Kateřina ŠTĚPÁNKOVÁ*

Workplace Surveillance of Employees from the Czech Perspective

ABSTRACT: *This contribution focuses on workplace surveillance from the Czech perspective. Its basis is to present the essence of surveillance by employers in the Czech Republic – a much-discussed topic influenced by a number of facts such as the development of modern technologies, also included in this paper. These issues are presented from several perspectives – specifically: employees under video surveillance; monitoring of employees' computers; and consumption of alcohol or other addictive substances under surveillance. In the case of video monitoring, the aspect of GDPR legislation and the Labour Code are discussed in detail. The national attitude towards hidden monitoring and dummy camera systems is also emphasised. For example, it is important that - according to some opinions - the employer is obliged to directly inform the employees about the scope and methods of the employee surveillance in advance. This would completely eliminate employee surveillance carried out with hidden cameras. However, this approach would basically be much harder on employers than the European Court of Human Rights' case-law. This paper, therefore, represents a different way of interpreting the relevant Czech Labour Code. The role of the Czech Personal Data Protection Office is also highlighted. The development of the opinion of this Office on employee email surveillance is also included. In relation to the topic of employee surveillance through a work computer, the paper also summarises the basic limits that the employer must take into account. Finally, monitoring work premises for the presence of alcohol is a highly important topic as well, with employees forbidden from working under the influence of alcohol. However, the employee surveillance faces some major restrictions in this respect, not only from Czech Labour Code legislation but also by the case-law of the Supreme Court of the Czech Republic.*

KEYWORDS: *labour law; employee surveillance; employer; workplace; Czech Republic*

* Associate professor at the Department of Labour Law and Social Security Law, at the Law faculty of the Charles University in Prague, a national correspondent for the Max Planck Institute for Social Law and Social Policy, in Germany, and also an attorney at law in Prague with Kocián Šolc Balaštík, advokátní kancelář, s.r.o.

http://doi.org/10.62733/2024.1.319-336

1.
Introductory notes

Surveillance of employees is certainly a much-discussed topic. Many employers are now thinking about how to approach the surveillance of their employees, or are introducing it to their workplaces as a new measure. This can be induced by many causes, the most common of which will likely be the effort to control efficiency and performance, while also including health and safety monitoring, natural monitoring of the working environment, or any other relevant cause. At the same time, employee surveillance is not only related to moments when the employee is performing distance work, such as on home office. Currently, these surveillance methods can be frequently encountered even during routine work in the employer's workplace and on its premises.

It is also necessary to emphasise that there are many new information technologies appearing – often directly associated with much easier and more intensive surveillance. And the more thorough these new surveillance possibilities are, the more essential it is to pay attention to the protection of employees, who can be excessively affected by such surveillance.

This is, at the same time, a very broad topic that can be viewed from different angles. This paper, therefore, includes employee surveillance from several different points of view. In this respect, employees under video surveillance and computer monitoring – and monitored for consumption of alcohol or other addictive substances – are discussed.

2.
Employees Under Video Surveillance

2.1. The GDPR legislation

Video surveillance is probably the most frequent method of employee surveillance in the Czech Republic, and the associated employee protection has two levels. By all means, recording of employees may be considered as processing of their personal data under the General Data Protection Regulation (hereafter GDPR).[1] This is especially the

1 Cf. 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.

case if the recording from the cameras can be kept for a longer period – in which case the employer will fulfil the requirements of Article 4 Points 2, 7 and 8 of the GDPR,[2] and will act as the controller and processor of the personal data of its employees.

In addition, the internal Act No. 110/2019 Coll., on the processing of personal data, as amended (hereafter the Act on Personal Data Processing), which closely follows this GDPR Regulation, was adopted in the Czech Republic. Therefore, the relevant legislation is included in both of these legal sources. On an application level, these jointly represent the general legislation in relation to camera systems and employee surveillance, which is to stipulate the basic[3] obligations placed on the employer — for example, the obligation to specify the purpose of processing personal data, records of processing activities, balance test, instruction of the data subject on the scope of their processing, on the proportionality test, or on the securing of protection of the personal data processed. The relevant supervisory body is then the Czech Personal Data Protection Office (as well as the European legal framework for personal data protection).

Although there are not many court decisions at this general level, a judgment by the Supreme Administrative Court of the Czech Republic can be referred to at this point. Specifically, it stipulates that the aim of the national legislation contained in the Act on Personal Data Processing (as well as in the previous legislation) is to fulfil the right of everyone, including the employees, to be protected against unauthorised interference with their privacy - and to get the rights and obligations regarding personal data processing in compliance with the European legislation.[4]

2 Article 4 Point 2 of the GDPR Regulation stipulates that processing means any operation or set of operations, '*such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*'

3 Cf. Štefko, 2019, pp. 1246–1254.

4 Cf. Supreme Administrative Court, 2006, 3 As 21/2005-105.

2.2. The Role of the Czech Personal Data Protection Office and the Methodology

2.2.1. Division of Camera Systems into 4 Classes

In response to the European Data Protection Board Guidelines 3/2019,[5] the Personal Data Protection Office has prepared its national methodology.[6] This methodology is not a binding legal act, but a draft document to help with the GDPR application on video surveillance. In principle, it can be said that the office attempts to make the processing much easier for those processing personal data in a lower quality and smaller extent. Therefore, the office divides camera systems into 4 classes. The criteria of this division are - among other things - the quality of the recording, its sensitivity, or the degree of interference with the rights of the data subject (i.e. the employee).

The methodology also defines four types of threats to which the employer must react if using the camera systems for employee surveillance:

a) Unauthorised access to camera systems
b) Access by unauthorised persons to camera recordings
c) Unauthorised reading (even online), copying, transmission, modification, and erasing of camera recordings
d) Potential weather damage to surveillance cameras

For each of these 4 classes and types of threats, technical and organisational measures used for a specific camera system are subsequently determined by the methodology. These measures must be adopted by the employer to prevent the abuse of camera systems. The lower the recording quality of a specific camera included in the relevant class is, the fewer measures the employer is obliged to implement. In this case these measures are usually less demanding for the employer.

2.2.2. Camera Systems in Online Mode

In its methodology the office newly stipulates that – in order to save camera recordings – the processing of personal data can be carried out in 'online mode' – i.e. with a

5 Cf. European Data Protection Board (2020): Guidelines 3/2019 on processing of personal data through video devices [Online]. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (Accessed: 27 October 2023).

6 Cf. Czech Personal Data Protection Office (2023): Methodology for the design and operation of the camera systems in terms of the processing and protection of personal data [Online]. Available at: https://uoou.gov.cz/media/novinky/dokumenty/metodika-kamery0-983.pdf (Accessed: 27 October 2023).

camera system that does not store the recording. However, these videos can be monitored by the employer or by any other person online. The principle here is that any shot of an identifiable person represents personal data, and therefore enabling access to an unlimited circle of recipients also represents the processing of personal data.

Thus, the office extends the scope of GDPR legislation to all cameras, camera systems, photo traps and all similar devices capturing or transmitting shots of natural persons – whether they make a long-term recording or not.

2.2.3. Sample Documentation

The methodology also contains three sample documents. One is a sample document for fulfilling the information obligation; one is a sample record of the operation of the processing by the camera system; and one is a sample balance test within the processing of personal data on the basis of legitimate interests.[7] This is a step helping – in particular – smaller controllers to comply with the obligations of the GDPR in the using of camera systems.

2.3. Czech Labour Code

In addition to the GDPR legislation, some basic requirements are also stipulated in the Czech Act No. 262/2006 Coll., the Labour Code, as amended (hereafter the Labour Code). The legislation contained in the Labour Code is especially in relation to the general GDPR rules. The relevant supervisory bodies are then the Regional Labour Inspectorates and the State Labour Inspection Office.

In accordance with Section 316 of the Labour Code, without a serious reason the employer must not interfere with the employee's privacy in the workplace and in the joint premises of the employer. This means that the employer is forbidden from monitoring the employee openly or covertly, to intercept or record telephone calls, or to check email or other mail shipments addressed to employees. More importantly, if a reason is provided to justify such control mechanisms, the employer is obliged to directly inform the employees about the scope of the surveillance and the methods of its implementation.

7 *Ibid.*

2.3.1. Hidden Camera Systems

According to some opinions,[8] the provision of the above information should always precede the surveillance itself – and therefore secret employee surveillance was generally prohibited with regard to Section 316 of the Labour Code. However, this would also mean that the legislation of the Czech Labour Code would be much stricter on employers than foreign judicial decisions, such as those of the European Court of Human Rights (ECtHR). Out of these reasons, I cannot in principle identify with the opinion that provision of the information should always precede the surveillance itself.

An example of such ECtHR case-law is the judgment in Lopez Ribalda et al. versus Spain. This judgment dealt with a case in which a supermarket employer installed camera systems to prevent continuing theft at the workplace. Employees were informed about the installation of visible cameras, which were directed towards the entrances and exits of the supermarket. However, there were also several hidden cameras in the supermarket, of which the employees were not informed.

The court noted that Spanish law – as well as international standards – requires fulfilment of the employer's informational obligation previous to surveillance, but this is only one of the criteria taken into account in assessing the adequacy of employee surveillance. If the information has not been disclosed, other guarantees will be more important. It is essential to balance the employees' right to privacy with the protection of the employer's assets. The court observed that the interference with the employees' privacy was proportionate in the end, judging that there existed a reasonable suspicion of serious misconduct by the employees, and that the extent of the losses did constitute appropriate justification.

Therefore I strongly support the second interpretation, according to which it is sufficient to either inform the employees about the monitoring afterwards, or get the employees acquainted with the sole possibility of video monitoring without any other relevant details preceding the surveillance,[9] provided there is a significantly relevant reason for it (such as a risk of a severe property harm caused to the employer). Generally speaking, the possibility to use hidden cameras is still an open issue in the Czech Republic.

8 Cf. Jelínek, 2022, 1013.
9 Cf. Morávek, 2022, pp. 950–965.

2.4. Dummy Models of Cameras

The above-mentioned implies that legislation in the Czech Republic is partly duplicated and overlapping. The powers of the competent supervisory bodies are also doubled. This was relatively well reflected in a recent case dealt with by the Personal Data Protection Office,[10] dealing with the location of dummy cameras in the common premises of the workplace. The surveillance did not meet the definition of hidden monitoring, with the employees fully informed about the presence of these cameras. However, they were not informed that they were only dummy models – unable to make or store any record at all.

As part of its investigation, the office concluded that no breach of general GDPR legislation was caused. As a dummy camera is not capable of collecting any personal data at all, it cannot cause a GDPR breach. However, it pointed strongly to the fact that -in addition to the GDPR obligations - the employer is also obliged by the Labour Code to create favourable working conditions for the employees and ensure their health and safety.[11]

The dummy cameras were located in the common areas of the employer's workplace – specifically at the toilets. The office referred the whole matter to the relevant Regional Labour Inspectorate, which considered the location of the dummy cameras as a breach of the employer's obligation. Camera surveillance done in this form was assessed to be creating undue pressure on the affected employees, which while it represented no breach of the GDPR still violated the Czech Labour Code.

2.5. Partial Summary

In conclusion, it should be highlighted that there is duplicate legislation on camera surveillance in the Czech Republic – with not only the GDPR, but also the Labour Code. There is also an overlap between the competence of the Personal Data Protection Office and the Labour Inspectorates. In accordance with the Section 316 of the Czech Labour Code the employer must not interfere with the employee's privacy in the workplace or in the joint premises of the employer without a serious reason. However, it is not determined what this serious reason may be.

The employer is obliged to directly inform the employees about the scope of the employee surveillance and the methods of its implementation – however I am convinced that this does not prohibit employers from using hidden camera systems.

10 Cf. Czech Personal Data Protection Office (2022) Camera atrapa does not violate GDPR, but its installation can be sanctioned [Online]. Available at: https://uoou.gov.cz/vismo/dokumenty2.asp?id_org=200144&id=55810 (Accessed: 2 October 2023).

11 Cf. Section 302, para. c) of the Czech Labour Code.

This approach is entirely consistent with ECtHR case-law. However, for such monitoring the employers must have very serious reasons.

The general criterion is to proceed adequately towards the employees and always choose the more suitable and less invasive approach of surveillance carried out by the camera systems (this may be surveillance by a superior employee). At the same time, it is unacceptable to continuously monitor common relaxation spaces, especially toilets. On the other hand, the ruggedness of this legislation in some cases – such as the installation of dummy cameras – allows us to sanction a much wider range of inappropriate behaviour by employers than the GDPR would alone.

3.
Monitoring of Employees' Computers

3.1. Basic Definition

3.1.1. Several Comments on the Legislation

This section presents several notes on monitoring work computers. This can include not only installation of programs to allow the employer to remotely monitor activity, but also monitoring of emails and the employees' working environment. In principle, it is not decisive who the owner of these computers is, whether the employer or even a third party. The only important thing is how the employer performs surveillance in relation to a particular computer. In line with the development of modern technologies, there are a number of ways that employees can be monitored. Their range is extensive, and it is certainly not possible to deal with all of them. Some examples include monitoring of keystrokes, screens, mouse movements, observation of the environment around the computer, surveillance by webcam, and email monitoring. In addition there is the installation of data leak prevention systems and new generation firewalls. It should be said that with the current rapid development of technologies, this type of surveillance is becoming increasingly frequent.

Regarding computer surveillance, the above-mentioned legislation applies as well, especially when it comes to camera or video monitoring (in particular random activation of a webcam or microphone, and taking pictures of the environment around the computer). If the employee's personal data is processed through the selected means of surveillance, the GDPR legislation will apply again. In addition, the same Section 316 of the Czech Labour Code can always be related to the matter. Thus, for the employer to carry out surveillance their interest must outweigh the

interests (especially privacy) on the employee's side. And again, there is some overlap between the competence of the Personal Data Protection Office and the Labour Inspectorates.

Based on ECtHR case-law, the employees' privacy in the workplace is always to be protected by the employer. However, this does not grant employees permission to take paid leave and use the employers' devices to arrange their private affairs. According to the relevant interpretation, this is not contrary to the case-law of the ECtHR and the Court of Justice of the EU.[12] It is clear enough that no employer must be obliged to accept the use of professional equipment for employees' private purposes. Compliance with these rules is to be monitored by the employer.

The Czech Labour Code presents the very same opinion. In accordance with Section 316 the employee is prohibited from using work devices for their personal needs, and can do so only with previous consent from their employer. This can be implicit as well. If the employees violate this rule, they carry all the costs and it represents a breach of their duties, which can also lead to the termination of the employment relationship.[13]

However, it should be emphasised that for surveillance carried out by the employers, Section 316 stipulates conditions that must be observed by the employers in addition to the general conditions according to the GDPR.[14] The employer is entitled to monitor compliance solely in a proportionate manner. The Supreme Court of the Czech Republic extends this conclusion, as it stipulates that the surveillance "cannot be performed by the employer completely arbitrarily (in terms of scope, length, thoroughness, etc.), since the employer is entitled to perform this surveillance only in a proportionate manner."[15] The Labour Code leaves the court to define the circle of circumstances at its discretion. In particular, it should be relevant whether "it was a continuous or subsequent surveillance, its length, the scope of whether and to what extent it restricted employees in their activities, whether and to what extent it also interfered with the right to the employees' privacy, etc."[16] It is still necessary to say that the employer's right to monitor its property is not limited to working hours. However, in terms of determining the degree of proportionality of employee surveillance, employees in general are given a greater amount of privacy outside working hours.[17]

12 Cf. Morávek, 2017, pp. 573–577.
13 Cf. Supreme Court, 2014, 21 Cdo 747/2013.
14 Cf. Štefko, 2019, pp. 1246–1254.
15 Cf. Supreme Court, 2012, 21 Cdo 1771/2011.
16 *Ibid.*
17 Cf. Morávek, 2022, pp. 950–965.

3.1.2. Illustrative Examples of Appropriate Execution of the Employees' Surveillance

The method of proportional employee surveillance is essential. For example, if a physical inspection carried out by a superior is sufficient, it may always be more proportionate than surveillance through any kind of tracking software.

At the same time, technical tools preventing computer abuse (e.g. whitelists or blacklists) will always prevail over the subsequent surveillance – i.e. prevention always prevails over surveillance. Even in the case of subsequent monitoring, the employer should restrict the monitoring itself to the quantity and size of the mail correspondence or to the list of domains visited by the employee. It is generally decisive for the proportionality of employee surveillance whether it is a continuous or subsequent surveillance, its length, and whether and to what extent it restricted employees in their activities or interfered with their privacy.[18]

A completely different approach must be applied if the employer knows and accepts that employees use professional devices to arrange their private affairs. If the employer's approach represents a tolerated practice, it is not possible to penalise the employees in any way as they have not committed any breach of their obligations at all. This applies to all employees, including incoming employees, otherwise it would represent a discriminatory approach. Any possible change in the conditions would then have to be made in relation to all employees.

3.2. The Personal Data Protection Office – Surveillance of the Employees' Email Correspondence

3.2.1. The Previous Unsatisfactory Development

Although the rules presented so far may seem natural enough, the preceding development was rather confusing in the Czech Republic. The approach of the Personal Data Protection Office towards email surveillance was significant. The office had previously presented its Standpoint No. 2/2009,[19] focused exclusively on workplace surveillance with a special consideration to monitoring employees' email correspondence.

The office used to strictly divide employees' mail into private and work-related according to the email addresses used. For instance, in case the email was sent to the address *distribution@employers-domain.cz* it was always considered a work-related

18 Cf. Morávek, 2017, pp. 573–577.

19 Cf. Czech Personal Data Protection Office (2009): Stanovisko č. 2/2009, Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště [Online]. Available at: https://uoou.gov.cz/files/stanovisko_2009_2.pdf (Accessed: 2 October 2023).

mail, and the employee was never granted any protection of privacy. Therefore, the employer could monitor the messages delivered to the employee using this address without any restrictions. This rule had to be followed even if this address was only used by one particular employee.

Conversely, the office claimed that in case of the email address starting with the name of the employee (e.g. *Svoboda@employers-domain.cz*), it is more reasonable to assume that the email may contain a message of a private nature, and is therefore subject to privacy protections. Emails sent to an address containing the name and surname of the employee were to be considered private, with no access allowed by the employer. Therefore, the employer was only allowed to monitor the number of received and sent emails, or (if the employer had a real suspicion of misuse of the work facilities for employees' private needs) to whom the employees write these emails, and from whom they receive them.[20] However, this division of email addresses was evidently very strict and in certain cases also outdated and inaccurate.

3.2.2. Remedy of the Harmful State of Things

The office finally realised that this approach had its limits, and the system was partially abandoned. The approach towards email addresses has since been modified, and now the employer shall determine themselves whether the email correspondence is private or work-related according to the topic, the sender, the recipient, or the salutations used, etc. "The employer may carry out the surveillance and check the contents of the employees' e-mail messages (open them and read them) only for a serious reason."[21] Emails qualified as private or containing any private information cannot then be read by the employer. If the employer realises that the email contains any private information only while reading it, they are strongly prohibited from reading on and must pass the email on to the appropriate employee.[22] If possible, the employee shall be informed in advance about the monitoring of their correspondence. Unfortunately, the previous Standpoint No. 2/2009 of the Personal Data Protection Office is still quite widely spread among the employers and the employees, which sometimes results in malpractice in email surveillance.

At the same time, the basic principle of minimising intervention into the protected values of the employees is still applied – proportionality is still the principle on which employee surveillance stands. For example, if an employee is not at the workplace (due to illness or holiday etc.) and does not respond to email correspondence, this

20 Cf. Morávek, 2010, pp. 3–7.
21 Cf. Morávek, 2017, pp. 573–577.
22 Cf. Štefko, 2019, pp. 1246–1254.

would seem to give the employer the right to view the emails instead of the employee – especially if the employer is threatened by serious property damage as a result of any kind of a delay. However, if we really follow the relevant proportionality principle, it is more appropriate to set an automatic response within the employees' e-mail address. This automatic response will then inform the sender that the employee is not present, and to what substitute address the message should be forwarded. In this way, the employer avoids any possible danger in delay and the sender receives all necessary information. However, it should also be emphasised that any automatic response that returns to the sender must not contain any other personal data of the employee in question. It is sufficient to report that the employee is absent until a certain date, but not the reason for their absence at work, etc.[23]

This approach is significantly more appropriate than going through all employees' emails immediately and without prior warning. Nevertheless, there will undoubtedly always be a certain number of cases where an automatic response would not be enough in order to prevent employer's property damage. In such a situation, the employer is justified to carry out surveillance and go through the employees' correspondence themselves.

4.
Consumption of Alcohol or Other Addictive Substances Under Surveillance

4.1. Initial Considerations

The final part of this article focuses on the monitoring of alcohol in the workplace, though everything listed in the following part can also be used regarding other addictive substances. Under Section 106 para. 4 of the Czech Labour Code, the employee is strictly prohibited from consuming alcohol at the employer's workplace;[24] consuming alcohol during working hours both inside and outside the employer's workplace; and entering the workplace under the influence of alcohol. Section 106 of the Labour Code, among other things, generally stipulates that each employee "is obliged to pay attention to his or her own safety, his or her health and the safety and health of natural persons who are directly affected by his or her actions or omissions at work." It is consequently obvious that 'alcohol surveillance' is part of the Health and Safety

23 Cf. Morávek, 2017, pp. 573–577.
24 This prohibits the employees from consuming alcohol in the workplace both during and after the end of their working hours.

requirements in the Czech Republic. Thus, although the main purpose of the previous types of employee surveillance was monitoring of the fulfilment of the employees' work tasks, protection of the employer's property, and prevention of data loss, in the case of alcohol surveillance it is less a case of protection of the employer's property than to prevention of injuries in the workplace and protection of employees' health.

However, the prohibition against alcohol does not apply to employees for which these beverages are part of the performance of their work tasks, or are usually associated with the performance of these tasks.[25] This is especially the case of tasters in the production or trade of alcohol. It can also be the case for employees working in unfavourable microclimatic conditions, who are allowed to drink beer with reduced alcohol content for these causes. Such employees will be, for example, staff of the metallurgical industry.[26]

The employees are also obliged to undergo monitoring as to whether they are under the influence of alcohol. This surveillance can be performed directly by the employer, or the employee can be sent to a suitable medical facility. The employee is only obliged to undergo surveillance based on the instruction of the authorised superior employee.[27] Such a superior must be determined in writing by the employer in advance. If the employee refuses to undergo surveillance, this may mean a breach of professional obligations.[28]An employer who does not ensure the prohibition of alcohol consumption in the workplace - in accordance with the Labour Code - may be fined up to a maximum of CZK 300,000.[29]

4.2. The Surprising Attitude of the Supreme Court of the Czech Republic

Following all of this, it would seem as if the legislation itself is unambiguous. Nevertheless, the Czech Supreme Court recently made the topic much more confusing. In principle, being under the influence of alcohol is not always enough for the employee to seriously breach their contractual obligations. Typically, being under the influence does not always grant the employer any permission to terminate the employment relationship.

In the assessed case,[30] the employee performed dangerous work within the operation of a steel plant. Before the shift started, the employee had a measured blood level of 0.32 ‰ of alcohol during the first breath test. In the second breath test

25 Cf. Section 106 para. 4 of the Czech Labour Code.
26 Cf. Pichrt and Stádník, 2019, pp. 590–599.
27 Cf. Section 106 para. 4 of the Czech Labour Code.
28 Cf. Pichrt and Stádník, 2019, pp. 590–599.
29 Cf. Section 30 para. 1 of the Act No. 251/2005 Coll., on the labour inspection, as amended.
30 Cf. Supreme Court, 2016, 21 Cdo 4733/2015.

(half an hour later) he had a blood alcohol level of 0.23 ‰. The court stressed that even if the employee had entered the employer's workplace under the influence of alcohol, "a state when he or she severely violates his or her duties, may not be given by mere ingestion of alcoholic beverages, but his or her ingestion must happen to such an extent that it affects the reduction of mental functions and overall employee's unreadiness." The assessment of intensity of the relevant breach always depends on specific circumstances. The court also noted that the blood level of 0.2 ‰ of alcohol is considered inconclusive with regard to the so-called physiological level, i.e. the natural level of alcohol.[31] In this case, the court took into account the personality of the employee and fulfilment of his existing tasks as well. The Supreme Court (after assessing all these facts) concluded that there was no fundamental breach of obligations.

The influence of alcohol is apparently only decisive if it directly leads to a certain decrease in the employees' mental or physical abilities. An explanation can be that the employees' abilities must be influenced to such an extent that cannot be ignored (for example the inability to speak, walk, etc.). This conclusion of the quoted judgment means that employers, as a rule, must tolerate a blood alcohol level of up to 0.20 ‰ of alcohol. However, the employers should be able to detect whether an employee who has exceeded this limit has or has not been sufficiently influenced. Nevertheless, there is no concrete guidance set for the employers as it may differ from employee to employee,[32] and Supreme Court case-law is extremely rare in this respect. Another negative aspect of this case-law lies in the fact that it forces any employer who wants to fight against alcohol abuse not only to carry out the appropriate alcohol surveillance, but also to seek witnesses or any other acceptable proof of the decrease in the employees' abilities.

This decision is groundbreaking in a manner. In principle it may now be possible to consume alcoholic beverages during working hours and enter the workplace under the influence of alcohol, unless the alcohol level exceeds a certain limit. However, it is still true that the circumstances of each individual case must always be thoroughly assessed.[33]

For the sake of completeness it should be noted that the Constitutional Court of the Czech Republic also rejects zero tolerance of alcohol in the case of the employees' alcohol surveillance.[34]The Constitutional Court relies its argumentation on the fact that, among other things, even the public law legislation does not provide for the zero

31 Therefore, it also evaluated, among other things, the fact that before the beginning of the shift the result of the finding was only 0.23 ‰ of alcohol, which is close to the given physiological level.

32 Cf. Supreme Court, 2016, 21 Cdo 4733/2015.

33 Cf. Jelínek and Odrobinová, 2022, pp. 418–423.

34 Cf. Constitutional Court, 2017, III. ÚS 912/17.

tolerance of alcohol, including in driving. "In practice, even the Road Traffic Act mentioned by the employer does not consider zero alcohol levels in the body but works with a so-called physiological level of 0.20 ‰, from which the eventually measured values exceeding it are deducted."[35]

5.
Conclusions

I strongly believe that, regardless of the aforementioned legislation and case-law, employee surveillance should be especially well balanced to prevent employees from feeling stressed or over-monitored. These employees habitually tend to work less hard, which results in precisely the opposite effect we want to achieve.

This contribution focused on the issue of employee surveillance from the Czech point of view. It discussed the basic legal framework of surveillance that employers in the Czech Republic carry out upon their employees. In particular, the aspect of relevant GDPR legal regulations and the Labour Code, were discussed in detail. Obviously, other topics such as the development of modern technologies were also mentioned, as they have an impact on monitoring as well.

The intention was to cover employee surveillance in the Czech Republic relatively widely and from different aspects, including video surveillance, monitoring of the employees' computers, and consumption of alcohol or other addictive substances under surveillance. There are many conclusions. For example, the employer is obliged to directly inform the employees of the scope of surveillance and the methods of its implementation in advance. According to some opinions, this condition stated in Section 316 of the Czech Labour Code completely excludes the possibility of carrying out covert employee surveillance. However, my opinion is that it is necessary to conclude the exact opposite. Only this conclusion can be consistent with the case-law of the European Court of Human Rights.

Naturally, the article also brought an overview of the basic limits that the employer must take into account when monitoring employee computers and monitoring alcohol in the workplace. In this respect, the surveillance faces some major restrictions, with which each employer should become acquainted. At the same time, the role of the Czech Personal Data Protection Office was emphasised in many places. The methodology, which contains the office's view on employee surveillance carried out through camera systems, was obviously mentioned and disassembled in detail. Its positive could probably be a degree of facilitating the position of certain personal data processors (i.e. employers) dealing with personal data obtained from the camera

35 *Ibid.*

systems. In direct contradiction then is the former unclear and confused opinion of the Personal Data Protection Office on surveillance and monitoring of the employees' emails. This original state was clearly unsatisfactory and was therefore subject to much criticism. Nevertheless, the new approach adopted by the office seems to be significantly more appropriate.

In summary, employee surveillance is certainly a highly relevant topic. Most employers have either tested it in the workplace in some form, or have already included it in their ordinary operations at their workplaces. As it often happens that some of these employers tend to modify and interpret the relevant legislation incorrectly – most often in a manner more favourable for them – it is necessary to pay particular attention to compliance with legal rules. The right to employees' privacy and the interest of the employer in protecting their assets often collide, and it is precisely for these reasons that flawless knowledge of legal regulations is so important.

Bibliography

- Act No. 251/2005 Coll., on the labour inspection, as amended.
- Act No. 262/2006 Coll., the Labour Code, as amended.
- Act No. 110/2019 Coll., on the processing of personal data, as amended.
- Czech Personal Data Protection Office (2009): Stanovisko č. 2/2009, Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště [Online]. Available at: https://uoou.gov.cz/files/stanovisko_2009_2.pdf (Accessed: 2 October 2023)
- Czech Personal Data Protection Office (2022) Camera atrapa does not violate GDPR, but its installation can be sanctioned [Online]. Available at https://uoou.gov.cz/vismo/dokumenty2.asp?id_org=200144&id=55810 (Accessed: 2 October 2023)
- Czech Personal Data Protection Office (2023): Methodology for the design and operation of the camera systems in terms of the processing and protection of personal data [Online]. Available at: https://uoou.gov.cz/media/novinky/dokumenty/metodika-kamery0-983.pdf (Accessed: 27 October 2023)
- Constitutional Court of Czech republic, 2017, III. ÚS 912/17
- European Data Protection Board (2020): Guidelines 3/2019 on processing of personal data through video devices [Online]. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (Accessed: 27 October 2023)
- Great Senate of the ECHR on López Ribalda and others Versus Spain [GC], as of the day 17. 10. 2019, in matters 1874/13 and 8567/13.
- Jelínek T. (2022) '§ 316' in Valentová, K. et al. *Zákoník práce, komentář*, 2nd edn. Praha: C. H. Beck, p. 1013.
- Jelínek T. and Odrobinová V. (2022) '§ 106' in Valentová, K. et al. *Zákoník práce, komentář*, 2nd edn. Praha: C. H. Beck, pp. 418–423.
- Pichrt, J. and Stádník, J. (2019) '§ 106, Práva a povinnosti zaměstnance' in Bělina, M. and Drápal, L. et al. *Zákoník práce. Komentář*, 3rd edn. Praha: C. H. Beck, pp. 590–599.
- Morávek, J. (2010) '*Kdy je možné evidovat přístup zaměstnance na internet a otevřít jeho e-mailovou poštu?*', Právo pro podnikání a zaměstnání, 20(3), pp. 3–7.
- Morávek, J. (2017) '*Kontrola a sledování zaměstnanců – výklad § 316 ZPr*', Právní rozhledy, 25(17), pp. 573–577.
- Morávek, J. (2022) '§ 316' in Pichrt, J. et al. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*, 2nd edn. Praha: Wolters Kluwer, pp. 950–965.
- 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.
- Supreme Administrative Court of the Czech Republic, as of the day 10. 5. 2006, file number 3 As 21/2005-105.

- Supreme Court of the Czech Republic, as of the day 16. 8. 2012, file number 21 Cdo 1771/2011.
- Supreme Court of the Czech Republic, as of the day 7. 8. 2014, file number 21 Cdo 747/2013.
- Supreme Court of the Czech Republic, as of the day 19. 12. 2016, file number 21 Cdo 4733/2015.
- Štefko, M. (2019) '§ 316; Majetek zaměstnavatele; soukromí zaměstnance; nesouvisející informace' in Bělina, M. and Drápal, L. et al. *Zákoník práce. Komentář,* 3rd edn. Praha: C. H. Beck, pp. 1246–1254.