection and processing and workplace surveillance – have not eliminated all the problems and inconsistencies that are associated with this topic.

8 Ball, 2021, p. 29.
9 Štefko, 2016, p. 11 – Štefko describes the "Facebook fired" group as a group of employees who lost their jobs because of posts or comments on social media.
10 Štefko, 2017, p. 131.
11 Florek, 2015, p. 31.
12 Orenstein, 2013, pp. 378-379.
13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter: GDPR).

2.
Models of Employee Surveillance in Czech and Polish Legislation

On the subject of broadly understood personal data protection, 25 May 2018 is an important date for all EU member states – including Poland and the Czech Republic. On that day, the fundamental legal act regulating data protection within the European Union became regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC" (hereafter: General Data Protection Regulation, or GDPR). The regulation is of a general nature, binding in its entirety and should be directly applicable, although it leaves the member states a certain degree of regulatory discretion in certain areas.[14] An example of such an area is the regulation of personal data protection in employment. Indeed, according to Art. 88 (1) of the GDPR, member states may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context.[15] Moreover, in line with Art. 88 (2) of the GDPR, those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in joint economic activity and monitoring systems at the workplace.[16] The legislative discretion in the context of personal data protection in employment is illustrated by the workplace surveillance models regulated in the Polish and Czech labour codes. These models have some similarities, but are notably different. The Polish model for regulating workplace monitoring can be briefly described as detailed yet narrow.[17] Czech legislators have taken the opposite approach, regulating the model more in the form of open guidance, which is described by some as a puzzle.[18]

14 Barański, 2022, p. 56.
15 Art. 88 (1) of the GDPR.
16 Art. 88 (2) of the GDPR.
17 Otto, 2023, p. 412.
18 Šmejkal, 2019, pp. 58.

2.1. Employee Surveillance under the Czech Legal Framework

The issue of surveillance in the workplace in the Czech Labour Code is addressed in Chapter VIII, Protection of an Employer's Property Interests and Protection of an Employee's Personal Rights. This chapter consists only of Section 316, which is divided into four paragraphs. However, it is the first three paragraphs that are of relevance to this article, as they touch upon the issue of surveillance measures over the tasks performed by the employees. Paragraph 4 expresses the prohibition against employers collecting employee information that does not directly relate to the performance of work and the basic labour relationship.[19]

There is a certain duality between Paragraphs 1-3 of Section 316, as they can be divided into two groups.[20] Paragraph 1 introduces a general right of the employer to check compliance with the prohibition against employees using the employer's means of production and other means necessary for the performance of work for personal use.[21] In this provision, the legislature has not specified the concrete means by which such compliance can be checked. It has only indicated that it should be conducted in an appropriate way. In turn, Paragraphs 2 and 3 regulate the issue of the impermissibility of an employer's encroachment upon an employee's privacy at a workplace without serious cause and establish an information obligation.[22] However, in contrast to the first paragraph, Paragraph 2 points out the means of possible workplace surveillance, which under certain conditions[23] will constitute an admissible infringement of the employee's privacy.[24] These are open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, and checking email or postal consignments addressed to a certain employee.

19 Section 316 (4) LABOUR CODE (full translation) No. 262/2006 Coll., as amended „Zákoník práce".

20 Šmejkal, 2019, p. 58.

21 Section 316 (1) [LABOUR CODE (full translation) No. 262/2006 Coll., as amended „Zákoník práce"] - Without their employer's consent, employees may not use the employer's means of production and other means necessary for performance of work, including computers and telecommunication technology for their personal needs. The employer is authorized to check compliance with the prohibition laid down in the first sentence in an appropriate way.

22 Section 316 (3) [LABOUR CODE (full translation) No. 262/2006 Coll., as amended „Zákoník práce"] - Where there is a serious cause on the employer's side consisting in the nature of his activity which justifies the introduction of surveillance (monitoring) under subsection (2), the employer shall directly inform the employees of the scope and methods of its implementation.

23 According to Section 316 (2) of the Czech Labour Code, this condition is a serious cause consisting of the employer's nature of the activity.

24 Section 316 (2) [LABOUR CODE (full translation) No. 262/2006 Coll., as amended „Zákoník práce"] - Without a serious cause consisting in the employer's nature of activity, the employer may not encroach upon employees' privacy at workplaces and in the employer's common premises by open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee.

Although these paragraphs may, at first glance, appear similar and relate to the same issues, they should not be interpreted as synonymous. This has in fact been confirmed by the Czech Supreme Court. In its judgement of 16 August 2012, as well as in the judgement of 7 August 2014, the Supreme Court indicated that the first paragraph of section 316 of the Czech Labour Code concerns mainly the issue of employer's property, while the second and third paragraphs touch on the protection of employees' privacy.[25] An employer's monitoring – according to Paragraph 1 – does not constitute an infringement of the privacy indicated in Paragraph 2. However, it must be conducted in an adequate manner so as to remain within the limits set by the employee's subordination to the employer, according to which the employer is entitled to check that its employees use the entrusted means of production or services exclusively for the performance of the assigned tasks, manage them correctly, ensure their protection against harm or misuse, and refrain from actions against the employer's rightful interest.[26] Therefore it can be said that, in practice, Paragraph 1 serves primarily as a basis for the employer's surveillance of employee tasks. After all, a correctly performed task should not involve misuse of the employer's property, which has been entrusted to carry out a specific work. However, an important question arises. How should surveillance under Paragraph 1 be carried out in order to comply with the statutory requirement of adequacy? The answer can be found in the judgement of the Supreme Court of 16 August 2012,[27] in a case concerning the possibility of an employer checking the use of a company computer – specifically the extent of internet use by an employee during working time – and the legality of the dismissal resulting from this control. In the case, during his monitoring, the employer detected that - despite the prohibition on employees using company equipment for private purposes - one of the employees spent 102.97 out of 168 working hours (in a single month) visiting non-work-related websites through the company computer. Citing gross negligence within work duties, the employer took the decision to terminate the employment contract immediately. Nevertheless, the legal qualification of the surveillance and the legality of the dismissal became a matter of dispute. According to the employee, the employer's monitoring – which provided him with information on employee misuse of company equipment and improper performance of assigned tasks – was carried out covertly without the employee's knowledge and consent, which constituted a breach of Paragraphs 2 and 3 of Section 316 of the Labour Code (LC). However, the Supreme Court settled the issue by ruling that, in this case, the employer acted in accordance with its right to check granted by Paragraph 1, and there was no impermissible encroachment on the employee's privacy. However,

25 Judgement of the Czech Supreme Court of 16.08.2012 on the case 21 Cdo 1771/2011; Judgement of the Czech Supreme Court of 07.08.2014 on the case 21 Cdo 747/2013.

26 Šmejkal, 2019, p. 60.

27 Judgement of the Czech Supreme Court of 16.08.2012 on the case 21 Cdo 1771/2011.

using the example of this case we can see that within the Czech model of workplace surveillance, there is a general problem with the subsumption of the employer's act of control over the employees' tasks – namely, when should it fall under Paragraph 1, and when Paragraphs 2 and 3? Indeed, this problem was partly pointed out by the Supreme Court itself. Justifying its judgement, the court drew attention to two key factors indicating the need to qualify the employer's action as an exercise of the right set out in Paragraph 1, rather than surveillance under Paragraphs 2-3. First of all, the court stated that the employer's monitoring cannot be exercised by the employer in a completely arbitrary manner, since the employer is entitled to exercise such control only in a 'reasonable manner' and it must be examined whether the inspection was continuous or subsequent, what was the scope and duration, whether it interfered with the employee's right to privacy, and to what extent. The court also ruled that the object of the inspection can only be the determination of whether the employee has breached the absolute prohibition laid down by law. The second key point highlighted by the court was that the employer did not intercept the employee's phone calls or check his emails and text messages (the measures mainly indicated in Paragraphs 2-3) during his inspection, but limited itself to checking whether the employee browsed websites not related to his work (the employer also focused only on their type and not on their detailed content). The view expressed by the court in its 2012 judgement was later confirmed in another judgement in 2014, in a case concerning unauthorised private calls via a company phone.[28]

Following the jurisprudence, the doctrine has defined two conditions, which are a kind of guidepost on how the employer should use the right indicated in Section 316 Paragraph 1, in order not to exceed the statutory framework of adequacy.[29] These conditions are: 1) the restriction of the scope and extent of control, including the exclusion of the possibility to check the exact content of non-work 'activities' undertaken by employees during work[30] (e.g., the precise content of browsed websites – there is no doubt that data which can be collected from them might allow an employer to obtain knowledge about the employee's private life, health, sexual preferences, etc.); 2) refrain from using the employee surveillance measures listed in Section 316 Paragraph 2.[31]

However, there is also a critical approach in the doctrine to this type of interpretation of workplace surveillance in the context of Paragraph 1. Vobořil argues that it is rather difficult to agree that tracking the URLs of websites visited is not an intrusion into privacy, because access to websites is connected with the storing of specific data, which can be used to identify the personal information of users, their preferences,

28 Judgement of the Czech Supreme Court of 07.08.2014 on the case 21 Cdo 747/2013.
29 Šmejkal, 2019, p. 61.
30 See also: Štefko, 2016, p. 15.
31 Šmejkal, 2019, p. 61.

etc. Moreover, it is questionable whether supervising internet activity is a proportional method of checking under Paragraph 1. There are different and more adequate ways to prevent the misuse of the employer's resources, e.g. by blocking websites that are unrelated to work and those that disrupt the performance of assigned tasks. The author also draws attention to another important point with which it is difficult to disagree, namely that – with such broadly defined surveillance criteria under Paragraph 1 – an employer may try to hide, behind the right to protect its property, a real intent to supervise and collect employee data of a private nature.[32]

On the other hand, there is an ongoing discussion on the relation of Paragraphs 1 and 2, especially in the context of the second of the mentioned conditions: non-use of surveillance means listed in Paragraph 2 within the monitoring conducted under Paragraph 1. According to Morávek, Paragraph 1 is exclusively applicable if there is a high probability (or *de facto* certainty) that the employee's privacy cannot be encroached upon, regardless of the method of surveillance. Furthermore, even in a situation in which an employee's privacy has been violated, this provision should apply only if a different method of surveillance is chosen than those enumerated in Paragraph 2.[33]

Considering the above interpretation, it is possible to come to the false but nonetheless dangerous conclusion that, since the list of surveillance measures listed in Paragraph 2 is exhaustive, an employer using other methods can freely intervene in an employee's privacy. This conclusion is erroneous because its adoption would violate the entire logical construction of Section 316 Labour Code, a key element of which is the assumption that – when acting within the framework set out by Paragraph 1 – there can be no infringement of the employee's privacy.[34]

However, despite efforts by both the judiciary and the doctrine to clarify the relationship between Paragraphs 1 and 2, it remains unclear. Paragraph 1 only deceptively resembles safe harbour for a Czech employer.[35] In reality, it rather looks like an open sea full of hidden dangers. This is illustrated particularly by the Supreme Court, which in its judgement of August 2012 indicated that Paragraph 1 constitutes a norm with an abstract hypothesis, thus leaving it to judicial discretion to determine the very hypothesis of the legal norm in each individual case.[36] This, in turn, opens up the possibility of excessive judicial activism, which – with regard to the regulation of employment relations and privacy within the workplace – is particularly undesirable,

32 Vobořil, 2012.
33 Morávek, 2017, p. 6.
34 Šmejkal, 2019, p. 62.
35 Šmejkal, 2019, p. 60.
36 Judgement of the Czech Supreme Court of 16.08.2012 on the case 21 Cdo 1771/2011.

as it results in provisions becoming hard to understand for the ordinary addressee and undermines legal certainty for both employer and employee.[37]

Paragraph 2 also raises interpretation problems. Under this provision, a serious cause – depending on the nature of the employer's activity – may justify proportional encroachment upon employees' privacy at workplaces and in the employer's common premises. Again, as in Paragraph 1, addressees of this norm are confronted with an abstract hypothesis. What is the serious cause, and who is authorised to use the surveillance measures indicated in this provision? Every employer, or only those engaged in a particularly hazardous activity? On this matter, the doctrine takes different views.

Šimečková indicates that Paragraph 2 cannot be interpreted in a way that only employers involved in specific dangerous activities may exercise the power granted to them by the law. She claims that the grounds for implementing surveillance facilities are compliance with occupational health and safety, protection of the life and health of employees, protection of the property that belongs to the employer or employee, and productivity monitoring. These grounds apply to every employer, and that is why every employer may find justification to use the measures listed in Paragraph 2.[38] The opposite approach is taken by the State Labour Inspectorate (SUIP). In one of its publications on the protection of employees' personal rights and the protection of the employer's property interests, the inspectorate pointed out that 'a serious cause' is generally not applicable in the production of ordinary products or the supply of ordinary services.[39] Thus, Paragraph 2 does not apply to all employers, regardless of their field of activity. On the other hand, Šmejkal is critical of the SUIP view – stating that such a straightforward answer does not provide good guidance for the doctrine – and of Šimečkova -denying that Paragraph 2 can apply to every employer. Following the literature on the subject[40] and the position of the Office for Personal Data Protection (UOOU), Šmejkal advocates a 'situational analysis', which in his view allows for a more accurate assessment of an increased or extraordinary need for workplace surveillance.[41] Within this approach, he distinguishes the following situations which may justify a proportionate encroachment upon an employee's privacy: a) significant amounts of cash are processed; b) the workplace operates under specific regulations (e.g. when highly sensitive or classified information is handled[42]); c) there is a heightened risk of accidents, explosions, etc. (e.g. in a nuclear power

37 Morávek, 2017, p. 12.
38 Šimečková, 2017, p. 95.
39 Státní Úřad Inspekce Práce (hereinafter: SUIP), 2019, p. 3.
40 See: Zemanová Šimonová, 2016; Vych, 2015; Jouza, 2022.
41 Šmejkal, 2019, p. 74.
42 Zemanová Šimonová, 2016.

plant)[43]; d) there exists a significant need to safeguard intellectual and industrial property rights, valuable knowledge, personal data of third parties,[44] and ensuring equal treatment and non-discrimination.

There is another, different approach, which addresses Paragraphs 1 and 2 holistically. This approach is recommended by Štefko and can be called the 'practical approach'. Štefko identifies three steps that an employer should take before commencing surveillance in the workplace. The first step is a discussion about the scope, duration and manner of the surveillance mechanism with employee representatives – or employees if there are no representatives – before its introduction. The second step is the information obligation towards employees. The last is expressed in obtaining employees' consent.[45] Štefko also indicates that the requirement for consent is not set by the law, but such a practice may alleviate the legal consequences associated with breaches of employee privacy, as it reduces a reasonable expectation of privacy.[46] However, when analysing this aspect it should be borne in mind that an inherent feature of the employment relationship is the inequality of the parties – which in the context of the employee's consent as a factor limiting reasonable expectation of privacy in the workplace – is of significant importance, as consent cannot be given under coercion. It is the very nature of the employment relationship that makes it difficult to obtain the employee's entirely voluntary consent to relinquish part of his or her privacy, since the employee, as the party economically dependent on the employer, may always feel a kind of pressure from the side of employer.[47] This pressure does not necessarily have to be direct but can often involve a limitation of future employment prospects (such as promotion, etc.).[48] Taking this into account, it is fair to say that the 'practical approach' also does not solve all the problems that arise on the grounds of the Czech model of workplace surveillance.

2.2. Employee Tasks Surveillance under the Polish Legal Framework

The Polish model of workplace surveillance has been shaped in a different manner to the Czech one. In fact, it constitutes a more closed and specified system, defined by three areas of surveillance: video, email, and other forms of monitoring,[49] with the purposes indicated explicitly that each surveillance measure is intended to serve.

43 Vych, 2015.
44 Jouza, 2022.
45 Štefko, 2016, p. 15; Štefko, 2017, p. 129; Štefko, 2023, p. 153.
46 Štefko, 2023, p. 153, footnote 44.
47 Otto, 2016, p. 86.
48 Morris, 2001, pp. 53-54.
49 Otto, 2023, p. 394.

This model appears to be more in line with current standards related to privacy in the workplace, and is more understandable to the parties of the employment relationship, as it clearly addresses some issues that in the Czech model are not directly regulated by the provisions of the Labour Code. This is primarily because the Polish regulation is more recent than the Czech one, as it was only implemented in connection with the delegation and the requirements established by GDPR. Previously, the issue of workplace surveillance and the protection of personal data processed in relation to employment was regulated in a fragmentary and implicit way.[50] Some of the principles were derived from the Constitution,[51] some were interpreted from the Labour Code,[52] and some had their source in the Act of 29 August 1997 on the protection of personal data.[53] It was only on 10 May 2018 with the new personal data protection act that the Labour Code was amended and Articles 22^2 and 22^3 were added,[54] regulating the conditions and scope of admissible workplace surveillance. The need for change and the regulation of a proper model of workplace surveillance within the framework of the Labour Code has been advocated by the doctrine for a long time.[55]

Article 22^2 of the Polish Labour Code states that an employer may introduce special supervision over the premises of the establishment, or the area around the establishment, in the form of technical measures that enable video recording (monitoring). However, this form of surveillance can be introduced only if it is necessary to ensure at least one of the prerequisites listed in the form of *numerus clausus*.[56] These prerequisites are the necessity to ensure the safety of employees or protection of property, or production control or confidentiality of information, the disclosure of which might damage the employer's interests. Given the subject matter of the article, the premise of production control is of particular importance, as it is closely linked to the surveillance of the tasks assigned to the employee. On the basis of this premise, the problem arises whether video monitoring can only be used as a surveillance of the work process – which serves the purpose of its continuity and correctness – or also to measure the productivity and efficiency of work.[57] In accordance with the position taken above and the opinion of the President of the Personal Data Protection Office,

50 Otto, 2023, p. 393.
51 In this context Art. 47 (Principle of protection of private life), Art. 49 (Principle of freedom of communication), Art. 50 (Principle of "domestic mir") and Art. 51 (Prohibition on the obligation to disclose information) of the Constitution of the Republic of Poland of 2nd April 1997 no. 78 item 483, are relevant.
52 Art. 11^1 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (hereinafter: LC).
53 For an overview of the employer's obligations to protect the employee's personal data under the Act of 29th August 1997 no. 133 item 883 on the protection of personal data, see – Drzewiecka, 2013.
54 Art. 111 of the Act of 10th May 2018 item 1781 on personal data protection.
55 See: Kuba, 2014, pp. 561 and 569.
56 Art. 22^2 §1 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
57 Dąbrowska, 2019, p. 16.

as expressed in the guidelines on the use of video monitoring,[58] a narrower scope of monitoring and the inadmissibility of using video monitoring to measure work efficiency or productivity should be advocated.

Moreover, the Polish legislature – in §1[1] and §2 of Article 22[2] of the Polish Labour Code – specifies the sites that should be excluded from the video monitoring. Monitoring shall not cover rooms made available to a company trade union organisation, sanitary rooms, locker rooms, canteens, or smoking rooms.[59] The law provides an exception to this general restriction: listed areas might be monitored if it is necessary to ensure the safety of employees, protection of property, control of production or confidentiality of information, the disclosure of which might damage the employer's interests. There is also a condition that it should not infringe upon the dignity and other personal rights of the employee, especially by techniques making it impossible to recognise individuals present in those areas. Additionally, the monitoring of sanitary rooms shall require the prior consent of a company trade union organisation, and when the employer does not have a company trade union organisation within its structure, the prior consent of the employees' representatives selected in accordance with the procedure adopted by the employer.[60]

Further, according to the principle of the data storage limitation expressed in the GDPR,[61] Article 22[2] §3-5 regulates precisely the retention period of the video-recorded data. As a general rule, this period cannot exceed 3 months from the date of the recording.[62] This means that the employer may set a shorter period. An exception to this rule is when the video recordings constitute evidence in proceedings conducted under law, or the employer has become aware that they may constitute evidence in proceedings. In such a case, the storage period is extended until the proceedings have been terminated.[63] After the end of these retention periods, the recordings containing personal data must be destroyed, unless separate regulations provide otherwise.[64]

An integral part of the procedure for implementing video surveillance is defining its objectives, scope and manner of its use. Article 22[2] §6 states that it shall be established in a collective labour agreement or in the work regulations, and if the employer is not covered by a collective labour agreement or is not obliged to adopt work regulations, in an announcement.[65] This regulation corresponds to the principle of transparency of data processing and is in line with the opinion 2/2017 of the now

58 Personal Data Protection Office, 2018, p. 20.
59 Art. 22[2] §1[1] and §2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
60 Art. 22[2] §2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
61 Art. 5 (1)(e) of the GDPR.
62 Art. 22[2] §3 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
63 Art. 22[2] §4 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
64 Art. 22[2] §5 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
65 Art. 22[2] §6 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.

defunct Article 29 Data Protection Working Party. The Working Party recommended involving a representative group of employees in the creation and evaluation of rules and policies regarding monitoring.[66] The introduction and amendment of both the collective labour agreement and the work regulations require agreement with the trade union organisation active in the establishment.[67] Miłosz and Świątek-Rudoman write that in cases where the areas of application of video monitoring vary according to the criterion of the purpose of its use, the said documents should specify which areas are covered by which objectives – and this is particularly important with regard to monitoring used to ensure production control.[68] In addition, there is an obligation on the employer to inform the employees of the introduction of the monitoring no later than 2 weeks prior to its commencement. The method of the notification should be the one adopted by the employer concerned.[69] In relation to new employees, contrary to employees already in an employment relationship, the information obligation is of an individual character.[70] According to the Labour Code, before permitting a new employer to perform his/her work duties, an employer must provide the employee with the information on objectives, scope and manner of the use of monitoring in writing.[71] The information obligation also includes the need to designate monitored areas in a visible and legible manner. This should be done by appropriate signs or sound announcements, but no later than one day before starting the monitoring.[72] The President of the Personal Data Protection Office, in his guidance on the use of video surveillance at work, indicated that, firstly, persons present in the monitored area must be aware that monitoring activities are taking place in their location. Thus, the signs notifying workers of the installed monitoring should be visible, synthetic, and permanently placed not too far from the monitored areas, and the size of the signs must be proportional to the place where they are located. Additionally, pictograms informing of the coverage of cameras may be used. However, pictograms are not a sufficient means of marking, as the information obligation in Article 13 of the GDPR must be taken into account. Full monitoring information, including all the requirements of Article 13, should be available at the monitored site. However, this does not mean that all this information should be included on one board. In order to comply with this obligation, layered information notes can be used, e.g. in the form of documents available at reception or at the administrator's representative.[73]

66 Article 29 Data Protection Working Party, 2017, p. 23.
67 Art. 241^2, 241^9, and 104^2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
68 Miłosz and Świątek-Rudoman, 2019, p. 36.
69 Art. 22^2 §7 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
70 Dąbrowska, 2019, p. 17.
71 Art. 22^2 §8 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
72 Art. 22^2 §9 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
73 Personal Data Protection Office, 2018, pp. 14, 20.

Following the model of regulation adopted in the case of video surveillance, the Polish legislature decided to explicitly regulate the second form of monitoring in the workplace, namely monitoring of employees' business email (Art. 22^3 of the Labour Code).[74] The employer may conduct control of employees' business mail if it is necessary to ensure an organisation of work that enables the full use of the working time and the proper use of the tools made available to the employee. Both of these prerequisites must be met cumulatively.

There is no doubt that employees' business email control translates directly into the supervision of tasks performed by an employee, especially those that involve the use of email or even generally of electronic equipment with access to business email. This is also confirmed by the Personal Data Protection Office, indicating that the employer on this ground can control the activity of his employees while they are at his disposal at the workplace.[75] However, it is important to consider the adequacy of this surveillance measure in relation to the premises for its admissibility. Kuba points out that the monitoring of business email – introduced to ensure an organisation of work that enables the full use of the working time and the proper use of the work tools made available to the employee – might not comply with the rule of adequacy or data minimisation set by regulation 2016/679 in Article 5 (1)(c).[76] In Kuba's view, it would be more appropriate to use other forms of monitoring, such as control of the use of company computers or websites visited by an employee during work, without the need to monitor the contents of an employee's business electronic mailbox.[77] It is difficult to disagree with this position since, in reality, business email is rarely the only tool for providing work. Thus, its control may be insufficient and, in some cases, even too severe to fulfil the premises of this form of surveillance.

Email monitoring constitutes a specific limitation of the freedom and privacy of communication, which is protected at a constitutional level.[78] This is also expressed by the legislature, indicating that it shall not violate the confidentiality of correspondence and other personal rights of employees.[79] Therefore, there is a serious need to define the exact boundaries of an employer's email control. It should be stated with certainty that the literal wording of the act makes it clear that only business email boxes, and under no circumstances private ones, may be subject to monitoring.[80]

74 Art. 22^3 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
75 Personal Data Protection Office, 2018b, p. 34.
76 Kuba, 2019, p. 31.
77 *Ibid,*
78 Art. 49 of the Constitution of the Republic of Poland of 2nd April 1997, Dz. U. No. 78 Item 483.
79 Art. 22^3 §2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
80 Kuba, 2019, p. 34.

Moreover, the control of private correspondence is completely prohibited.[81] Hence, if a private message is found in a business email box, it cannot be checked.

When it comes to the establishment of the objectives, the scope, the manner of use and the information obligation regarding email monitoring, the legislature has stated that the provisions of Article 22^2 §6-10 shall apply accordingly.[82] Therefore, the considerations and conclusions made above on the grounds of video monitoring will also apply to the control of the employees' business mail.

The last of the provisions that constitute the Polish model of employee surveillance is Article 22^3 §4. This regulation extends the catalogue of admissible forms of surveillance within the workplace because it enables, under certain conditions, the use of other forms of monitoring than those specified in the previous articles. However, for other forms of monitoring, the provisions regarding the monitoring of an employee's business email should apply *mutatis mutandis*.[83] Therefore, the other forms of monitoring can be introduced only when it is necessary to ensure an organisation of work that enables the full use of the working time and the proper use of the work tools made available to the employee. Such forms of control may include geolocalisation, monitoring of IT systems, monitoring of the use of the internet by employees, the use of systems based on algorithms to record and check the working time,[84] and many others depending on the target of surveillance and the nature of the activity of the employer.

3.
Similar Paths, Different Outcomes – A Comparison of Both National Models of Employee Tasks Surveillance

A comparison of the two models of employee task surveillance is a challenging task. As can be deduced from the considerations above, Polish and Czech legislatures have taken two different paths when regulating this issue. This is already apparent from the structure of the regulation, which illustrates the approach of the legislatures to the key issues, namely the interest of the employer (i.e. the protection of property) and the interest of the employee (the protection of privacy).

Czech legislation separates issues of the protection of employer's property and the protection of employees' privacy. The protection of the employer's property is addressed in Paragraph 1 of Section 316 of the Czech Labour Code, which introduces a general right of the employer to check compliance with the prohibition on

81 Personal Data Protection Office, 2018, p. 35.
82 Art. 22^3 §3 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
83 Art. 22^3 §4 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
84 Otto, 2023, pp. 409-410; Dąbrowska, 2019, p. 19.

employees using the employer's means of production for personal use. According to the jurisprudential line of the Czech Supreme Court, this provision does not touch upon the question of the employees' privacy and cannot be considered as an infringement of the privacy indicated in Section 316 Paragraph 2.[85] In turn, the notion of the employees' privacy is established in Paragraph 2 by indicating that without a serious cause consisting in the employer's nature of activity, the employer may not encroach upon employees' privacy at workplaces by specific means of surveillance enumerated in this provision. Unlike the Czech one, the Polish legislature did not treat the issues of protection of the employer's property and employees' privacy as separate. While individually regulating video monitoring, business email monitoring and the possibility of using other forms of monitoring, the Polish legislature has restricted them with specific conditions under which such forms of surveillance may be used. The conditions concern in their essence, among other things, the protection of the employer's property. Moreover, the Polish legislature has regulated the issue of the usage of each type of monitoring in detail so as not to allow excessive infringement of employees' privacy. In comparison, the Czech Labour Code does not stipulate any further details on how or when the potential surveillance should be conducted. It only uses vague terms such as that the employer's monitoring should be done in an appropriate way (Paragraph 1 of Section 316), or that the employer may encroach upon the employee's privacy by monitoring or other mentioned forms of surveillance when there is a serious cause consisting in the employer's nature of the activity (Paragraph 2 of Section 316).

Moreover, further differences will emerge when we look at the specific elements of the models applied by legislatures, such as the territorial scope of monitoring, retention period, information obligation, covert surveillance and the question of private usage of employer's equipment.

While commencing with the territorial scope of monitoring, it should be pointed out that not every location within the workplace can be monitored. Premises where the surveillance could lead to the collection of sensitive data, or data not related to the purpose of the monitoring as set out in laws, should not be subjected to monitoring. Such monitoring could constitute a violation of the employee's dignity and the principles set out by the GDPR.[86] The Polish Labour Code seems to adhere to this principle. It defines the sites that should be excluded from the video monitoring and regulates the possibility of derogating from the general prohibition.[87] On the other hand, the Czech legislature did not indicate *explicite* in Section 316 of the Labour Code which areas of a workplace should be excluded from monitoring, or where it should be

85 Judgement of the Czech Supreme Court of 16.08.2012 on the case 21 Cdo 1771/2011; Judgement of the Czech Supreme Court of 07.08.2014 on the case 21 Cdo 747/2013.

86 See the principle of data minimisation - Art. 5 (1)(c) of the GDPR.

87 Art. 22^2 §1^1 and §2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.

limited, which creates rather a problematic situation. However, the task of clarifying the 'territorial scope' of video monitoring has been undertaken by doctrine[88] and jurisprudence. The Czech Supreme Administrative Court, in the judgement of 23 August 2013, noted that the monitoring should be directed at the employer's property, not at the employee's person, and should be carried out in the workplace, not in areas designated for hygiene or resting.[89]

Another difference between Poland and the Czech Republic that arises on the grounds of video monitoring is the issue of the principle of data storage limitation.[90] To comply with this principle, the Polish legislature has comprehensively regulated the data retention period, indicating how long it may last, in which situation it may be extended, and what should happen to the data after the expiry of the period.[91] The Czech Labour Code does not introduce any similar regulation on the data retention period. In this case, once again, the answer should be sought within the doctrine. Skubal writes that the generally accepted period for the storage of records resulting from video monitoring (CCTV surveillance) shall not exceed 7 days. However, the period can be longer if it is properly justified by the employer. Moreover, he notes that when a data controller has solid arguments for a longer period of retention, the Office for Personal Data Protection (UOOU) often accepts it.[92] On the surface, it may seem that a time limit of 7 days more appropriately corresponds to the principle of data storage limitation. However, it should be considered that this time limit is not directly set in law and is dependent on the approval of the public authority responsible for personal data protection. This creates a situation of uncertainty for the parties to the employment relationship. Furthermore, the Czech legislation does not specify what should happen to the data after the retention period, whether it should be destroyed or archived.

The situation partially changes with regard to the information obligation. Although the Polish legislature continues to proceed along the path of the extended and detailed regulation[93] discussed earlier, the change is evident on the Czech side. The Czech model of workplace surveillance, just like the Polish one, directly addresses an information obligation. However, it is formulated in a much briefer manner than under the Polish Labour Code. Namely, its regulation is limited to a single provision. Section 316 Paragraph 3 of the Czech Labour Code stipulates that in the case of the

88 Šmejkal, 2019, p. 72.
89 Judgement of the Czech Supreme Administrative Court of 23.08.2013 on the case 5 As 158/2012-49 – "Monitoring musí být směřován na majetek zaměstnavatele, nikoliv na osobu zaměstnance (nasměrování kamer) a musí být prováděn na pracovišti, nikoliv na místech určených k hygieně nebo k odpočinku zaměstnance".
90 Art. 5 (1)(e) of the GDPR.
91 Art. 22^2 §3-5 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
92 Skubal, 2023, p. 17.
93 Art. 22^2 §6-10 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.

introduction of the surveillance measures referred to in Paragraph 2, the employer is obliged to directly inform the employees of the scope and methods of their implementation.[94] Therefore, this obligation can be fulfilled in any appropriate form that enables the individual and direct transfer of information to each employee.[95] Thus, this may be done through an adopted and duly promulgated internal regulation or through a channel with which the employer customarily communicates with the employee – written communication, oral communication, email, etc.[96] The specific discretion of the form of information on monitoring is also expressed in the Polish Labour Code with the expression that "an employer shall notify employees of the introduction of monitoring, in the manner adopted by the given employer."[97] The information should, in particular, allow the employee to familiarise him/herself with the scope of the surveillance, i.e. it should specify the duties entrusted to the employee that are to be monitored; the period during which the surveillance will take place; the premises under monitoring; and the means by which the surveillance is to be carried out.[98]

On the grounds of the information obligation, one more point of divergence arises between the Polish and Czech models of employee surveillance. Namely, it concerns the possibility of covert surveillance. Under Polish law, both doctrine[99] and jurisprudence[100] unequivocally state that such surveillance cannot be conducted, irrespective of the type (video monitoring, email monitoring and other forms of employee surveillance). The situation is the opposite with regard to the Czech model, as the Czech Labour Code explicitly expresses the possibility of concealed monitoring by an employer.[101] This poses the question of how to comply with the requirements imposed by the regulation on information obligation. As a rule, in such a situation the information obligation is limited in a certain way, which does not change the fact that the employer should fulfil it to the maximum extent, but in the *ex-post* manner only after the surveillance was conducted.[102] Moreover, the employer should give advance notice of the possibility of control.[103] However, this solution seems rather fictitious because as Šmejkal rightly points out, in any future conflict between an employer and

94 Section 316 (3) LABOUR CODE (full translation) No. 262/2006 Coll., as amended „Zákoník práce".
95 Sehnálek, 2023, p. 259.
96 Morávek, 2017, p. 10.
97 Art. 22^2 §7 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
98 Morávek, 2020, pp. 26-27.
99 Barański, 2018, p. 48; Personal Data Protection Office, 2018, pp. 25-26.
100 Judgement of the Supreme Administrative Court of 13.02.2014 on the case I OSK 2436/12.
101 Section 316 (2) LABOUR CODE (full translation) No. 262/2006 Coll., as amended „Zákoník práce".
102 Sehnálek, 2023, p. 260.
103 Morávek, 2020, pp. 26.

an employee, the employee will find out that the employer collected evidence of his/her misconduct as a result of workplace surveillance.[104]

Another interesting question that arises is connected to the surveillance of business email inboxes, and touches on issues of the possibility of private usage of employer's equipment by employees and privacy of correspondence. In both countries, such a form of surveillance is permitted and, as indicated earlier, in both countries it is prohibited to check private messages even within a company's email inbox, as it would constitute an infringement of the privacy of correspondence, which is safeguarded by both Polish and Czech constitutional orders.[105] The mere fact that a message is sent or received via a business email does not determine that such a message does not contain private content, nor does the proper designation of the subject and the parties suggest the business character of the conversation.[106] Therefore, employers need to be particularly careful when conducting this form of monitoring, which may prove to be more of a challenge in Poland than in the Czech Republic. This is mainly because of the issue of the use of the company's equipment for private purposes, which obviously has an impact on the process of possible surveillance and its correctness. This issue under Polish labour law is less clear-cut than under Czech law. Czech regulation indicates unequivocally that without the employer's consent, employees may not use the company's equipment for private purposes.[107] However, the situation is reversed in the case of the Polish model of regulation. It follows that in principle, unless such use is prohibited, it is permitted. This state of affairs can cause many problems, infringements and uncertainty on both sides of the employment relationship. Hence, it is reasonably advocated in the doctrine that employers should prohibit the use of business email for private purposes.[108] Such a solution should make it possible to significantly facilitate the control criteria.

Despite the above differences, which are in the overwhelming majority, there is one provision that brings a rather closed and specified Polish model of workplace surveillance closer to the more open and vague Czech one. Namely, Article 22^3 §4 of the Polish Labour Code, which under certain conditions widens the closed catalogue of forms of monitoring to other forms. It resembles to a certain extent Section 316 Paragraph 1 of the Czech Labour Code, which by its vague wording that the employer's monitoring should be carried out in an appropriate way, also opens up a catalogue of forms of surveillance. The discussed provision of the Polish Labour Code is rather

104 See more in: Šmejkal, 2019, p. 76.

105 Art. 49 of the Constitution of the Republic of Poland of 2nd April 1997 no. 78 item 483, Art. 13 of the Charter of Fundamental Rights and Freedoms of the Czech Republic of 16 December 1992 (Const. act No. 2/1993 Coll. as amended by constitutional act No. 162/1998 Coll.).

106 Kuba, 2019, p. 34.

107 Section 316 (1) LABOUR CODE (full translation) No. 262/2006 Coll., as amended „Zákoník práce".

108 Dąbrowska, 2019, p. 18; Kuba, 2019, p. 34.

controversial. On the one hand, it might bring a certain level of risk, especially towards the privacy of employees; but on the other hand, it is a practically useful mechanism to keep up in terms of employee surveillance to rapidly changing and evolving concepts of the workplace.

4.
Conclusion

The issue of surveillance of tasks assigned to the employees is linked to two important aspects. The first is the work itself performed by the employees. Under the Polish and Czech Labour Codes, this work is framed by specific obligations/duties setting out how the work should be performed. Czech employees should work properly in accordance with their strength, knowledge and capabilities, fulfil instructions given by their superiors in compliance with the statutory provisions, and cooperate with other employees.[109] Very similarly, Polish employees shall perform work conscientiously and with due diligence, and shall comply with the work-related instructions of their superiors, unless they are contrary to the provisions of law or the contract of employment.[110] However, for the work to be performed in this manner, it firstly needs to be concretised (in the form of specific tasks); secondly, it needs an adequate system to check its process and outcomes. The realisation of these needs is made possible by the second-mentioned aspect – the organisational function of labour law. This function enables the employer to assign specific tasks to a specific employee, and is a source of the employer's control entitlements.[111]

It is only by bringing these two aspects together that a fair model for the surveillance of employees' tasks can be shaped, which recognises both the employee's right to privacy, dignity and respect for their work, and the need of the employer to organise work and the related need for surveillance. Tannenbaum expressed this relationship in the following words: "organisation implies control."[112] In our case, the organisation is the workplace.

The Polish and Czech legislatures have both considered these aspects when shaping their national models of employee tasks surveillance. However, they have taken different measures to implement them. The discrepancy between the two models is mostly due to the fact that the Polish regulation is more recent than the Czech one, as it was only implemented in connection with the delegation and the

109 Section 301 (a), LABOUR CODE (full translation) No. 262/2006 Coll., as amended „Zákoník práce".
110 Art. 101 § 1 of Act of 26 June 1974. Labour Code (Dz. U. z 2023 r. poz. 1465).
111 Kuba, 2022, section 2.2.
112 Tannenbaum, 1962, p. 237.

requirements established by GDPR. The Czech model already existed in its current shape beforehand.

This has also resulted in the fact that the Polish model appears to be more in line with current standards related to privacy in the workplace, and is more understandable to the parties of the employment relationship. It clearly addresses issues that, in the Czech model, are not directly regulated by the provisions of the Labour Code. However, its detailed and partly casuistic nature may lead to its obsolescence in a situation of rapid technological development. In this context, the openness of the Czech model can be perceived as a positive feature; on the other hand, its over-vagueness results in many interpretation problems, lack of certainty, and may lead to excessive activism of judges, which is rather an undesirable situation, especially in a case of labour law regulations.

Based on conducted research, two general conclusions can be drawn. The first is that, despite a similar path followed by the labour law systems in the countries of Central and Eastern Europe, their individual parts may differ significantly - as can be seen in the Czech Republic and Poland with regard to their models of employee surveillance. The second conclusion is that there is an urgent need to find a balance between the two approaches to workplace surveillance, and to propose a more comprehensive and equitable model which will have to face so far unknown challenges caused by new surveillance techniques.

Bibliography

- Article 29 Data Protection Working Party (2017), *Opinion 2/2017 on data processing at work*. Brussels [Online]. Available at: https://ec.europa.eu/newsroom/article29/items/610169 (Accessed 4 April.2024).
- Ball, K. (2021) *Electronic Monitoring and Surveillance in the Workplace, Publications Office of the European Union*. Luxembourg: Publications Office of the European Union; doi:10.2760/5137.
- Barański, M. (2022) 'Ochrona danych osobowych pracowników w orzecznictwie Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości' [Protection of Employees' Personal Data in Judgments of the Polish Constitutional Tribunal and the Court of Justice of the EU], *Państwo i Prawo*, 1/2022, pp. 46-65.
- Barański, M. (2018) 'Labor impact of technological devices in Poland' in Galvez Durán, S., Camargo Rodríguez, A. (eds.) COMPARATIVE LABOR LAW DOSSIER LABOR IMPACT OF TECHNOLOGICAL DEVICES, *IUSLabor,* 2/2018, pp. 44-52 [Online]. Available at: https://doi.org/10.31009/IUSLabor.2018.i02.02 (Accessed 6 April 2024).
- Chang, S.E., Liu, A.Y. and Lin, S. (2015) 'Exploring privacy and trust for employee monitoring', *Industrial Management & Data Systems*, Vol. 115, No. 1, pp. 88-106 [Online]. Available at: https://doi.org/10.1108/IMDS-07-2014-0197 (Accessed 22 March 2024).
- Dąbrowska, O. (2019) 'Criteria of admissibility to use video surveillance in a workplace and duties of an employer in the light of reform on personal data protection', *Prawo Mediów Elektronicznych*, 1/2019, pp. 12-19 [Online]. Available at: https://repozytorium.uni.wroc.pl/dlibra/publication/edition/122485?id=122485 (Accessed: 22 March 2024).
- Florek, L. (2015) 'The Evolution of the Labour Code', *Studia Iuridica Lublinensia*, Vol. 24, No. 3, pp. 29-43 [Online]. Available at: http://dx.doi.org/10.17951/sil.2015.24.3.29 (Accessed 22 March 2024).
- Góral, Z. (2016) 'Principles of labour law' in Baran, K.W. (ed.) *Outline of Polish Labour Law System*. Warsaw: Wolters Kluwer, pp.45-73.
- Instytut Analiz Rynku Pracy (Institute for Labour Market Analysis) (2020), *Czwarta rewolucja przemysłowa i jej wpływ na rynek pracy (The fourth industrial revolution and its impact on the labour market)*, Warsaw.
- Kuba, M. (2014), Monitoring w miejscu pracy – refleksje na tle aktualnego stanu prawnego (Monitoring in the workplace - reflections on the current legal status). *Krytyka Prawa. Niezależne Studia Nad Prawem*, 6(1), 559-570 [Online]. Available at: https://doi.org/10.7206/kp.2080-1084.68 (Accessed 4 April 2024).

- Kuba, M. (2019) 'Employee Email Monitoring - Reflections on the New Regulations', *Praca i Zabezpieczenie Społeczne,* 11/2019 [Online] Available at: DOI 10.33226/0032-6186.2019.11.4 (Accessed 4 April 2024).
- Kuba, M. (2022) 'Art. 22(2) Monitoring w zakładzie pracy (Art. 22(2) Monitoring in the workplace)' in Baran, K.W. (ed) *Kodeks pracy. Komentarz.* T. I, Art. 1-93, 6th edn., Warsaw: Wolters Kluwer, Art. 22(2) [Online]. Available at: https://sip.lex.pl/#/commentary/587769454/697659?tocHit=1&cm=URELATIONS (Accessed 6 April 2024).
- Miłosz, M., Świątek-Rudoman, J. (2019) 'New Legal Framework for Usage of Video Surveillance by an Employer at the Work Place', *Praca i Zabezpieczenie Społeczne,* 4/2019 [Online]. Available at: DOI 10.33226/0032-6186.2019.4.4 (Accessed 4 April 2024).
- Morávek, J. (2017) 'Kontrola a sledování zaměstnanců - výklad § 316 ZPr (Control and monitoring of employees - interpretation of § 316 LC)', *Právní rozhledy,* Vol. 25, No. 17, pp. 573-581 [Online]. Available at: https://www.spolpracsoc.cz/files/2018/04/Morávek-Kontrola-a-sledování-zaměstnanců-–-výklad-§-316-ZPr-.pdf (Accessed 26 March 2024).
- Morávek, J. (2020) 'Kamerové systémy z hlediska inspekce práce a Úřadu pro ochranu osobních údajů (Camera systems from the perspective of the Labour Inspectorate and the Office for Personal Data Protection)' in Morávek, J. (ed.) *Důkazní Prostředky A Jejich Přípustnost Zejména Se Zaměřením Na Kamerové Sledování.* Prague: Eva Rozkotová Publishing, pp. 6-43 [Online]. Available at: https://dspace.cuni.cz/bitstream/handle/20.500.11956/117235/DŮKAZNÍ%20PROSTŘEDKY_Morávek_ekniha.pdf?sequence=1&isAllowed=y (Accessed 6 April 2024).
- Morris, G.S. (2001) 'Fundamental Rights: Exclusion by Agreement', *Industrial Law Journal*, 30(1), 49-71.
- Orenstein, M.A. (2013) 'Reassessing the neo-liberal development model in Central and Eastern Europe' in Schmidt, V.A., Thatcher, M. (eds.) *Resilient Liberalism in Europe's Political Economy.* Cambridge: Cambridge University Press, pp. 374-400.
- Otto, M. (2016) *The Right to Privacy in Employment: A Comparative Analysis.* Oxford, Portland, Oregon: Hart Publishing.
- Otto, M. (2023) 'Privacy at Work in Poland' in Hendrickx, F., Mangan, D., and Gramano, E. (eds.) *Privacy@Work: A European and Comparative Perspective.* Wolters Kluwer, pp. 393-412.
- Personal Data Protection Office (2018) W*skazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego (Guidelines of the President of the Personal Data Protection Office on the use of video monitoring).* Warsaw: Personal Data Protection Office [Online]. Available at: https://uodo.gov.pl/data/filemanager_pl/1200.pdf (Accessed 4 April 2024).
- Personal Data Protection Office (2018b), *Ochorna danych osobowych w miejscu pracy. Poradnik dla pracodawców (Data protection in the workplace. A guide for employers).*

Warsaw: Personal Data Protection Office [Online]. Available at: https://orka.sejm.gov.pl/BOP_info.nsf/0/43826AB057FD3661C125832E00368D2F/%24File/Poradnik%20dotyczÄ…cy%20zatrudnienia.pdf (Accessed 4 April 2024).

- Polster, C. (2021) 'Economic Development and Growth in Central and Eastern Europe', *Comparative Economic Research. Central and Eastern Europe*, Vol. 24, Iss. 4, pp.69-84 [Online]. Available at: https://doi.org/10.18778/1508-2008.24.31 (Accessed: 22 March 2024).
- Rozmysłowicz, M., Krzyżaniak, P. (2023) 'Automated Processing of Data on Work Performance and Employee Evaluation: A Case Study of Practices at Amazon Warehouses in Poland', *Italian Labour Law e-Journal*, Vol. 16, Iss. 2, pp. 149-164 [Online]. Available at: https://doi.org/10.6092/issn.1561-8048/18084 (Accessed 22 March 2024).
- Sehnálek, D. (2023) 'The Right to Privacy in the Digital Age in the Czech Republic' in Wielec, M. (ed.) *The Right to Privacy in the Digital Age: Perspectives on Analysis of Certain Central European Countries' Legislation and Practice*. Miskolc-Budapest: CEA Publishing, pp. 235-272.
- Šimečková, E. (2021) 'Legislation on Employer Monitoring of Employees at the Workplace in the Czech Republic', *Studia Prawno-Ekonomiczne*, Vol. *105*, pp. 91–105 [Online]. Available at: https://doi.org/10.26485/SPE/2017/105/6 (Accessed 27 March 2024).
- Šmejkal, V. (2019) 'High Tech Monitoring Versus Privacy in the Workplace in the Law and Case Law of the Czech Republic', *Białostockie Studia Prawnicze,* Vol. 24, No. 2, pp.53-89 [Online]. Available at: https://bsp.uwb.edu.pl/en/bialystok-legal-studies-vol-24-nr-2/, DOI: 10.15290/bsp.2019.24.02.03 (Accessed 26 March 2024).
- Štefko, M. (2016) 'Social Media in the Workplace in the Czech Republic, Poland and Slovakia', *The Lawyer Quarterly*, Vol. 6, No. 1, pp. 11-17. Available at: https://tlq.ilaw.cas.cz/index.php/tlq/article/view/177 (Accessed 26 March 2024).
- Štefko, M. (2017) 'Social media in the workplace (Bărbulescu vs Romania, ECHR 61496/08)' in Łaga, M., Bellomo, S., Gundt, N., María, J., Boto, J.M.M. (eds.) *Labour law and social rights in Europe: the jurisprudence of international courts, selected* judgements. Gdańsk: Gdańsk University Press, pp. 122-131.
- Štefko, M. (2023) 'Privacy at Work in the Czech Republic' in Hendrickx, F., Mangan, D., and Gramano, E. (eds.) *Privacy@Work: A European and Comparative Perspective*. Wolters Kluwer, pp. 137-156.
- Tannenbaum, A.S. (1962) 'Control in Organizations: Individual Adjustment and Organizational Performance', *Administrative Science Quarterly*, 7(2), pp. 236-257. Available at: http://hdl.handle.net/2027.42/86669 (Accessed 9 April 2024).

Legal sources

- Act of 10th May 2018 item 1781 on Personal Data Protection of the Republic of Poland.
- Act of 26 June 1974 Dz.U.2023.1465 Labour Code ("Kodeks Pracy") of the Republic of Poland.
- Charter of Fundamental Rights and Freedoms of the Czech Republic of 16 December 1992 (Const. act No. 2/1993 Coll. as amended by constitutional act No. 162/1998 Coll.).
- Constitution of the Republic of Poland of 2nd April 1997 no. 78 item 483.
- Labour Code of the Czech Republic of 21 April 2006 (full translation) No. 262/2006 Coll., as amended „Zákoník práce".
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Jurisprudence

- Judgement of the Czech Supreme Administrative Court of 23.08.2013 on the case 5 As 158/2012-49.
- Judgement of the Czech Supreme Court of 07.08.2014 on the case 21 Cdo 747/2013.
- Judgement of the Czech Supreme Court of 16.08.2012 on the case 21 Cdo 1771/2011.
- Judgement of the Polish Supreme Administrative Court of 13.02.2014 on the case I OSK 2436/12.

Internet sources

- Drzewicka, E. (2013) *Obowiązki pracodawcy w zakresei ochorny danych osobowych pracownika (Employer's obligations regarding the protection of employee's personal data)* [Online]. Available at: https://www.prawo.pl/biznes/obowiazki-pracodawcy-w-zakresie-ochrony-danych-osobowych,194562.html (Accessed 4 April 2024).
- Jouza, L. (2022) *Ochrana osobnosti zaměstnance v pracovněprávních vztazích (Protection of the employee's personality in employment relations)* [Online]. Available at: https://advokatnidenik.cz/2022/05/21/ochrana-osobnosti-zamestnance-v-pracovnepravnich-vztazich/ (Accessed 27 March 2024).
- Skubal, J. (2023) *Czechia - Employee Monitoring* [Online]. Available at: https://www.dataguidance.com/notes/czechia-employee-monitoring (Accessed 5 April 2024).
- Státní Úřad Inspekce Práce (2019) *Ochrana Osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele (Protection of employees' personal rights and*

protection of the employer's property interests) [Online]. Available at: https://www.suip.cz/documents/20142/43720/ochrana_os_2019.pdf/6e6c9012-7616-40f3-1fef-b443c682e94a (Accessed 27 March 2024).

- Vobořil, J. (2012) *Nejvyšší Soud k možnostem utajeného sledování zaměstnanců (Supreme Court on the possibility of covert surveillance of employees)* [Online]. Available at: https://zpravodaj.genderstudies.cz/cz/clanek/nejvyssi-soud-k-moznostem-utajeneho-sledovani-zamestnancu (Accessed 27 March 2024).
- Vych, J. (2015) *Navrhovaná změna v oblasti ochrany soukromí zaměstnanců (Proposed change in the area of employee privacy)* [Online]. Available at: https://www.epravo.cz/top/clanky/navrhovana-zmena-v-oblasti-ochrany-soukromi-zamestnancu-98803.html (Accessed 27 March 2024).
- Zemanová Šimonová, H. (2016) *Právní Prostředky Ochrany Osobnosti Zaměstnance (Legal Means Of Protecting The Personality Of The Employee)* [Online]. Available at: http://www.bulletin-advokacie.cz/pravni-prostredky-ochrany-osobnosti-zamestnance (Accessed 27 March 2024).