University of Miskolc

Faculty of Law

Deák Ferenc Doctoral School of Law

Forms of Monitoring in the Workplace in the Visegrad Countries. Comparative Legal Research

PhD Thesis

Head of the Doctoral School: Prof. Dr. Erika Róth

Programme: Central European Comparative Law

Author: mgr Tomasz Mirosławski

PhD Supervisor: dr Michał Barański, Assistant Professor at the University of Silesia in Katowice

MISKOLC

2026

Recommendation for the final defence of the dissertation authored by mgr Tomasz Mirosławski, entitled: *Forms of Monitoring in the Workplace in the Visegrad Countries. Comparative Legal Research.*

Hereby, I submit my recommendation of the PhD dissertation entitled: "Forms of Monitoring in the Workplace in the Visegrad Countries. Comparative Legal Research" prepared by mgr Tomasz Mirosławski under the framework of the Central European Comparative Law programme of the University of Miskolc and Central European Academy of the University of Miskolc.

The dissertation addresses a particularly dynamic and timely topic situated at the intersection of labour law, privacy law, and data protection law. Using the framework of comparative legal research, it explores the evolution, forms, and limitations of workplace monitoring within the Visegrad Group countries. The growing presence of new technologies in the employment sector underscores the need for relevant and scrutinized legal environments at the national and regional levels. The selection of the Visegrad Group is highly justified, as these countries share a unique historical transition and similar socioeconomic conditions that have shaped their post-transition labour laws. Furthermore, their simultaneous integration into the European Union provides an excellent comparative basis for analysing how these regional legal systems adapt to common European data protection standards.

The dissertation is structured into four main chapters, preceded by an introduction and concluding with de lege ferenda remarks. Chapter I provides comprehensive introductory remarks, exploring the origins of monitoring, from its analogue history and Taylorism to modern applications. It outlines extra-legal perspectives - including sociological, psychological, and colloquial views - before systematically detailing workplace monitoring through the lens of international, European, and specific national regulations across Hungary, Poland, Czechia, and Slovakia. Chapter II meticulously details the objectives and forms of employee monitoring. It analyzes the employer's general right to monitor the usage of production means and explores various methods, such as communication monitoring, covert surveillance, and GPS tracking. Furthermore, it addresses critical practical dimensions including personal workplace inspections and occupational health and safety measures, such as sobriety monitoring, under the varying Visegrad models. Chapter III is devoted to the critical balance between surveillance and the right to privacy. It presents a constitutional perspective on privacy rights within the Visegrad Group and evaluates the employee's right to privacy from a human rights standpoint, paying particular attention to the inclusion of the professional sphere in the concept of private life by the European Court of Human Rights. Chapter IV delves into the axiological considerations of workplace monitoring. It discusses the protective function of labour law, human and worker dignity, and the profound shift from traditional subordination to "technological subordination" in the modern work process. Finally, it reflects on the humanisation of work and human interactions within a world governed by new technologies.

The dissertation effectively integrates comparative legal analysis with a focus on domestic legal frameworks in Central Europe, offering a significant contribution to the understanding of modern labour law development. The comprehensive analysis of national regulations from the Visegrad region represents a novel and highly relevant approach.

Tomasz Mirosławski exhibits a keen insight into the legal complexities surrounding the implementation and regulation of modern monitoring forms in the workplace.

The PhD thesis contains credible data, and the scientific results of the PhD thesis are the result of the candidate's own research work. The PhD thesis meets the formal requirements of the Doctoral School.

In conclusion, I recommend that the doctoral thesis be admitted to the final defence as part of the candidate’s doctoral programme.

Budapest, 24 August 2026

Supervisor
dr Michał Barański
University of Silesia in Katowice

I would like to thank my supervisor, dr Michał Barański, for his invaluable guidance and willingness to support me throughout the research that has resulted in this doctoral thesis. I am also deeply grateful to the entire team at the Central European Academy of the University of Miskolc, and especially its management, for the trust they placed in me and for giving me the extraordinary opportunity to contribute to the development of labour law scholarship in Central and Eastern Europe.

Finally, my special gratitude goes to my wife, my parents, and my entire family, whose unwavering care and support have helped me overcome the challenges of everyday life.

Table of Contents

List of abbreviations

AI – artificial intelligence
BYOD – Bring Your Own Device
CCTV – closed-circuit television
CFREU – Charter of Fundamental Rights of the European Union
CJEU – Court of Justice of the European Union
CLC – Czech Labour Code
CoE – Council of Europe
CoP – Code of Practice
DPA – data protection authority
ECHR – European Convention on Human Rights
ECSR – European Committee of Social Rights
ECtHR – European Court of Human Rights
EDPB – European Data Protection Board
EDPS – European Data Protection Supervisor
ESC – European Social Charter
EU – European Union
GDPR – General Data Protection Regulation
GPS – Global Positioning System
HLC – Hungarian Labour Code
ICT – information and communication technology
ILO – International Labour Organization
IoT – Internet of Things
IT – information technology
MDM – Mobile Device Management
NAIH – Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information)
OECD – Organisation for Economic Co-operation and Development
OHS – occupational health and safety
PLC – Polish Labour Code
SIM – subscriber identity module
SLC – Slovak Labour Code
SUIP – Státní úřad inspekce práce (Czech State Labour Inspection Office)

UK – United Kingdom

UOOU – Úřad pro ochranu osobních údajů (Czech Office for Personal Data Protection)

V4 – Visegrad Group (Visegrad Four)

VSD – Value Sensitive Design

WHO – World Health Organization

WP – Article 29 Data Protection Working Party

Introduction

1. The topic

The 21st century has brought the world a new phase of economic development called the fourth industrial revolution. This phenomenon is based on digitisation, platformisation, the automation of workplaces, and the development of AI, creating a system whose main engine is data processing.[1] It has led to the situation in which technology permeates every aspect of our daily life. We communicate through messaging apps, search for information online, share intimate details with "self-tracking apps", and even use algorithms to find romantic partners. As a result, vast amounts of personal data are being collected with increasing precision.

While technological progress offers many benefits, it also exposes significant risks - particularly the erosion of privacy and the uncontrolled accumulation of personal data by numerous external actors. These concerns are widely acknowledged in consumer protection debates.

However, one critical area remains underexamined, namely, workplace surveillance. Despite undergoing a parallel technological transformation, it has not received the public attention it deserves.

In modern workplaces, employees can expect that an extensive part of their daily activity will become the object of monitoring, including the content of their emails, internet usage, keys pushed on the keyboard, social media, what paths they take within the workplace and even how many times they use the bathroom. Moreover, in recent years, employees' collected data are increasingly analysed with the help of specific algorithms, also in order to assess the efficiency and quality of the work provided.

Certainly, surveillance at the workplace is not a new topic, and it is widely acknowledged that it has been an inherent component of the capitalist mode of production since its early beginnings. Nevertheless, as it is pointed out in the thesis, monitoring has been an important part of the labour process even before capitalism.

However, due to the emergence of the new electronic forms of monitoring, its increasing scope and extensive interference with the lives of employees, also outside the workplace, it has become an invaluable topic requiring detailed research.

As Edwards, Martin and Henderson indicate:

---

[1] Męcina, 2023, pp. 23-67; Instytut Analiz Rynku Pracy, 2020, pp. 3-5.

"(Employee surveillance) is the Cinderella sister of surveillance studies: neither as outright shocking to citizens as state surveillance in the post-Snowden era, nor as ubiquitously discussed as consumer targeting and profiling in the "surveillance capitalism" ecology of social media, search and e-commerce platforms like Google, Facebook, Amazon, etc."[2]

Considering the fact that most people spend a significant part of their lives as employees in the hierarchical employer-employee relationship, where they are exposed to excessive monitoring and a lack of privacy, the fundamental research questions are:

1. Are the regulations underpinning current workplace monitoring models in the V4 countries capable of ensuring respect for employees' dignity, particularly in the context of modern forms of workplace monitoring?
2. Is there a model of workplace monitoring in the Visegrad region that strikes the desired balance between employees' privacy and employers' interests, and could serve as a benchmark for the other V4 countries?

The path to answering these research questions has shaped the structure of this thesis, which consists of four chapters and a conclusion.

Chapter I "Introductory Remarks" introduces the conceptual, historical and legal foundations of the whole thesis. It commences with examining the origins and evolution of the phenomenon of workplace monitoring, including pre-industrial forms of labour surveillance, the five-phase model of the development of monitoring and the influence of the idea of Taylorism on contemporary forms of managerial control and deriving from them monitoring measures. Moreover, the chapter broadens the analysis by describing extra-legal perspectives on monitoring, including sociological, psychological and colloquial ones. Eventually, it places the subject matter of the thesis in the realm of international, European and national regulations, with specific attention to the workplace monitoring models adopted in Hungary, Poland, the Czech Republic and Slovakia.

Chapter II "Objectives and Forms of Employee Monitoring" takes the focal role within the comparative part of the thesis and is based on the methodological assumption that the form of workplace monitoring should be analysed only in connection with the objectives that are intended to be achieved. Instead of presenting monitoring measures as independent technical tools, the chapter categorises them according to their purpose: monitoring connected with the

[2] Edwards, Martin, and Henderson, 2018, p. 11.

performance of employees' tasks, monitoring aimed at protecting the employer's property, and monitoring justified by occupational health and safety principles, and focuses on the most characteristic forms of monitoring being in the "forefront" of each of the mentioned areas. Taking into account the specificity of V4 workplace monitoring models, the chapter examines communication monitoring, monitoring extending beyond communication, covert monitoring, GPS tracking, personal inspections in the workplace and sobriety monitoring. Particular attention may be attracted by the fact that, within the category of Occupational Health and Safety, the analysis focuses exclusively on sobriety monitoring. This methodological choice is justified by several crucial factors: sobriety monitoring is a legally important and practically topical form of monitoring within workplaces, present in all Visegrad countries; it most clearly fits within the broader concept of workplace monitoring among health and safety control means; and most significantly, it reflects a continuing practical problem in the region, where sobriety remains a sensitive and socially relevant issue. Furthermore, it properly illustrates the ongoing conflict between the employer's organisational obligation to ensure hygienic, healthy and safe conditions within the workplace and the employee's right to privacy, bodily integrity, dignity and personal data protection. Subsequently, the chapter delves into the general principles governing the usage of monitoring, such as its territorial scope, data retention period; the determination of objectives, scope and manner of monitoring; information obligation; proportionality and the requirement of legitimate grounds for interference with employee privacy. The presented structure of the chapter enables the comparison not only of the admissibility of particular forms of monitoring in the Visegrad countries in legal terms, but also of the different regulatory and social logics behind their use.

Chapter III "Surveillance and the Right to Privacy" analyses workplace monitoring from the perspective of the employee's right to privacy. It examines this right from the perspective of three interconnected levels: the constitutional system of the V4 countries, the human rights framework established particularly by the European Convention on Human Rights and the jurisprudence of the European Court of Human Rights, and the notion of privacy as a personal right. The chapter focuses on the scope of privacy protection in employment, the involvement of the professional sphere within the "circle" of private life, and the possible limitations of privacy regarding employees. In other words, the chapter outlines the legal framework on the basis of which it is possible to assess the circumstances in which an interference with the privacy of employees caused by monitoring measures may be justified.

Chapter IV "Axiological Considerations on Workplace Monitoring" develops an axiological review of workplace monitoring, relating it to the fundamental values of labour law in the

Visegrad countries. It begins with the concepts of human dignity, worker's dignity and the protective function of labour law, treating them as the main limits to the employer's monitoring authority. Further, the chapter portrays employee subordination as a defining feature of the employment relationship in Poland, Hungary, the Czech Republic and Slovakia, and shows how technological development has transformed traditional subordination into forms of technological subordination. In the last part, it reflects on the relationship between workplace monitoring and the humanisation of work, especially in the context of new technologies and the changing nature of human interactions in the workplace.

The final part"Conclusion – *De lege ferenda* remarks" serves as a synthesis of the findings indicated in the thesis and formulates *de lege ferenda* remarks concerning the future development of workplace monitoring regulation in the Visegrad countries. It highlights the perception of the workplace monitoring not merely as a technological phenomenon, but as a socio-political and legal construct driven by historical development, power relations, economic systems and the changes in the organisation of work processes. This fragment identifies the need to improve existing workplace monitoring models, especially by clarifying ambiguous legal concepts, strengthening legal certainty and ensuring compliance of monitoring measures with employee autonomy, privacy and dignity. The approach adopted in this part distinguishes between narrower legal proposals whose main objective is to improve existing regulations and broader, more systemic recommendations concerning the future relationship between technology, labour law and the idea of the humanisation of work.

In summary, the main objective of the research is to analyse, describe and compare legal regulations governing workplace monitoring in the Visegrad countries. On this basis, the thesis aims to develop certain *de lege ferenda* proposals concerning the future development of workplace monitoring regulation, in light of the increasing advancement of monitoring technologies and the requirement to ensure a just balance between employers' legitimate interests and the protection of employees' dignity, privacy and fundamental rights. The proposals are intended to provide an initial basis for further legislative reflection, with a particular focus on the national level.

2. The area of comparative legal research - countries of the Visegrad Group

The dissertation states a contribution to the developing field of studies on the legal culture and legal systems of the Central and Eastern European region, the central point of which, without any doubt, are countries of the Visegrad Group.

Poland, Hungary, the Czech Republic, and Slovakia, according to a broader collective European consciousness, are widely regarded as a bloc of countries sharing the geographical position and, to a certain extent, the same or at least similar historical experiences. These factors have fostered a common understanding of interests and a distinct legal culture of the four states - one that often contrasts with that of Western Europe and is not always fully recognised or understood by outsiders. Indicated similarities, but also the existing differences, have created a need for pioneering comparative legal research on the issue of workplace monitoring within the legal systems (primarily labour law) of the V4 countries, so that the ongoing debate on changes to labour law brought about by technological developments - including the possibility of employers applying new forms of monitoring that have a significant impact on employees' right to privacy - does not take place without a strong voice from this region, which covers approximately 14.3% of the European Union's population.[3]

The basis for this research within the Visegrad Group region is the fact that all four member states belong to the same scheme covering the right of employees to privacy, which consists of three interlinked levels of regulation.

2.1. The first level of regulation

The first level is the human rights framework established by the European Convention on Human Rights[4], whose signatories are all four V4 countries. Particularly, Article 8 of the ECHR grants the right to respect for private and family life. In addition to the provisions of the ECHR, the case law of the European Court of Human Rights in Strasbourg[5] is also of great importance as it provides remarkable guidelines on workplace monitoring.

At the EU level, the Charter of Fundamental Rights of the European Union[6] provides a right to respect for private life and the protection of personal data in Articles 7 and 8. It is also noteworthy that, according to its preamble, the Charter reaffirms the rights guaranteed by the ECHR as well as the case law developed by the ECtHR.

---

[3] Ambroziak, Ł., Chojna, J., Gniadek, J., Juszczak, A., Miniszewski, M., Strzelecki, J., Szpor, A., Śliwowski, P., Święcicki, I., Wąsiński, M. 2020, *Grupa Wyszehradzka – 30 lat transformacji, integracji i rozwoju*, Warszawa: Polski Instytut Ekonomiczny, p. 6.
[4] European Convention on Human Rights, as amended by Protocols Nos. 11, 14 and 15, ETS No. 005 (hereinafter: ECHR).
[5] Hereinafter: ECtHR.
[6] Charter of Fundamental Rights of the European Union, 200/C 364/01 (hereinafter: CFREU).

Moreover, human rights that are relevant in the context of the issue of workplace monitoring are also protected at the constitutional level of Poland, Hungary, the Czech Republic and Slovakia.

The Constitution of the Republic of Poland from 1997[7] gives everyone the right to privacy (Art. 47), and information autonomy (Art. 51). Similarly, the Fundamental Law of Hungary[8] in Art. 6 (1) and (3) establishes the right to privacy and right to protection of personal data. The Charter of Fundamental Rights and Freedoms of the Czech Republic[9] also guarantees the inviolability of the person and his or her privacy (Art 7 (1)), protection against unwarranted processing of personal data (Art 10) and confidentiality of communications (Art 13). The situation is no different in the case of Slovakia. The Constitution of the Slovak Republic[10] recognises the right of every individual to integrity and privacy (Art 16), the general right to privacy and family life and the right to be protected against unjustified processing of personal data (Art 19) and, like the Czech Charter of Fundamental Rights, the confidentiality of communications (Art 22).

2.2. The second level of regulation

The second level is the law related specifically to data protection. In particular, the data protection regimes of the EU Member States, including countries of V4, have been regulated with the 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)[11], which entered into force on 25 May 2018 and is directly and in its entirety applicable in all of them.

The entry into force of the GDPR marked a milestone for personal data protection systems in the Visegrad Group countries, as, with the exception of the Czech Republic, it triggered a process of amending national legislation covering it, including, what is most important in view of the subject matter of the thesis, the provisions of labour codes concerning monitoring.

---

[7] Constitution of the Republic of Poland of 2nd April 1997 no. 78 item 483.
[8] Fundamental Law of Hungary of 25 April 2011.
[9] Charter of Fundamental Rights and Freedoms of 16 December 1992 (Const. act No. 2/1993 Coll. as amended by constitutional act No. 162/1998 Coll.).
[10] Constitution of the Slovak Republic of 1 September 1992, 460/1992 Zb.
[11] 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).

2.3. The third level of regulation

The third level concerns employee privacy, which is a source of diversity among Member States stemming from the national labour laws. Article 88 of the GDPR gave room for Member States to specify rules on data processing in the context of employment according to their own views and needs. The "flexibility clause" resulted in different approaches to regulating workplace monitoring among member states. The different approaches reflect national traditions and the different regulatory methods in which labour law has been shaped for decades, which is clearly visible, for instance, within the Visegrad Group.

3. Methodology

The research is grounded in the EU law, international law and first and foremost, national regulations.

Regarding national legislation, the core of the analysis is labour law provisions and provisions of other acts from the field of, *inter alia*, civil law, occupational health and safety and data protection, regulating directly and indirectly the V4 states' models of workplace monitoring. In order to comprehensively approach the topic, the thesis also takes into account constitutional standards concerning privacy, dignity and personal rights. The statutory research is complemented by a detailed examination of the case law of Constitutional Courts and Tribunals, Supreme Courts, domestic common courts, along with the decisions, guidelines and secondary materials issued by national data protection authorities. Applied method makes it possible to assess not only the formal wording of national regulations, but also their practical interpretation in the context of forms of workplace monitoring.

In the realm of European Union law, the main focus is on 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[12]. However, given its direct and comprehensive applicability to Member States, an analysis of its individual parts, and in particular the rules relating to data processing, has not been presented in a separate, comprehensive section of the thesis, but is

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter: Directive 95/46/EC).

primarily addressed in Chapter II as part of the analysis of specific forms of surveillance, as this approach enables a better understanding of the relationship and the impact that the GDPR has had on workplace monitoring models in the V4 countries. A considerable amount of focus is also devoted to the Charter of Fundamental Rights of the European Union, as well as acts from the EU legal sphere with no legally binding effect - framework agreements of European social partners, opinions of Article 29 Data Protection Working Party, guidelines of the European Data Protection Board, etc.

Due to international law, the specific analysis is carried out in the context of the European Convention of Human Rights, European Social Charter and Convention no. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data[13] (currently Convention 108+ as it was modernised in 2018[14]). As in the case of EU law, international soft law instruments are also examined, in particular the Council of Europe's Recommendation of the Committee of Ministers to Member States No. (89) 2 on the Protection of Personal Data Used for Employment Purposes[15] and the Recommendation CM/Rec(2015)5 on the processing of personal data in the context of employment[16], as, despite their lack of binding force, some of the solutions presented in them have been incorporated into legally binding acts. Such measures also have a significant influence on doctrinal debate.

The dogmatic-legal analysis employed in this thesis also encompasses secondary materials developed during legislative processes, particularly of national regulations, as well as a wide range of national and foreign reference works devoted to labour law doctrine, human rights, European Union and international law, legal axiology, modern technologies and AI, and digital economy. A significant point of reference for conducted research is also the literature from the field of occupational psychology and organisational sociology. Owing to the practical nature of the subject matter, a substantial part of the considerations included in the thesis is based on the case law of national courts, constitutional courts and tribunals, and data protection authorities, as well as that of the Court of Justice of the European Union and the European Court of Human Rights. The body of the indicated case law addresses issues related to employee monitoring, the protection of personal data, and the right to privacy in the employment context.

---

[13] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981 (hereinafter: Convention 108).
[14] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data adopted on 18 May 2018 (hereinafter: Convention 108+).
[15] Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes, 18 January 1989 (hereinafter Recommendation No. (89) 2).
[16] Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the Processing of Personal Data in the Context of Employment, 1 April 2015 (hereinafter: Recommendation CM/Rec(2015)5).

Therefore, the backbone of the research is the legal-comparative method, supplemented by theoretical, dogmatic-legal and axiological perspectives.

Moreover, the initial part of the thesis approaches workplace monitoring not only as a legal institution but also as a socio-political phenomenon that has evolved alongside changes in society, industrial development, and models of work organisation. It examines the historical origins of workplace monitoring and argues that contemporary practices remain strongly influenced by the principles of scientific management developed by Frederick Winslow Taylor. At the same time, current labour market trends contribute to the re-emergence of even pre-Taylorian forms of control, such as the moral scrutiny of employees exemplified by Robert Owen's "silent monitor." Consequently, in addition to the legal research methods outlined above, the historical-materialist method also plays a significant role in this study.

Chapter I. Introductory Remarks

1. Origins

It is a challenging task to define workplace monitoring. The notion itself is very vague and, in general, can be described as an action of an employer which aims to observe employees by various means.[17] Similar definition of employee monitoring is expressed by the International Labour Organisation (ILO), which in the Code of Practice on the Protection of Workers' Personal Data indicates that "the term 'monitoring' includes, but is not limited to, the use of devices such as computers, cameras, video equipment, sound devices, telephones and other communication equipment, various methods of establishing identity and location, or any other method of surveillance".[18] Therefore, ILO states that the term "monitoring" may incorporate a variety of surveillance methods, catalogue of which cannot be enumerative and closed.

It is puzzling that, despite years of research and interest in this subject, it remains impossible to encapsulate it within a single, universal definition. It is not without reason. Employee monitoring or broader labour monitoring has been accompanying mankind for thousands of years and is a constantly evolving concept, making it exceedingly complex, if not impossible, to encapsulate in a unique and uniform definition. The definition of employee monitoring will evolve according to societal changes and the forms of work that are dominant at the time. It will have to be defined differently in relation to hunter-gatherer societies and primitive communes, in relation to the times of the first industrial revolution and in relation to the contemporary digital era of Industry 4.0. Moreover, the understanding of monitoring and the connotation associated with the term may vary regionally, due to the experiences and history of certain nations and social groups. Nations that have experienced totalitarian or authoritarian regimes[19], where control and surveillance were key elements, will have a different understanding and associations with workplace monitoring than nations with no such experiences.

On the other hand, as noted in the introduction, workplace monitoring remains less of a focus of research than other areas of monitoring within the field of surveillance studies. This raises

[17] Barański and Giermak, 2017, p. 197.
[18] ILO Code of Practice (hereinafter: CoP) on the protection of workers' personal data indicates, 1997, point 3, par. 3.3.
[19] Such, e.g. countries of the Visegrad group during the times of Soviet-type dictatorship – Poland (Republic of Poland 1944 – 1952 and Polish People's Republic 1952 – 1989), Czech Republic (Czechoslovak Socialist Republic 1948 - 1992), Slovakia (Czechoslovak Socialist Republic 1948 - 1992) and Hungary (Hungarian People's Republic 1949 - 1989).

an important question – Why does workplace monitoring receive relatively so little attention, despite the fact that most people spend a significant part of their lives at work? Considering its impact on individuals' daily lives, one would expect it to be a major area of concern for both citizens and researchers. Yet, it receives less coverage than other forms of surveillance and monitoring. Could it be that, after so many years of employee monitoring, it has become seen as a natural aspect of work, stemming from an organisational function of an employer defined in the labour law legislation of most European countries? And if so, has it always been this way?

Recently, under the influence of changes in the working environment, new forms and an increasingly broader scope of employee monitoring, there has been a growing and recurring interest in this topic. However, in order to fully understand the issue of contemporary workplace monitoring and the shape it has taken, it is essential to look at the phenomenon of workplace monitoring from a historical perspective - examine how it has developed, how its characteristics have evolved and which scientific theories have decisively influenced its forms.

1.1. Five-phase Model of the Historical Development of Workplace Monitoring

Many authors covering the subject of workplace monitoring in their works, when writing about its history, identify its origins with the emergence of the factory work system at the beginning of the 20th century and, above all, with the person of F. W. Taylor and his work entitled "The Principles of Scientific Management"[20].

One of the models that takes as its starting point the evoked historical moment of the birth of a new form and organisation of production is the five-phase model proposed by Edwards, Martin and Henderson.[21] In that model, the first phase of the historical development of workplace monitoring is referred to as "Surveillance 1.0: Analogue World". While elaborating on that phase, the authors point out that the growth of factories as a new organisational form of workplace[22], in combination with the ideas of J. Bentham[23] and F. W. Taylor, resulted in placing the main focus on workforce efficiency, which was to be significantly increased by managerial control and monitoring of employees. In the initial stage, forms of monitoring were based on the adequate distribution of tasks among workers, their close observation and the measurement

[20] Taylor, 1919 (1911).
[21] Edwards, Martin and Henderson, 2018. pp. 3-4.
[22] Landes, 1969, p. 2.
[23] Božovič, 1995 (1787), pp. 29-95.

of the time required to perform certain activities in the workplace. However, as employers began to attach greater importance to monitoring, the forms of monitoring expanded and became a dominant factor influencing employees' working and wage conditions, recruitment policies, and overall work environment.

The second phase, "Surveillance 2.0: Database Nation", dates back to the second half of the 20th century and began with the increasing use of computers in the workplace, advancing digitalisation and electronic data processing. At this stage, the monitoring of employees has become more detailed, as computers used by employees as a work tool have given employers the ability to monitor the employee's interactions and activities carried out through such equipment. By monitoring the keyboard keys, the mouse cursor and the programmes used by the employee, employers were able to gather detailed data on the employee's behaviour and preferences. In addition, the recording of employee data in databases gave employers the ability to engage in "database surveillance" - focusing on individuals and continuously comparing and analysing them against the total workforce. The usage of databases enabled the creation of extensive profiles, including access to employees' personal lifestyles. The development of data collection techniques provided fertile ground for even more sophisticated monitoring systems in the future, which increasingly encroached on employees' privacy.

The next phase of workplace monitoring is "Surveillance 3.0: The Internet and Interception of Communications". This phase is a continuation of the second phase, closely tied to ongoing digitisation. However, the defining characteristic that separates these phases is the Internet, specifically its increasing use as a new tool in many workplaces starting in the mid-1990s. On one hand, this development enhanced work efficiency and led to new forms of work (e.g., telework or remote work). On the other hand, Internet access in the workplace brought new risks related to its misuse by employees, such as wasting working time, neglecting duties, using the Internet for non-work purposes, or downloading inappropriate content onto company devices. Employers, recognising these threats and seeking to counteract them, began adopting new employee monitoring tools, such as checking company phone records, examining company email accounts, and reviewing the history of browsing during working hours.

These new forms of monitoring extended beyond the traditional boundaries of the workplace. Through them, employers not only obtained information about work-related activities but also accessed data about workers' private lives, such as personal opinions expressed online, interactions on social media, and personal relationships.[24] Authors aptly point out that the boundary between online and real "offline" life is increasingly blurred. Many individuals consider their online presence an integral part of their identity, sharing details about their private lives, families, friends, and interests on various online platforms, thus exposing themselves to a greater likelihood of being monitored.

Nevertheless, employers should restrict their monitoring to work-related activities, and employees' private lives should remain respected. However, modern surveillance tools and the monitoring opportunities they provide often lead to these limitations being inadequately observed by employers.

The fourth and penultimate phase is "Surveillance 4.0: Smart Tech, Ubiquitous Computing and the Internet of Workers". This phase, as proposed by Edwards, is grounded in a new technological phenomenon significantly impacting workplace monitoring: the Internet of Things (IoT). The IoT refers to a network of objects and environments equipped with processors and wireless connections, allowing them to be identified, located, and managed via the Internet.[25] This connectivity enables devices and spaces to interact autonomously without human intervention while continuously collecting data on various aspects.[26]

In the workplace, IoT typically takes the form of small devices that can be installed in specific locations, on everyday items, work tools, or even on employees' bodies. These devices enable discreet, continuous, and extensive real-time monitoring of employees, collecting data on a wide range of activities.[27] The development of IoT has resulted in the monitoring of employee behaviours and activities that were previously difficult or deemed impossible to measure.[28] This is especially evident in the monitoring of employees' mental and emotional states, which has gained increasing attention in recent years.[29] In earlier phases of workplace monitoring development, such surveillance would not have been feasible primarily due to technical limitations.

The final fifth stage of the proposed historical model is "Surveillance 5.0: The Age of Algorithms". It marks the current state of workplace monitoring development, characterised by

[24] Intrusion into the private lives of employees through the aforementioned forms of monitoring has been confirmed by ECtHR case law. See e.g. ECtHR judgments in Halford v. the United Kingdom from 25 June 1997, Copland v. the United Kingdom from 3 April 2007, Bărbulescu v. Romania from 5 September 2017.
[25] Molè, 2022, pp. 89-90.
[26] Lupton, 2016, pp. 28–29.
[27] A characteristic example of such devices are the wristbands that employees are expected to wear to monitor their movement and activities in the workplace - see: Jarrahi et al., 2021, p. 5. It is worth mentioning that there are even more controversial devices used to track employees, such as subcutaneous chips, that can be injected into employees - see: Surdykowska, 2023, pp. 1-15.
[28] Richards, 2013, p. 1940.
[29] Ienca and Malgieri, 2022, pp. 2-4.

the extensive use of machine learning technologies and algorithms to observe the workforce and assist management in decision-making concerning employees. Machine learning and algorithms are tied to vast databases, or "big data," established over the preceding phases.

Analysing data using algorithms allows employers to identify recurring patterns, which can be used to classify and profile the workforce. In practice, this translates to automated or algorithmically supported decision-making regarding various aspects of human resource policy, including recruitment, dismissals, promotions, and disciplinary measures.[30]

As in previous phases, algorithms allow employers to monitor and observe new aspects of employees' lives that were not previously subject to scrutiny.[31] Increasingly, traditional monitoring tools such as CCTV cameras are being integrated with algorithmic systems enabling facial recognition[32] and beyond. Many employers also use devices to analyse employees' tone of voice to assess their mood.[33]

Algorithmic systems can be viewed as an extension of traditional forms of workplace monitoring, enriched with new elements designed to offer greater predictability and objectivity.[34] In reality, however, the lack of transparency in their operation and uncertainty regarding the data sets on which they were trained often result in algorithmic bias[35] and excessive intrusion into employees' privacy.

Devices and systems based on algorithms, while currently representing the most advanced forms of workplace monitoring - offering employers vast capabilities for oversight and management of the company and personnel - also pose risks that were previously unknown. This situation makes them the greatest challenge to date in the context of protecting employee privacy.

---

[30] E.g. this is the situation in Amazon’s distribution centre in Poznań (POZ1) in Poland. The automated system of worker performance reviews introduced in that workplace integrates employee evaluation with surveillance, gathering extensive personal data throughout the workday. Using algorithms, it assesses two key metrics: productivity and quality of work - see more in: Rozmysłowicz and Krzyżaniak, 2023, pp. 149-164.

[31] As this kind of spheres, Edwards, Martin and Henderson enumerate employees’ behaviours of interests, uncover emotional states and unshared personal preferences - Edwards, Martin and Henderson, 2018, p. 6.

[32] Dixon,et al., 2021, pp. 121-130.

[33] Moore, Akhtar and Upchurch, 2018, p. 37; Barański, 2021, p. 344; De Stefano, 2018, p. 11.

[34] Edwards, Martin and Henderson even equate algorithms to parasites – see: Edwards, Martin and Henderson, 2018, p. 7.

[35] Algorithmic bias can be defined as the tendency for algorithms to produce outputs that lead to a disadvantage for certain groups, such as women, ethnic minorities, or people with a disability, which is caused by biased or poor-quality data used for developing it – see: European Union Agency for Fundamental Rights, 2022, p. 17-19.

1.2. Employee Monitoring Before the "Analogue World"

The aforementioned model of employee monitoring development, composed of five stages, accurately reflects the dynamics of the evolution of this phenomenon. However, it does not account for the perspective of pre-industrial societies and pre-Taylorist management models, which are crucial for a comprehensive understanding of the history of workplace monitoring.

At this point, it is essential to consider the system of labour division and surveillance existing during the Middle Kingdom of Ancient Egypt. It is commonly believed that the labour performed in Ancient Egypt, and its remarkable achievements, were solely the result of the slavish treatment of workers and their complete subjugation to the divine authority of the pharaoh. However, as Kadish notes:

"Work and workers needed to be organized so as to achieve a desired level of production and delivery of goods and services. While laborers of all sorts were subject to a certain amount of violent coercion, that is not a sufficient explanation of the general successful discipline of labor, nor is the likely correct notion that workers obliged to perform corv´ee labor on major royal projects, such as pyramid-building, were, at least, in part, motivated by religious devotion (i.e., to the monarchy)."[36]

Certainly, coercion and religious subjugation played significant roles in shaping labour relations at the time. However, they were not the only factors influencing them. Analysing the methods and discipline of work in Ancient Egypt leads to the conclusion that the primary factor contributing to their extraordinary development and the creation of enduring legacies was the appropriate organisation of labour, of which surveillance was a key element. Moreover, at a very general level, we can observe some similarities between the organisation and surveillance of work in the Middle Kingdom and modern workplace monitoring practices.

As Ezzamel points out, rosters and name lists with workers' names were widely used during the Middle Kingdom. Some of these served as attendance lists, while others divided workers into groups and assigned them to specific tasks.[37] Already then, the division of labour and the establishment of concrete work goals were of great significance. It is also noteworthy that a characteristic feature of labour organisation in Ancient Egypt was the reporting of productivity,

[36] Kadish, 1996, p. 439.
[37] Ezzamel, 2004, pp. 507-509.

work in progress, and completed tasks. Reports often took the form of letters and accounts.[38] Individuals who were unwilling or failed to perform their duties properly faced sanctions, often of a criminal law nature, such as imprisonment in the Great Prison of Thebes.[39] Moreover, a policy of differentiated wages was also applied, which emphasised the difference in skills, achievements, and social status. One could argue that the wage level reflected the value of a particular individual within Egyptian society.[40]

Examining the history of labour organisation in Ancient Egypt, it is difficult not to draw parallels, at least at a general level, between some of the practices of that era and modern workplace organisation and employee monitoring.[41] Attendance checks, task observation by supervisors (then humans, nowadays increasingly robots), setting standards and detailed divisions of labour, monitoring work quality, and rewarding or disciplining workers—all these elements, albeit in different forms and with varying intensity, are visible in both contemporary and ancient systems of labour organisation and surveillance.

However, labour surveillance in Ancient Egypt was characterised by a certain distinctive feature that was later changed under the influence of industrial development, the explanation of which will allow us to better comprehend the present system of organisation and monitoring in the workplace. It concerns the concept of time, specifically the relationship between a task and the time needed to complete it. In the Middle Kingdom, this relationship was understood entirely differently than in the pivotal era of industrial capitalism. Egyptian society of that time was unfamiliar with the concept of "timed labour", as work was performed within a "task orientation" system - focused on completing a specific goal, often disregarding the time required.[42] Goals were either physical, e.g. completion of the building, or time-based – never mixed.[43] The fusion of these two spheres only occurred in the later era of the first industrial revolution (early 19th century) with the emergence of a new labour discipline in which the relationship between work and time became an indicator subject to constant evaluation.[44][45]

[38] Ezzamel, 2004, pp. 515-518.
[39] Ezzamel, 2004, pp. 514-515.
[40] Ezzamel, 2004, p. 531.
[41] Sewell, 2021, pp. 12-13.
[42] Thompson, 1967, pp. 60-61.
[43] Ezzamel, 2004, p. 531.
[44] Ezzamel, 2004, p. 531; Clark, 1994, p. 128; see also: Hoskin and Macve, 1986, pp. 105-136.
[45] Interestingly, the distinction between time-based pay and task-based work was still present in the 18th century. As described by Carmona, Ezzamel, and Gutierrez, the 18th-century Royal Tobacco Factory in Spain operated in such a way that cigar operators, who required a high level of skill, were paid on a piece-rate basis, which was intended to positively impact product quality, whereas snuff operators, mostly unskilled workers, were paid weekly – see: Carmona, Ezzamel, and Gutierrez, 1997, p. 417.

Surveillance was also a significant aspect of medieval times; however, it was understood in a manner characteristic of pre-modern communal societies, which primarily revolved around the community.[46] Unlike in modern and especially postmodern times, the individual and its privacy did not hold as much importance in the Middle Ages.[47]

Surveillance encompassed almost all spheres of life and was primarily focused on the lower social classes. This stemmed from the hierarchical social relations prevailing in the Middle Ages and the fear among the ruling elites of a popular uprising against them.

A crucial role in maintaining the social order of the time was played by labour surveillance, exemplified by late medieval England. As Chatziathanasiou points out, supervision over the workforce was strongly promoted in labour legislation of the time, especially in the period following the plague epidemic. For instance, the Statute of 1388 *de facto* introduced surveillance over workers' and vagrants' places of residence, as it prohibited them from leaving their place of residence to take up work or change their place of living unless they possessed an appropriate letter approved by royal and local authorities. The statute also led to the creation of written registers for storing workers' data. [48]

Another labour-related institution based on worker supervision, or rather the master's control over the servant, was compulsory service.[49] According to the Statute of Labourers from 1351:

"Every man and woman of our kingdom of England, of whatever condition, whether bond or free, who is able bodied and below the age of sixty years, not living from trade nor carrying on a fixed craft, nor having of his own the means of living, or land of his own with regard to the cultivation of which he might occupy himself, and not serving another, if he, considering his station, be sought after to serve in a suitable service, he shall be bound to serve him who has seen fit so to seek after him (…)."[50]

Another legal act characteristic of that period, fitting within the framework of medieval labour surveillance, was an order issued in 1492 by the Coventry Leet, which stated:

---

[46] Chatziathanasiou, 2024, p. 32.
[47] In 1890, Samuel Warren and Louis Brandeis indicated that the "right to privacy" should be understood as the right to control access to information about oneself. This interpretation of the right to privacy, focusing primarily on the individual, has shaped the modern debate on privacy – see: Longfellow, 2006, p. 315; Warren and Brandeis, 1890, pp. 193-220.
[48] Chatziathanasiou, 2024, pp. 45-46.
[49] Bennett, 2010, p. 7-51.
[50] The Statute of Laborers from 1351.

"Also that no singlewomen, being in good health and mighty in body to labour, within the age of 50 years, take or keep from henceforth houses or chambers by themselves, nor that they take any chamber with any other persons, but that they go into service until they be married".[51]

This legal act has been subject to numerous interpretations. Some suggest it aimed to combat prostitution, others see it as an expression of fears regarding self-sufficient women, while yet others argue that it served to domesticate women.[52] Regardless of these interpretations, one thing is certain - it contributed to positioning women as a source of cheap labour and reinforced surveillance over them.

However, it must be noted that it was not only women who were subjected to "domestication," or rather, of finding a permanent place for them. Similar measures were taken against unruly journeymen, who, by being placed under one roof, became easier for masters to control in terms of their behaviour and work. This also strengthened the hierarchical socio-economic model.[53]

The world of labour in the Middle Ages was approached with great suspicion, partly because workers, lower-ranking clergy, and artisans often joined forces in political protests and strikes against the ruling elites.[54] Such actions were met with a definite response from the authorities in the form of the Royal Statute of 1495, which established monetary and corporal punishment for craftsmen and labourers who made or caused an assembly against those appointed to control and supervise their work.[55]

Analysing labour surveillance in the Middle Ages, it is evident that it was entirely different from the Taylorist understanding of the term. Its primary aim was to preserve the existing social system, which was built upon strong pillars of hierarchy and master-servant relations, rather than to oversee the tasks performed by workers for the purpose of increasing production efficiency. However, it is worth considering whether modern workplace monitoring does not also have certain features that serve to perpetuate certain social relations?

Another characteristic example of workplace surveillance, somewhat diverging from the principles of Frederick W. Taylor's later dominant "scientific management," is the "Silent Monitor." This tool for employee monitoring was designed and implemented by Robert Owen in his cotton mill in New Lanark around 1800. It was a rectangular block of wood, resembling

[51] Harris, 1907, p. 545.
[52] Bennett, 2010, p. 45.
[53] Chatziathanasiou, 2024, p. 47.
[54] Chatziathanasiou, 2024, p. 49; Robertson, 2006, p. 56.
[55] Chatziathanasiou, 2024, p. 52.

part of a post, installed at each workstation. Each side of the block was painted a different colour. The colour displayed on the front of the block represented the worker's performance from the previous day. White indicated "super excellence," yellow signified "moderate goodness," blue denoted "a neutral state of morals," while black was dreaded by workers as it indicated "excessive naughtiness." [56]

Workers' performance was recorded by Owen in a "book of character". As Sewell notes, maintaining such a record enabled a broader assessment of the employee's moral condition.[57] Moreover, an important role in this scrutiny mechanism was played by a sense of shame resulting from a "public" or at least visible to colleagues, negative evaluation. Public shaming contributed to improving the deficiencies apparent in the conduct of some workers. [58]

The feature distinguishing Owen's four-sided wooden block, known as the "Silent Monitor," from later forms of workplace monitoring is that it was never intended to measure employees' productivity or output. Instead, it served to assess the temperament or behaviour of workers—or, in a broader sense, their morality.[59] As Donkin says, "if you kept your nose clean, the least you could expect was a blue."[60]

Analysing the mechanism of the "Silent Monitor" and the intentions behind its use, it is difficult not to see parallels with modern forms of employee monitoring, particularly in jobs where interaction with customers plays a significant role. These include workplaces such as call centres[61] or digital platform jobs. In both cases, the subject of evaluation becomes the employee's behaviour, particularly its qualitative aspects.[62] The behaviours of call centre operators are monitored by recording their conversations with customers and assessed by specially designated bodies. In addition to the substantive content of the conversations, the tone of voice used by workers is often scrutinised to see whether it is sufficiently polite.[63][64] Moreover, both call centre and platform workers are subject to "bottom-up" evaluations by customers. This process bears a strong resemblance to the mechanism of Owen's "Silent Monitor."

---

[56] Donkin, 2010, p. 94.
[57] Sewell, 2021, p. 14.
[58] Sewell, 2021, p. 14.
[59] Donkin, 2010 p. 94.
[60] Donkin, 2010 p. 94.
[61] Donkin, 2010 p. 94.
[62] Bronowicka et al., 2020, p. 15.
[63] Bronowicka et al., 2020, p. 22.
[64] In addition, new, technologically advanced forms of workplace monitoring are causing this type of monitoring to become more severe for employees. As Molè notes "a call centre employee will be obliged to keep a kinder voice on a steady basis, since the employer will not check occasionally but constantly through a sensor directed at the employee's tone of voice." – see: Molè, 2022, p. 90.

In fact, the "book of character" can be likened to reports or files detailing the assessment of individual call centre operators compiled by their supervisors. Similarly, the "star ratings" and average score of a worker visible to every user of apps for ordering rides or food strongly resemble the colours on the sides of the "Silent Monitor." In this context, the aforementioned shame mechanism also plays an important role. Just as in Owen's cotton mill, it is intended to motivate workers to improve their behaviour.[65]

1.3. Taylorism as a Cornerstone of Modern Workplace Monitoring

Examining the history of workplace monitoring, we can identify a pivotal moment that significantly shifted the discourse on this subject and became the cornerstone of many contemporary forms of employee monitoring. This cornerstone was the emergence of the factory work system and, particularly, the creation of scientific management principles by F. W. Taylor. Therefore, in order to properly understand the contemporary direction of workplace monitoring, it is essential to consider what had the greatest formative effect on it. Accordingly, this section of the thesis will examine Taylorian management theory with its implications for contemporary forms of workplace monitoring.

Adam Smith, in "An Inquiry into the Nature and Causes of the Wealth of Nations," argued that the key factor influencing a nation's prosperity was the efficiency and scale of industrial production. He claimed that the greater and faster industrial progress is, the more prosperous society becomes. However, for industrial development to continue, changes in the production system were necessary. According to Smith, the crucial change underpinning the new production system was the division of labour.[66]

The division of labour was based on the premise that traditional tasks performed by workers were overly complex, requiring time and specialised knowledge or skills to complete. By breaking down these tasks into simpler activities, they could be performed quickly and without the need for specialised expertise.[67] Goods that previously required skilled craftsmen could now be produced by groups of unskilled workers using tools and machinery designed

[65] It should also be mentioned that the overall rating on the application may affect the price paid to the platform worker – see: Mirosławski, 2023a, p. 5.
[66] Smith, 1776(1976), p. 17-28.
[67] Smith illustrates this with the example of pin production – "one man draws out the wire, another straights it, a third cuts it, a fourth points it, a fifth grinds it at the top for receiving the head." – see: Smith, 1776(1976), p. 18.

specifically for these simpler tasks. Consequently, production could increase without a proportional rise in labour costs.[68]

However, as Smith noted, the new division of labour would result in workers becoming:

"…as stupid and ignorant as it is possible for a human creature to become. The torpor of his mind renders him not only incapable of relishing or bearing a part in any rational conversation, but of conceiving any generous, noble, or tender sentiment, and consequently of forming any just judgment concerning many even of the ordinary duties of private life."[69]

Smith recognised that progress has a price, which is worth paying, and that the evoked situation is an inevitable side effect of any civilised society. Nevertheless, he points out that every responsible state should be aware of this and develop a public education system to counterbalance the stultifying effects of the division of labour.[70]

Less than a century later, Karl Marx also warned of the dangers inherent in labour division and the large-scale expansion of factory work. In the first volume of "Capital", he argued that the division of labour under the capitalist form of large-scale industry transforms the worker into a living appendage of the machine. He also drew attention to the meaning of women's, children's and unskilled men's labour as a new foundation for the division of labour.[71] What Smith had written earlier came to fruition.

Smith's division of labour played an important role in Frederic Winslow Taylor's theory of scientific management. Taylor agreed that breaking down the tasks performed by the workers into smaller, easily measurable, and monitorable activities would contribute to more efficient production. However, he argued that the true potential to overcome inefficiencies arising from the previous management models lay in combining the appropriate division of labour with new scientific management methods. [72] He believed that knowledge, rather than mere muscle power, is the primary source of productivity.[73]

Taylor developed the principles of scientific management, inspired by experiments he conducted at the Bethlehem Steel Company and several other factories.[74] The core tenets of his theory covered the setting of work standards to establish a target rate of productivity higher

---

[68] Crawford, 2021, p. 59.
[69] Smith, 1776(1976), p. 1040.
[70] Smith, 1776(1976), pp. 1042-1045.
[71] Marx, 1867(1992), pp. 614-615.
[72] Taylor, 1911(1919), p. 7.
[73] Kanigel, 2000, p. 9.
[74] Hatch and Cunliffe, 2013, p. 25.

than previous averages, and the standardisation of working methods to ensure that workers could achieve specific goals, including the creation of work instructions, setting the precise sequence of shifts, and the development of material specification charts and stock control systems.[75] The basis for all this was a thorough scientific analysis and measurement of each of the tasks performed by the workers. This approach stemmed from Taylor's conviction that:

"The natural laziness of men is serious, but by far the greatest evil from which both workmen and employers are suffering is the "systematic soldiering" which is almost universal under all of the ordinary schemes of management and which results from a careful study on the part of the workmen of what will promote their best interests."[76]

He further claimed that in a large workplace, it was rare to find a competent worker who would not devote considerable effort to determining how slowly he could work while convincing his employer that his pace was adequate.[77]

Taylorist management thought rejects the notion that workers could naturally strive to perform their duties adequately. Instead, it relies on the opposite logic of measurement and control. Social relations in the workplace must be replaced by a system in which the worker's body is separated from his or her mind, and the expertise and supervisory authority are exclusively held by managers.[78]

Herbert Stimpson - one of the "efficiency engineers" of the time, described his perspective on workers to a congressional committee investigating the effects of scientific management, by stating that he perceived them "as a little portable power plant… a mighty delicate and complicated machine… The physical body of the man is constructed on the same mechanical principles as the machine is, except that it is very much higher developed." Stimpson's view emphasised that workers' efficiency and limitations could be measured in the same way as mechanical machines.[79] A very similar approach to the person of the worker was expressed by one of Taylor's most famous apologists, who put his ideas into full-scale practice - Henry Ford. In his description of factory life, Ford indicated that:

[75] Hatch and Cunliffe, 2013, p. 25.
[76] Taylor, 1911(1919), pp. 20-21.
[77] Taylor, 1911(1919), pp. 21.
[78] Brown, Lauder and Ashton, 2011, p. 69.
[79] Kanigel, 2000, p. 460.

"A business is men and machines united in the production of a commodity, and both the men and the machines need repairs and replacements…. Machinery wears out and needs to be restored. Men grow uppish, lazy, or careless."[80]

Analysing the theory of scientific management, we see that its key feature is the continuous monitoring of workers through the measurement of their efficiency and the time required to complete assigned tasks. Workers need to be monitored as this theory to be applied, needs concrete and real data. Furthermore, the monitoring of workers does not need to meet any special requirements or account for workers' dignity and privacy since, according to the logic of Taylorism, they are nothing more than a more expensive version of a machine whose productivity should be constantly measured and, where possible, improved. Tools such as clocks, meters and scales were used to measure performance.

From a modern perspective, Taylor's system may seem brutal, disregarding the humanity of workers and appearing distinct from contemporary experiences. However, this perception is misleading. Taylor's principles have not disappeared but rather evolved to adapt to new conditions. To this day, many employers and companies continue to draw inspiration from Taylor and apply elements of his scientific management principles. It is not without reason that the 21st century is called the age of "Digital Taylorism."

Digital Taylorism, like its traditional counterpart, is based on the separation of the mind and body. Just as the knowledge of craftsmen was once appropriated and transformed into an organised production line in Ford's factories, today, the knowledge of white-collar workers is being captured, digitised, and converted into patterns, procedures, and scripts that can be applied on a global scale. Digital Taylorism no longer needs a single factory to house the entire workforce and human supervisors responsible for measuring and recording workers' performance. Technological advancements now enable the collection of productivity data at any time, regardless of an employee's location.[81] New forms of employee monitoring are serving this purpose, such as the surveillance of electronic devices used for work, company e-mail accounts, telephone conversations, GPS tracking, surveillance via so-called "wearable work instruments", and many other forms of monitoring that make it possible to obtain information about a worker's activities, work pace and breaks, his or her location, etc.[82]

[80] Rothschild, 1973, p. 34.
[81] Brown, Lauder and Ashton, 2011, p. 72.
[82] De Stefano, 2019, p. 9-10; Barański and Giermak, 2017, p. 197-208; Barański, 2021, p. 344.

However, in recent years, employee monitoring has expanded to include new categories of data. Increasingly, employers value information not strictly related to the work performed but concerning the personal sphere - workers' character, emotions, interests, and mental state. This shift is a response to changes in the labour market. On one hand, many modern jobs demand significant flexibility from employees; on the other hand, workers are more and more reluctant to spend their whole life in one job. This has resulted in a paradigm shift.

For employers, workers' specific skills have become less critical than their personal traits and whether these align with the roles they are expected to fulfil within an organisation.[83] As Suresh Gupta from Capco Consulting outlined, “we can’t teach people to be more flexible, to be more empathetic... but we can teach them the basics of banking.”[84]

With this shift in focus - from employees’ skills to their personalities - a new wave of employee monitoring tools has emerged to gather such data. Traditional tools like clocks, scales and meters, once used to measure workers’ productivity, have been replaced by psychological tests, team-building games, brain-computer interfaces, social media monitoring, emotion-detection devices and other applications and tools designed for so-called “self-tracking” purposes.[85]

2. Extra-legal View on Workplace Monitoring

Although this thesis aims to analyse and compare workplace monitoring as an institution regulated by the labour laws of the Visegrad countries, the issue is so broad and researched in other academic fields that it would be erroneous to overlook the extra-legal meaning of workplace monitoring, especially as it has a significant impact on the development of the law. Particular attention should be paid here to how occupational sociology and psychology approach this issue.

This section will focus on how these two disciplines approach the concept of workplace monitoring. An extremely important and unfortunately often neglected element in research is also the inclusion of a colloquial perspective - that is, how the issue of workplace monitoring

[83] Olšovská and Švec indicate that a new nature of work positions in Industry 4.0 requires employees who are more psychologically resilient to work stress, have certain cognitive, psychomotor and behavioural skills and personality features that help them fulfil their work tasks and at the same time prevent possible damage to the manufacturing means and/or reduce complaints from customers, which represent direct employer costs – see: Olšovská and Švec, 2017, pp. 23-24.
[84] Brown, Lauder and Ashton, 2011, p. 79.
[85] See: McGill, 1990, pp. 227-232; Trzyniec, 2017, pp. 23-25; Lukács, 2021; Swan, 2013, p. 85; Ienca and Malgieri, 2022, pp. 2-4.

is viewed by the public and those directly affected by it, which in the context of this thesis means primarily employees.

2.1. Sociological Perspective

The sociological perspective focuses primarily on power relations, social hierarchy, politics, and the methods of resistance used by workers. Certainly, figures such as Karl Marx[86] and his analysis of the relations occurring within capitalist production, or Max Weber with his concept of bureaucracy[87], have had a strong influence on this view of workplace monitoring. They can be considered to have laid the foundations for the later sociological analysis of surveillance in the workplace. However, Michel Foucault must be considered the most influential author in this context. Foucault devoted one of his most recognisable works - "Discipline & Punish - The Birth of the Prison" - to the issue of surveillance. In this work, inspired by the panopticon project created by Jeremy Bentham, he presents his own conception of panopticism. Foucault looks at the panopticon as an internalised surveillance that causes workers to control their own behaviour even when no one is looking, which in fact resembles training and creates a culture of fear.[88]

The conceptual framework set out by Foucault has, in a sense, shaped contemporary sociological discourse on labour monitoring and continues to resonate in it today. Graham Sewell and James Barker base their understanding of surveillance on the definition "the few watching the many" and apply the broader concept of disciplinary power, which enables them to portray the problem of management control in terms of how superiors monitor the actions of

---

[86] For Marx, surveillance is an integral part of production that contributes to alienation and the exercise of disciplinary power over the worker - "All directly social or communal labour on a large scale requires, to a greater or lesser degree, a directing authority, in order to secure the harmonious co-operation of the activities of individuals, and to perform the general functions that have their origin in the motion of the total productive organism, as distinguished from the motion of its separate organs. A single violin player is his own conductor : an orchestra requires a separate one. The work of directing, superintending and adjusting becomes one of the functions of capital, from the moment that the labour under capital's control becomes co-operative. As a specific function of capital, the directing function acquires its own special characteristics." – See: Marx, 1867(1992), pp. 448 – 449.

[87] Surveillance is one of the constant elements of bureaucratisation and rationalisation, which for Weber is the inevitable outcome of human development. However, for Weber, the future of the human species does not hold any positives, and resembles a steel cage rather than the Garden of Eden. – See: Coser, L. A., 1977, pp. 230-233.

[88] "Our society is one not of spectacle, but of surveillance; under the surface of images, one invests bodies in depth; behind the great abstraction of exchange, there continues the meticulous, concrete training of useful forcesl the circuits of communication are the supports of an accumulation and a centralization of knowledge; the play of signs defines the anchorages of power; it is not that the- beautiful totality of the individual is amputated, repressed, altered by our social order, it is rather that the individual is carefully fabricated in it, according to a whole technique of forces and bodies. We are much less Greeks than we believe. We are neither in the amphitheatre, nor on the stage, but in the panoptic machine, invested by its effects of power, which we bring to ourselves since we are part of its mechanism." – See: Foucault, M., 1975, p. 217.

subordinates.[89] In their research, they also present two, on the one hand coherent but on the other hand, competing perspectives on workplace (organisational) surveillance: the "coercive" perspective and the "caring" perspective.

The coercion perspective aligns with the radical tradition of organisational studies and perceives monitoring as a tool of managerial domination over the workforce. It highlights two key aspects: 1. the actions of managers who strive to maintain constant oversight of employees to ensure maximum productivity, and 2. the behaviour of employees to evade monitoring and reduce dependence on managerial control.[90] Within this perspective, managers and overseers serve as gatekeepers of the capitalist class owning the means of production, whose interests are in conflict with those of the employees. As we can see, the coercion perspective is associated with Foucault's concept of panopticon because it focuses on power imbalance and emphasises the disciplinary and hierarchical effects of workplace monitoring.

In turn, the care perspective is grounded in the liberal intellectual tradition. From John Rawls' theory of justice and especially his analysis of the structure of society and social institutions, we can derive the conclusion that surveillance of society, including employees, can be justified if it serves the greater good and benefits all members of society, e.g. by enabling the detection of behaviours contrary to those demonstrated by the majority of society.[91] In that sense, workplace monitoring becomes a protective mechanism from the selfish or destructive actions of some employees.[92] The care perspective also reflects fundamental elements of the neoliberal economic theory, especially the concept of mutual obligation and "moral hazard". In this context, the main purpose of monitoring is to compel the employee to fulfil his or her obligations under the contract with the employer and to counteract the so-called 'free ride' by checking whether the employee performs his or her work with due diligence and puts in sufficient effort.[93] It must therefore be considered that, in complete contrast to the radical interpretation, workplace monitoring in the liberal sense is a legitimate and neutral tool arising from a bilaterally binding employment relationship to serve its parties equally.

It should be noted, however, that contemporary occupational sociologists do not limit themselves to analysing and fitting into one of the above concepts. Sewell and Barker challenge the polarisation between the radical and liberal approaches. They claim that these two theories, most of the time, function in parallel without contradiction because workplace monitoring

---

[89] Sewell, G., Barker, J. R., 2006, p. 935.
[90] Sewell, G., Barker, J. R., 2006, p. 938.
[91] Rawls, J., 1971(1999), pp. 3-7, 54-60.
[92] Rushing, W. A., 1966, pp. 424, 432-437.
[93] Sewell, G., Barker, J. R., 2006, p. 940.

embodies elements of both coercion and care. In many situations, we may feel the invasive and limiting power of monitoring, but there are also occasions when it guards us against the hostile and antisocial behaviours of others.[94] Therefore, they propose an ironic approach, which focuses on the paradoxes inherent in surveillance.[95] The paradoxes present both sides of monitoring – coercive and caring.

Another author who goes beyond the classical theories on monitoring is Philip E. Agre. In his work entitled "Surveillance and Capture - Two Models of Privacy", he presents two models of privacy - the surveillance model and the capture model.

The surveillance model is the traditional model most commonly found in the monitoring and privacy literature and fits within the framework of the previously mentioned concepts. However, it should be pointed out that it is much closer to coercion theory than to caring theory. The surveillance model is perceived as a cultural phenomenon. It is rooted in visual metaphors, drawing from Orwell's 1984 and Foucault's panopticism. It is non-intrusive but omnipresent and assumes that individuals are under constant supervision of a central authority, which shapes the manner in which they behave and leads to self-discipline. The information is centrally collected and stored without direct involvement of the object of surveillance. This model points out hierarchical power structures and is typically associated with state control; however, it is also present in workplaces.[96]

The other model derives from the practices of computer system design and relies on structuring individuals' activities to facilitate automatic data collection. It uses linguistic metaphors rather than visual ones to bring human behaviour closer to a machine-readable format. Unlike the surveillance model, the capture model works through active intervention, applying tracking mechanisms to everyday systems such as digital transactions, workplace monitoring and online environment. Instead of political motives, it is driven by institutional and technical practices.[97] The capture model is gaining importance, especially in the context of modern forms of workplace monitoring, which are closely linked to technologies such as wearables and biometric systems.

[94] Sewell, G., Barker, J. R., 2006, p. 942.
[95] More on the ironic approach See: Sewell, G., Barker, J. R., 2006, pp. 934-961.
[96] Agre, P. E., 1994, pp. 743-744.
[97] Agre, P. E., 1994, pp. 744, 746-757.

2.2. Psychological Perspective

The psychological perspective, as opposed to the sociological one, does not focus on theoretical concepts and political questions related to workplace monitoring, but rather resolves how monitoring is used and what effects it has on the mental health of employees.

This approach is presented in the work of Paul Glavin, Alex Bierman and Scott Schieman titled "Private Eyes, They See Your Every Move: Workplace Surveillance and Worker Well-Being", in which the authors analyse workplace monitoring through the lens of workers' psychological well-being. The research highlights that workplace surveillance is closely related to the concept of stress proliferation, which means that an initial stressor in the workplace reinforces other negative sensations, leading to cumulative stress over time.[98] According to the authors, employees who experience intense surveillance, which in that case is the initial stressor, may report increased levels of three secondary work stressors: job pressure, struggle to maintain autonomy and privacy violations.[99]

The high objectivity and neutrality of the psychological perspective imply that the results of the research on the impact of monitoring on the mental state of employees should provide a strong basis for legislative work on new national models of workplace monitoring.

2.3. Colloquial Perspective

Given how controversial the issue of workplace monitoring is in the public debate, and that it does not only concern a narrow group of people, but encompasses most members of society who are employees, it is also important to look at how it is being understood from a non-expert, in other words, a colloquial perspective.

When considering the colloquial meaning of workplace monitoring, it is important to draw on sources available to the general public. Traditionally, such sources have included dictionaries. In most dictionaries, we will not find the term 'workplace monitoring', but rather phrases such as 'monitoring' or 'surveillance'. The PWN dictionary of the Polish language (Słownik języka polskiego PWN) states that monitoring is "constant observation and control of some process or phenomenon" or "constant supervision over some protected object".[100] In turn,

[98] Galvin, P., Bierman, A., Schieman, S., 2024, p. 331.
[99] Galvin, P., Bierman, A., Schieman, S., 2024, pp. 330-332.
[100] Phrase "monitoring" in online version of Polish language dictionary PWN – See: https://sjp.pwn.pl/szukaj/monitoring.html (Accessed: 23 February 2025).

the term ‘surveillance’, which in the legal sciences is used interchangeably with the expression ‘monitoring’ in the context of the workplace, means “controlling or watching over someone or something”, as well as “an organisational unit of an institution that supervises someone or something”.[101] Another popular online dictionary, the Cambridge Dictionary, states that the verb ‘to monitor’ means “to watch and check something carefully over a period of time.”[102] This dictionary also provides a definition of ‘surveillance’ as “the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected”.[103]

However, given the current state of development of the modern information society, much of the importance in shaping the colloquial meaning of ‘workplace monitoring’ should be attributed to online sources such as the online encyclopaedia Wikipedia and, above all, AI-based language models such as the American ChatGPT and the Chinese DeepSeek, which are used by many as the first source of information. Of course, these sources are more precise in defining the concept than the dictionaries referred to. In Wikipedia, we can find the keyword “employee monitoring,” which is defined as:

“The (often automated) surveillance of workers' activity. Organisations engage in employee monitoring for different reasons, such as to track performance, to avoid legal liability, to protect trade secrets, and to address other security concerns. This practice may impact employee satisfaction due to its impact on the employee's privacy. Among organizations, the extent and methods of employee monitoring differ.”[104]

In turn, ChatGPT and DeepSeek asked to give the colloquial meaning of workplace monitoring, answered in a very similar manner, pointing out objectives, exemplary forms of monitoring and making reference to the well-known text of culture – George Orwell’s “1984”. The definition prepared by ChatGPT reads – “Colloquially, workplace monitoring refers to how employers keep an eye on employees while they're on the job. This can include tracking emails, internet usage, phone calls, video surveillance, or even monitoring keystrokes and location. It’s often

[101] Phrase “nadzór” in online version of Polish language dictionary PWN – See: https://sjp.pwn.pl/szukaj/nadzór%20.html (Accessed: 23 February 2025).
[102] Phrase “to monitor” in online Cambridge Dictionary – See: https://dictionary.cambridge.org/dictionary/english/monitor?q=monitoring (Accessed: 23 February 2025).
[103] Phrase “surveillance” in online Cambridge Dictionary – See: https://dictionary.cambridge.org/dictionary/english/surveillance (Accessed: 23 February 2025).
[104] Phrase “Employee monitoring” in Wikipedia – See: https://en.wikipedia.org/wiki/Employee_monitoring (Accessed 23 February 2025).

seen as a way for companies to boost productivity and security, but employees might see it as "spying on workers" or "big brother watching."[105]

It is also worth noting the definition proposed by the British Trade Union Congress, which states that “workplace surveillance is any form of employee monitoring undertaken by an employer.” This definition might appear oversimplified and incomplete; however, in fact, it expresses the essence of the definition of “monitoring” indicated by the ILO in the Code of Practice on the Protection of Workers’ Personal Data.[106]

Analysing all of the evoked definitions of “workplace monitoring”, we can draw one important conclusion. The colloquial perspective has a strong connection to the previously mentioned scientific perspectives, especially the sociological one. For instance, the “surveillance model” of privacy described by Agre relates extensively to the colloquial perspective.

However, in order to make the examination of the colloquial perspective on workplace monitoring complete, one more point needs to be considered, namely, the perception of workplace monitoring by employees themselves.

Bronowicka, Ibanova, Klicki, King, Kocher, Kubisa and Zielińska, for the purpose of their research “‘Game that you can’t win’? Workplace Surveillance in Germany and Poland”, conducted a series of interviews with Polish and German call centre employees about their experience with workplace monitoring. During the interviews, employees had a chance to express their feelings about monitoring. Interestingly, Polish and German employees expressed two different opinions on this issue.

Polish employees generally expressed neutral or positive attitudes towards workplace monitoring. They accepted monitoring as a normal part of their working environment and did not have a problem with it. Some even saw monitoring as something beneficial, enabling them to improve their performance and ensuring fairness in the workplace. They even claimed that monitoring in the form of the recording of phone calls is useful for resolving disputes with customers. However, there were also some employees who mentioned that they would prefer

[105] DeepSeek indicates that: “Workplace monitoring refers to the practice of employers keeping an eye on what employees are doing during work hours. This can include tracking computer usage, monitoring emails, recording phone calls, observing through cameras, or even using GPS to track location. The goal is usually to ensure productivity, protect company assets, and maintain security, but it can sometimes feel like "Big Brother is watching" to employees.”

[106] “The term ‘monitoring’ includes, but is not limited to, the use of devices such as computers, cameras, video equipment, sound devices, telephones and other communication equipment, various methods of establishing identity and location, or any other method of surveillance.” – See: ILO, 1997, point 3, par. 3.3.

more privacy, especially during difficult workdays and for whom video monitoring was unacceptable.[107]

In contrast, German call centre employees' impression of workplace surveillance was overwhelmingly negative. Some of them acknowledged that monitoring is necessary to ensure that "everyone is doing their job"; however, excessive surveillance is counterproductive and demotivating. Employees noted that they feel less productive and more stressed under strict monitoring, which can even lead them to change their workplace. There was also an issue of frustration with inflated performance targets, which were not taking into account the efforts of employees. Some call centre agents even compared the monitored workplace to a "prison" or "contact factory" and highlighted the feeling of dehumanisation.

3. Workplace Monitoring in Terms of International and European Regulations

The issue of monitoring in the workplace and, even broader, the issue of the right to privacy, which encompasses monitoring, has become an integral element of labour law over time. However, phenomena such as the dynamic development of technology in recent decades, its impact on worker privacy and the increasing pressure to globalise markets and the work process itself, have resulted in the demand for appropriate regulation to address and protect against the negative effects of these changes.[108] In this context, international and European regulations have played a huge role. On many occasions, such regulations have set new standards and provided a reference point for national legislators. Therefore, even if the focal point of the thesis is the comparison of national models of workplace monitoring, it is still desirable to briefly mention the provisions addressing this issue in the international dimension.

Considering the geopolitical position of the countries of the Visegrad Group, the main emphasis of this section will be primarily on European regulations, operating within the framework of the Council of Europe and the European Union, as they are of fundamental relevance to the national laws of Hungary, Poland, the Czech Republic and Slovakia. Naturally, the reference will also be made to the instruments prepared by the ILO, which, being soft law due to their lack of binding force, constitute a set of proposals that resonate with the doctrine rather than in actual legislation.

As the issue of workplace monitoring from a human rights perspective will be discussed in detail later in the thesis, it will only be addressed in a limited manner in this section.

[107] Bronowicka et al., 2020, pp. 23–24.
[108] Hendrickx, 2019a, p. 147.

3.1. European Regulations[109]

When approaching the issue of workplace monitoring from the perspective of European regulations, two legal orders must be taken into account – the first, set by the Council of Europe, and the second, operating within the European Union. The two legal orders permeate each other, and within them we can distinguish legal instruments of different significance in terms of their legal binding force and area of application, such as conventions, acts with the rank of treaty, regulations, as well as recommendations and opinions of working groups.[110]

The analysis should begin with European mechanisms for the protection of human rights. Within the Council of Europe, the legal instrument underpinning the protection of human rights is the European Convention on Human Rights, which has an international character. In turn, in the EU, such a basis is the Charter of Fundamental Rights of the European Union, which is of a supranational nature.[111]

The ECHR does not directly address the issue of privacy in employment, including monitoring, but guarantees in Article 8 the general right to respect for private and family life. The explicit articulation of this right in the Convention provided a new direction for national privacy laws in Member States.[112]

Paragraph 1 of Article 8 of the ECHR states that "Everyone has the right to respect for his private and family life, his home and his correspondence." However, the second paragraph of the article indicates the possibility of certain derogations, as it provides that "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[113]

The general concept of the right to privacy under Article 8 of the ECHR has gradually evolved, under the influence of the ECtHR jurisprudence, covering also the right to personal

[109] Based on this fragment, an article was prepared and published: Mirosławski, T. (2025) 'Workplace Monitoring in Europe: A Review of Regulatory Perspectives and Developments', *Polish Review of International and European Law*, 14(2), pp. 123-143.
[110] Otto, M. 2016, p. 115.
[111] Fabbrini, F., 2010, p. 9.
[112] Rustad, M. L., Paulsson, S. R., 2005, pp. 870 – 871.
[113] Article 8 of the European Convention on Human Rights.

data protection[114] and the right to privacy in the employment context.[115] In addition, over time, more and more cases concerning workplace monitoring and surveillance of employees in the context of alleged violations of Article 8 of the ECHR have started to be brought before the ECtHR.[116] This, in turn, led the Strassburg Tribunal to develop appropriate criteria to assess the proportionality of the interference with the right to privacy caused by surveillance measures in the workplace and acknowledge whether the monitoring was legal.[117] It should be noted that, in accordance with the Court's judgement, these criteria are addressed to the domestic authorities in the first instance.[118]

Similar to the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union[119] does not explicitly address the right to privacy in the context of employment. However, Article 7 of the Charter sets out the right to privacy in general terms, closely mirroring Article 8 of the ECHR. Indeed, it can be stated that Article 7 of the Charter "substantially reproduces" Article 8 of the ECHR.[120]

Article 7 of the Charter reads as follows: "Everyone has the right to respect for his or her private and family life, home and communications."[121] The only difference between this provision and Article 8 of the ECHR is the use of wording. EU legislator instead of "correspondence" used the word "communications" This move reflects a desire to give the Charter a timeless character, which takes into account technological changes.[122] However, the

[114] The Grand Chamber in the case *S. and Marper v. the United Kingdom* adjudicated that "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention." – See: ECtHR judgment in S. and Marper v. the United Kingdom from 4 December 2008 (Application nos. 30562/04 and 30566/04), 103.

[115] In the case *Niemietz v. Germany*, the Court stated that "(…) it would be too restrictive to limit the notion (of "private life") to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world." – See: ECtHR judgment in Niemietz v. Germany from 16 December 1992 (Application no. 13710/88), 29.

[116] See e.g.: Halford v. the United Kingdom; Copland v. the United Kingdom; Köpke v. Germany; Bărbulescu v. Romania; Antović and Mirković v. Montenegro; López Ribalda and Others v. Spain; Florindo de Almeida Vasconcelos Gramaxo v. Portugal.

[117] Barański, M., 2020, p. 31.

[118] The criteria were mentioned by the Court in the judgment of Grand Chmaber in Bărbulescu v. Romania – See: ECtHR judgement of the ECtHR in Bărbulescu v. Romania from 5 September 2017 (Application no. 61496/08), 121.

[119] Hereinafter: CFREU

[120] CJEU (Court of Justice of the European Union) judgment in Productores de Música de España (Promusicae) v. Telefónica de España SAU from 29 January 2008 (C-275/06), 64.

[121] Article 7 of the Charter of Fundamental Rights of the European Union (200/C 364/01).

[122] Explanations relating to the Charter of Fundamental Rights (2007/C 303/02), explanation on Article 7 - Respect for private and family life.

difference tends to be rather illusory since, as the ECtHR has pointed out on several occasions in its judgments, the term "correspondence" covers all forms of communications regardless of their content.[123] This includes all "traditional" paper and "modern" electronic communications. Furthermore, the catalogue of means of correspondence is also open to new communications, which will be developed in the future due to technological changes.[124] Additionally, it should be indicated that the "correspondence" is not limited only to private correspondence but also to professional correspondence.[125]

The similarity between Article 7 of the Charter and Article 8 of the Convention and their frequent simultaneous reference in the literature is not coincidental. According to Article 52 (3) of the CFREU, "the meaning and scope" of the right to privacy stated in the Charter should coincide with that indicated in the ECHR.[126] Therefore, when examining what the scope of the right to privacy guaranteed by the Charter is, and in particular what is the exact meaning of the "private life", it should be assumed that it is determined by the interpretation provided by the ECtHR. Thus, the concept of the "private life" under the Charter must be interpreted broadly, which means that it also applies to matters relating to the employment relationship, including the issue of employee privacy in the context of workplace monitoring.[127] Nevertheless, the requirement of a compatible interpretation of Article 7 of the Charter with Article 8 of the ECHR and jurisprudence of the ECtHR constitutes merely a "minimum standard clause",[128] which does not deter the EU from developing more complex protection of the rights guaranteed by the Charter.[129]

In addition, when analysing Article 7 of the Charter in the context of employee privacy, it is important to recall the interpretative concept outlined by Otto based on the so-called "integrated approach" developed by the case law of the ECtHR. Otto points out that the Charter of Fundamental Rights of the European Union, through its catalogue of social rights, offers a framework for strengthening the protection of employees' privacy. Using an integrated approach in order to link civil and social rights, the Charter allows for a broader interpretation

[123] ECtHR judgement in Michaud v. France from 6 March 2013 (Application no. 12323/11), 90.
[124] Lafferty, M., 2014, p. 530.
[125] ECtHR judgement in Niemietz v. Germany from 16 December 1992 (Application no. 13710/88), 32.
[126] The first sentence of Article 52 (3) of the Charter of Fundamental Rights of the European Union states that "the Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention."
[127] As Kokott and Sobotta points out "According to both Courts (*ECtHR and CJEU*), the term 'private life' must not be interpreted restrictively." – See: Kokott, J., and Sobotta, C., 2013, p. 223.
[128] Otto, M., 2016, p. 109.
[129] The second sentence of Article 52 (3) of the CFREU reads as follows: "This provision shall not prevent Union law providing more extensive protection."

of privacy at work. Rights such as the right to freely choose an occupation and to engage in work[130], protection against unjustified dismissal[131], and the right to fair and just working conditions[132] may contribute to the clarification of the legal boundaries of permissible employer interference in employees' private lives, e.g. by means of workplace monitoring.[133]

Considering the privacy of employees, this concept should definitely be appreciated as it encourages a more comprehensive understanding of privacy in employment within EU law.

Under the Charter of Fundamental Rights of the European Union, a distinctive element, especially with regard to the ECHR, is Article 8. It guarantees the protection of personal data. However, it should be noted that the above considerations regarding Article 7 of the Charter also apply to Article 8 of the Charter since, although the right to the protection of personal data is not explicitly mentioned in the ECHR, it is included within the scope of the right to respect for private life, as has already been pointed out above.

The provision states that:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.[134]

The main basis for the Article was Article 286 of the Treaty establishing the European Community and Directive 95/46/EC,[135] which was sort of a clarification of the principles and conditions of data processing in the context of Article 8.[136] Over time, Article 286 of the Treaty establishing the European Community was replaced by Article 16 of the Treaty on the Functioning of the European Union, and Article 39 of the Treaty on European Union; in turn, Directive 95/46/EC was succeeded by Regulation 2016/679 (GDPR). The GDPR, as a regulation, is of general application, binding in its entirety and directly applicable in all EU Member States, although, due to Article 23 and, above all, Article 88, as will be elaborated later

130 Article 15 of the CFREU.
131 Article 30 of the CFREU.
132 Article 31 of the CFREU.
133 Otto, M., 2016, p. 109.
134 Article 8 of the CFREU.
135 Lock, T., 2019, p. 2122.
136 Explanations relating to the Charter of Fundamental Rights (2007/C 303/02), explanation on Article 8 - Protection of Personal Data.

in the thesis, it does not provide a uniform regulation of the protection of personal data in employment.[137]

The explicit inclusion of the right to the protection of personal data in the Charter of Fundamental Rights of the European Union should be considered a breakthrough, as it has granted it the status of a fundamental right.[138]

In addition, it should be pointed out that the issue of protection of personal data in the context of employment has been addressed on several occasions by the Court of Justice of the European Union[139], which oversees the application of EU law and its compliance by the Member States.[140] The Court ruled on this in the Rechnungshof v. Österreichischer Rundfunk case[141], the Bodil Lindqvist case[142], and the V and European Data Protection Supervisor v. European Parliament case[143]. These cases concerned actions that had the potential to violate an employee's private life and right to protection of personal data, but in none of them was this action employee monitoring.

Gradually moving away from the sphere of human rights, although not entirely, it is worth mentioning the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (so-called Convention 108)[144], which was the first legally binding document regulating the processing of personal data of an international nature.[145] The aim of the Convention 108 was to bring greater uniformity to the protection of personal data systems expressed in national laws and protect human rights[146] owing to the risks imposed by the increasing cross-border flow of personal data and its automated processing.[147] Although this convention was adopted by the CoE, it was not limited solely to its Member States; rather, it might be said that it aspired to become a convention of global reach.[148][149]

---

137 Barański, 2022, p. 56.
138 Hendrickx, 2023, p. 2.
139 Hereinafter: CJEU
140 Lukács, 2021, pp. 99-100.
141 CJEU: Joint Cases C-465/00, C-138/01 and C-139/01, 2003.
142 CJEU: Case C-101/01, 2003.
143 CJEU: Case F-46/09, 2011.
144 The Convention was addopted on 28 January 1981.
145 Lukács, 2021, p. 61.
146 Preamble of Convention 108 from 28 January 1981. See also: Hendrickx, F., 2019, p. 150.
147 Preamble of Convention 108 from 28 January 1981.
148 Covention 108 has been signed and ratfied by some non-members of Council of Europe - See: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 (Accessed 2 May 2026). See also: Hendrickx, 2023, pp. 3-4.
149 However, the outcome of such efforts has been rather poor as by 1992 only ten countries had ratified the convention - Austria, Denmark, France, Germany, Ireland, Luxembourg, Norway, Spain, Sweden and the United Kingdom - while eight countries - Belgium, Cyprus, Greece, Iceland, Italy, Netherlands, Portugal and Turkey - had signed it without ratification. See: Cate, 1997, p. 35.

The Convention advocated for a fair and lawful model of the collection and automated processing of data and established a number of principles and requirements that such a model should incorporate. According to the Convention, such data should be retained solely for clearly defined and legitimate purposes, and not used in ways that are incompatible with those purposes. Data must be adequate, relevant, and not disproportionate to the objective for which it is retained, and it should be accurate and, where necessary, kept up to date. Furthermore, it must be stored in a form permitting the identification of data subjects only for as long as is necessary to achieve the purposes for which the data are held.[150]

In 2018, the Council of Europe decided to modernise the Convention. This decision was justified by the Council's desire "to better address emerging privacy challenges resulting from the increasing use of new information and communication technologies (ICT), the globalisation of processing operations and the ever greater flows of personal data, and, at the same time, to strengthen the Convention's evaluation and follow-up mechanism."[151] The modernised Convention is currently referred to as "Convention 108+" and its major difference from the previous version of the act is that it adds transparency as a core principle of data processing[152] and dispels doubts about the inclusion of manual data processing within the scope of the Convention by pointing out that "Data processing" starts from the collection of personal data and covers all operations performed on personal data, whether partially or totally automated. Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria, allowing the controller or any other person to search, combine or correlate the data related to a specific data subject."[153]

Additionally, it should be noted that after the adaptation of the original version of the Convention 108, many declarations, resolutions and recommendations were published by different bodies of the CoE, among which were documents of particular relevance to the employment field, including the question of workplace monitoring.

The first such document, which also illustrated the CoE's policy shift towards sectoral regulations, was the Recommendation of the Committee of Ministers to Member States on the

[150] Article 5 of Convention 108 form 28 January 1981.
[151] Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, 1.
[152] Article 5 (4) a of Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data adopted on 18 May 2018 (Convention 108+).
[153] Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, 21. See also: Article 2 (a) and (c) of Convention 108+.

Protection of Personal Data Used for Employment Purposes, adopted on 18 January 1989.[154] The important feature of the Recommendation No. (89) 2 is that its scope covers the collection and processing of personal data for employment purposes in the public and private sectors.[155] The framework of the Recommendation can be reduced to five core principles. Firstly, employers should, as a general rule, obtain personal data directly from the job applicant or the employee concerned. Secondly, such data should be collected and processed solely for employment-related purposes (i.e. recruitment of employees; fulfilment of the contract of employment; management, including discharge of obligations laid down by law or laid down in collective agreements; and planning and organisation of work)[156] corresponding to the specific type of employment in question. Thirdly, employees must be regularly informed about the nature of the data held, the purposes of its processing, the recipients to whom it is routinely disclosed, and the legal grounds for such disclosures. Fourthly, employees should have the right to access all personal data relating to them, as well as the right to request the rectification or deletion of any data processed in violation of the Recommendation's principles. Finally, personal data should be retained only for as long as is necessary to fulfil the purposes for which it was collected. In particular, this entails an obligation to erase applicants' data promptly once it becomes clear that they will not be offered the position for which they applied.[157] The recommendation also draws attention to particular categories of employee data,[158] the processing of which should be limited and in compliance with the appropriate safeguards indicated by national laws. In the absence of such safeguards, particular categories of employee data may be processed and stored with the express and informed consent of the employees.[159]

However, considering the changes taking place in employment, triggered by, among other things, the globalisation of work and services, the increasing use by employers of information and communication technologies that enable the collection of broader sets of employees' data, the need to review the Recommendation No. (89) 2 has arisen.[160] Following this demand, on 1

[154] Hereinafter: Recommendation No. (89) 2.
[155] Recommendation No. (89) 2, 1.1.
[156] Recommendation No. (89) 2, 1.3.
[157] Simitis, S., 1998, p. 362.
[158] Such data are personal data relating to racial origin, political opinions, religious or other beliefs, sexual life or criminal convictions, referred to in Article 6 of the Convention 108 – See: Recommendation No. (89) 2, 10.1.
[159] Recommendation No. (89) 2, 10.1.
[160] See: Explanatory Memorandum to Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, 2; Preamble of the Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment, 1 April 2015.

April 2015, the Committee of Ministers to Member States adopted the Recommendation CM/Rec(2015)5 on the processing of personal data in the context of employment.[161]

The Recommendation CM/Rec(2015)5 is significant in the context of workplace monitoring as it addresses the use of modern technologies in the workplace and contains explicit provisions on employee monitoring.

The document emphasises that employers should avoid unjustifiable or unreasonable interference with employees' private lives when using the Internet and electronic communications at work. This principle extends to all ICT[162] devices used by employees. According to the Recommendation, employers should be obliged to implement and regularly update a privacy policy detailing the purpose of processing, retention periods, and the handling of professional communications. Preventive measures, such as filtering or anonymous random checks, are preferred over intrusive monitoring of employees' web activity. Moreover, access to professional communications is permissible only if it is necessary for legitimate purposes, it should be conducted in the least intrusive manner possible and only after informing the concerned employee.[163]

Touching upon the broader monitoring systems, including video surveillance, the Recommendation expresses the prohibition of the use of information systems and technologies for the sole purpose of directly tracking employees' activity and behaviour. When such monitoring occurs indirectly, for instance, owing to the systems aimed at protecting production, health and safety, or organisational efficiency, it should comply with strict safeguards such as informing employees before introducing monitoring means; taking proper internal measures connected to the processing of personal data and notification of employees about this in advance; consulting employees' representatives and the national personal data supervisory authority.[164] Particularly sensitive areas of employees' personal life, such as, e.g. rest areas, toilets, showers, and cloakrooms, are strictly off-limits for video surveillance. Additionally, employees should be granted access to any recorded materials in the context of disputes or legal proceedings, and such recordings must be stored only for a limited period.[165]

The document also addresses location-tracking equipment, which may only be introduced when necessary for legitimate purposes, which do not include monitoring *per se*, and should never serve as a tool for continuous monitoring. Employers are required to uphold

[161] Hereinafter: Recommendation CM/Rec(2015)5.
[162] Information and Communication Technology.
[163] Recommendation CM/Rec(2015)5, 14.
[164] Recommendation CM/Rec(2015)5, 21.
[165] Recommendation CM/Rec(2015)5, 15.

proportionality and data minimisation principles and to adopt additional safeguards[166] to protect employees' privacy and personal data protection. In addition, while introducing appropriate internal procedures regulating the processing of data on employees' location, employers should, in advance, notify the concerned persons about such procedures.[167]

What emerges from the indicated provisions is a model for regulating workplace monitoring that limits monitoring to specific purposes and only allows it when other, less intrusive measures would not achieve such aims. Furthermore, it stipulates that once monitoring measures are applied in the workplace, they must be proportionate, transparent and respectful towards the fundamental rights of employees.

Another outstanding feature of this document is that, as the first CoE document touching upon employee data protection, it addresses the issue of monitoring employees and job applicants via social media platforms.[168]

The Recommendation CM/Rec(2015)5 clearly indicates that employers should not request or require that employees or job applicants grant access to information they share with others online, particularly on social networking platforms.[169] Moreover, the explanatory memorandum provides us with more information on this subject, stating that employers should abstain from using intermediaries, alternative names or pseudonyms to personal data about an employee or a work candidate without their consent.[170] Employers are also prohibited from requesting the login details of employees and candidates to access their social media accounts.[171]

In view of the above, the interpretation that emerges on the ground of the principle expressed in paragraph 5.3 of the Recommendation CM/Rec(2015)5 is that an employer should refrain from any attempt to access information shared by an employee online, to which his or her access has been restricted due to the employee's privacy settings. On the other hand, if the data shared online is available to the public, there is no obstacle to it becoming the object of processing by an employer. Naturally, such processing must comply with the principles of lawful personal data processing.[172]

Despite being more than a decade old, the Recommendation, to a certain extent, demonstrated remarkable foresight. Most of its principles concerning the processing of

[166] These safeguards are expressed in the principle 21 of the Recommendation CM/Rec(2015)5.
[167] Recommendation CM/Rec(2015)5, 16.
[168] Lukács, 2021, p. 97.
[169] Recommendation CM/Rec(2015)5, 5.3.
[170] Explanatory Memorandum to Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, par. 45.
[171] Explanatory Memorandum to Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, par. 46.
[172] Lukács, 2021, p. 97.

employees' personal data, particularly those addressing workplace monitoring and the processing of employees' data shared online, e.g. via social media, are gaining increasing relevance in light of current developments. In the labour market of Visegrad countries, it is increasingly becoming noticeable that employers are starting to use sophisticated techniques to monitor employees, including monitoring via social media.[173] Cases of employees being dismissed due to criticism of the employer or social media activity potentially undermining the employer's interest are gaining prominence. Štefko refers to such employees as "Facebook fired."[174] As an example of such cases, it is worth mentioning, for example, a case decided by the Hungarian Supreme Court, in which an employee was disciplinarily dismissed for posting insulting remarks and threats against his employer on Facebook and calling on employees to organise themselves. In that case, the Curia ruled in favour of the employer, that the dismissal was lawful.[175] Another similar case also originates from Hungary and concerns a prosecutor who was disciplinarily dismissed because he published posts of a political nature on his Facebook profile. However, in this case, the courts of both instances ruled that the dismissal was excessive. Instead of dismissal, the prosecutor's salary was reduced.[176] There have also been similar cases in other V4 countries, like Poland and the Czech Republic. In Poland, strong emotions were aroused by the case of a post office employee dismissed for comments on social media supporting the actions of the Russian army in the war against Ukraine,[177] and by the case of an employee of the Ministry of Foreign Affairs who was dismissed for posting comments on his private social media profile that referred to political and social reality. In the present case, the Warsaw Regional Court found the termination of the employment contract without notice to be unjustified[178]. In turn, in the Czech Republic, a high-profile case involving the issue of "Facebook fired" employees is that of an editor and reporter who, in an online article, criticised his employer, TV Barrandov, comparing relations within its structures to a totalitarian regime, claiming that the plans of reportages must be approved in advance by supervisors, which leads to top-down censorship. Nevertheless, the Czech Supreme Court, adjudicating on the case,

[173] See: Štefko, 2016, pp. 11-17.
[174] Štefko, 2023, p. 138; See also: Štefko, M. 2017, p. 155.
[175] Judgement of Kúria (Curia, Supreme Court of Hungary) Mfv. 10.469/2013/4.
[176] Német, 2019, https://index.hu/belfold/2019/05/10/facebook_per_ugyesz_ugyeszseg_kirugas_itelet/?token=ec537fc4771e0f1a5fac51a7cefc3b19 (Accessed: 2 May 2026).
[177] Michalski, , 2022, https://www.gazetaprawna.pl/praca/artykuly/8386055,poczta-polska-zwolnienie-dyscyplinarne-media-spolecznosciowe-wpis-wojna-w-ukrainie.html (Accessed: 2 May 2026). See also: the statement of the Polish Post regarding that case – Poczta Polska, 2022, https://media.poczta-polska.pl/releases/oswiadczenie-2022-03-17 (Accessed: 2 May 2026).
[178] Leśniak, 2021, https://www.prawo.pl/kadry/pracownik-zwolniony-za-wpisy-w-mediach-spolecznosciowych-jaki,508257.html (Accessed: 2 May 2026).

found that the employee's criticism was subjective and unjustified, and objectively capable of endangering the employer's good reputation. Therefore, the disciplinary dismissal was justified.[179]

The momentous nature of these cases lies in the fact that the monitoring of employees via their social media not only and exclusively affects employees' privacy, but also their freedom of expression, which can certainly be included in the sphere of privacy, but which also constitutes a separate fundamental right under the ECHR and the CFREU.[180]

When analysing Recommendations of the Committee of Ministers to Member States, it should be remembered that they are only soft law instruments; they have no legal force and rules stated in their provisions cannot be enforced in any way. Nevertheless, they are of great doctrinal importance, and often even the postulates included in them are reflected in binding legal acts.

The last piece of legislation that should be mentioned in the context of workplace monitoring and employee privacy in the realm of the CoE is the European Social Charter[181], which constitutes a pillar of social and economic rights in Europe.[182] The ESC, in its regulations, does not explicitly address either employees' right to privacy or the right to personal data protection.

Nevertheless, on the basis of Article 1(2), which states that "[w]ith a view to ensuring the effective exercise of the right to work, the Parties undertake: to protect effectively the right of the worker to earn his living in an occupation freely entered upon", the European Committee of Social Right[183] pointed out that the freedom to engage in work inherently encompasses protection against infringements of the right to privacy. Accordingly, it is essential that workers' fundamental right to privacy be recognised and safeguarded within the framework of the employment relationship, ensuring its effective protection.[184] In addition, an interesting and pertinent position was expressed by the committee, justifying the derivation of the right to privacy from the right to take up an occupation freely. Namely, the Committee notes that the advent of new communication technologies has enabled employers to maintain continuous supervision over employees, while also making it possible for employees to perform work for their employers at any time and in any location, including their homes. This development has

[179] The Czech Republic Supreme Court judgement of 20 March 2017, 21 Cdo 1043/206.
[180] This issue has been addressed in the ECtHR judgment in Herbai v. Hungary from 5 February 2020 (Applicaiton no. 11608/15). See also: Koltay, 2022, pp. 331-345.
[181] Hereinafter: ESC.
[182] Lukács, 2021, p. 98.
[183] Hereinafter: ECSR.
[184] European Committee of Social Rights, 2013, p. 26.

blurred the boundaries between professional and private life, increasing the risk of work encroaching upon all spheres of private life, even beyond working hours and outside the workplace.[185]

Therefore, it can be concluded that the Committee's interpretation was directly influenced by the phenomenon of employee monitoring and especially its increasingly severe forms, which result in the fading of the boundary between work and private life. In 2016, the ECSR directly pointed out that Article 1(2) of the ESC also concerns the right to privacy at work.[186]

At the central point of the European Union's framework of personal data protection lies the General Data Protection Regulation[187], which, to a certain extent, originated from the previous Directive 95/46/EC of 24 October 1995[188]. The desire to change the previous model of personal data protection in the EU has been driven by the accelerating pace of technological development, coupled with the effects of globalisation, which fundamentally altered the ways in which vast quantities of personal data are collected, accessed, utilised, and transferred. Moreover, personal data has acquired significant economic value, with many businesses relying on its collection, aggregation, and analysis as a core element of their commercial activities. That is why it has become essential to ensure that individuals can exercise effective control over their personal information.[189] This pushed the EU to reform in order to build a modern, strong, consistent and comprehensive data protection framework.[190]

The GDPR regulation is based on a technology-neutral approach, originally expressed in Directive 95/46/EC.[191] Moreover, the Regulation establishes key principles according to which data are to be collected and processed. These principles are: 1. lawfulness, fairness and transparency; 2. purpose limitation; 3. data minimisation; 4. accuracy; 5. storage limitation; 6. integrity and confidentiality.[192] It also sets out specific categories of data, the processing of

---

[185] European Committee of Social Rights, 2013, p. 26.
[186] European Committee of Social Rights, 2017, p. 32.
[187] 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).
[188] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Offcial Journal L 281.
[189] European Commission, 2012, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Safeguarding Privacy in a Connected World a European Data Protection Framework for the 21st Century*, COM(2012) 9 final, p. 2.
[190] COM(2012) 9 final, p.12.
[191] European Commission, 2010, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, p. 3.
[192] Article 5 of the GDPR.

which should be, in principle, prohibited,[193] and introduces rules on accountability of organisations[194].

The GDPR is of universal scope, binding in its entirety and directly applicable to all EU Member States.[195] Its general regime of data protection law also applies to the employment sphere. Nevertheless, as points out, this presents a significant challenge from a labour law perspective, as the GDPR's provisions are highly detailed and drafted in a technical manner, yet not specifically with labour law in mind. Labour law is a specific field of law with its own set of rules, catalogues of notions and traditions; therefore, its intersection with privacy law creates a very complex relationship.[196]

However, in an attempt to allow the principles expressed in the GDPR to be adapted to the employment sphere, the EU legislator has included in the Regulation Article 88, which gives Member States a certain degree of discretion in setting up personal data protection systems within the employment context. Article 88 of the GDPR states that:

1. 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, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship. 2.
2. 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 a joint economic activity and monitoring systems at the workplace.

The implementation of the aforementioned article resulted in the creation of specific national models for data processing in the sphere of employment, which in turn led to different regulations in the sphere of workplace monitoring. Analysing the differences between these

[193] Article 9 of the GDPR.
[194] Article 5(2) and Article 24 of the GDPR. See also: Hijmans, 2021, pp. 244-246.
[195] Barański, 2022a, p. 56.
[196] Hendrickx, 2023, p. 3.

models of selected European countries (countries of the V4 group) represents the main objective of this thesis.

Article 88 is also of great importance for European and national social partners, primarily because of its component of collective agreements. European social partners in the 2020 Autonomous Framework Agreement on Digitalisation, which is a soft law instrument, evoke Article 88 of the GDPR, pointing out that it opens the way for the social partners to establish "more specific rules to ensure the protection of the rights and freedom with regard to the processing of personal data of employees in the context of employment relationships", through collective agreements.[197] Moreover, the Framework Agreement explicitly affirms that AI deployment at work must follow a "human-in-control" principle and remain under human oversight. It also warns that pervasive digital surveillance risks "compromising the dignity of the human being, particularly in cases of personal monitoring."[198] Thus, the document enshrines a rights-based framework for balancing technological innovation with fundamental labour rights and the preservation of human dignity in the digital transformation of work.

When describing the EU data protection system, especially in relation to employment, it is important not to forget about the Article 29 Data Protection Working Party[199], which was an independent European advisory body on data protection and privacy, established by Directive 95/46/EC and, after the entry into force of the GDPR, replaced by the European Data Protection Board.[200] The WP participated in the creation of the EU data protection system, playing a huge role in employees' data protection, and although the documents it issued were not legally binding, they are still relevant and of great importance for labour law doctrine. From the perspective of the issue of workplace monitoring, three of the most important documents issued by the WP are Opinion 8/2001 on the processing of personal data in the employment context[201], Working document on the surveillance of electronic communications in the workplace[202] and Opinion 2/2017 on data processing at work[203]. Opinion 8/2011 addresses the processing of personal data in the employment context in broad terms, without specifying how the general principles should be applied to particular instances of employee monitoring. The accompanying

---

[197] European social partners autonomous framework agreement on digitalisation of 2020, p. 12.
[198] European social partners autonomous framework agreement on digitalisation of 2020, p. 12.
[199] Hereinafter: WP.
[200] European Data Protection Board, https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en (Accessed: 2 May 2026).
[201] Opinion 8/2001 on the processing of personal data in the employment context, 13 September 2001, 5062/01/EN/Final WP 48.
[202] Working document on the surveillance of electronic communications in the workplace, 29 May 2002, 5401/01/EN/Final WP 55.
[203] Opinion 2/2017 on data processing at work, 8 June 2017, 17/EN WP 249.

Working Document narrows its focus to the monitoring of electronic communications, with particular emphasis on e-mail monitoring and Internet access. On the other hand, Opinion 2/2017 builds upon and complements both Opinion 8/2001 and the Working document, taking into account subsequent societal, technological and legal developments and offering guidance on various forms of data processing and monitoring, including screening of employees, monitoring of ICT usage at and outside the workplace; monitoring systems used to check the time and attendance; video monitoring; and geolocation monitoring[204].[205]

3.2. International Regulations

When looking at the issue of monitoring in the workplace from the perspective of international regulation, it is essential to mention the International Labour Organisation[206], whose competencies with regard to this issue have enabled it to have the greatest impact on legal reality. However, despite the possibilities and mandate possessed by the ILO, the organisation has not opted for any legally binding solutions in this sphere, but rather taken the path of soft law instruments.

In 1996, the ILO's Meeting of Experts on Workers’ Privacy adopted an ILO Code of Practice on Protection of Workers’ Personal Data. The Code aimed to provide guidance on the protection of workers’ personal data on an international scale. However, it was not intended to replace national laws, regulations, international labour standards or any other accepted standards.[207] The recommendatory dimension and the lack of binding force stem from the very nature of the instrument, that is, the Code of Practice. Nevertheless, the question that arises on this ground is why the ILO, on such an important issue as the protection of employees’ personal data, especially at a time when a growing number of related risks were becoming apparent, decided to use the weakest regulatory instrument rather than, for example, a legally binding convention. An interesting explanation of this move on the part of the ILO was provided by Simitis. As he claims, the decision to adopt a code of practice was largely strategic. A binding Convention would have required lengthy negotiations, multiple compromises and eventually faced the risk of deadlock, particularly given the highly controversial nature of employee data protection. By contrast, a Code of Practice could be adopted more swiftly, avoiding procedural impasses and

[204] Opinion 2/2017 on data processing at work, 8 June 2017, 17/EN WP 249, pp. 12-21.
[205] Lukács, A., 2021, p. 101.
[206] Hereinafter: ILO.
[207] Article 2 of the ILO CoP.

allowing the ILO to intervene promptly in the rapidly evolving international debate on digitalisation and personal data protection. Importantly, the Code enabled the ILO to set out concrete and detailed rules, while still avoiding the formal obligations imposed by a Convention. On the other hand, the form of the Code of Practice has only enabled the ILO to generate "moral pressure" rather than achieve a real change in the laws and practices of Member States and employers.[208]

Leaving aside the reflections on the nature and form of the ILO Code of Practice, it should be pointed out that it contains highly valuable and innovative solutions concerning the protection of employees' personal data and workplace monitoring.

First of all, it is important to note that the ILO CoP covers both public and private sectors, and when it comes to the method of workers'[209] data processing, it applies to manual and automated processing.[210]

The most significant part of the Code of Practice is Article 5, as it lists all the general principles and places them in the context of employment. The legitimacy and purpose limitation principle is expressed by Article 5.1, in which the Code provides that "personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker."[211] The principle of legitimacy is further developed in Article 5.13. It states that "workers may not waive their privacy rights."[212] This provision is extremely important from the point of view of the processing of employee data, and in particular of employee monitoring, as it means in practice that employee's consent cannot form a basis for legitimate processing of personal data.[213][214] Moreover, the processing of personal data should not result in unlawful discrimination against employees.[215]

[208] Simitis, 1998, pp. 362-363.
[209] Regarding the definition of "worker", the ILO Code of Practice leaves this issue to national law and practice. However, the use of this term in the Code is intended to cover current, former and potential future employees (job applicants), as data processing have specific implications for all of them.
[210] Article 4 of the ILO CoP.
[211] Aricle 5.1. of the ILO CoP.
[212] Article 5.13. of the ILO CoP.
[213] De Hert and Lammerant 2013, p. 20.
[214] An in-depth analysis of the issue of employee's consent as a basis for lawful employee monitoring will be carried out later in the thesis, but for the moment it should be pointed out that the view expressed in the ILO Code of Practice has reverberated widely in labour law doctrine and constitutes an imporatnt basis of argumentation for many authors. For example Barański and Giermak states that while there may be certain situations where employees' consent may constitute an appropriate basis for the processing of their personal data (e.g. when the employees are at the same time customers of their employer), it should in principle be considered that the specific nature of the employment relationship, in particular the inequality between the employee and the employer and the employee's subordination to the employer, prevents the employees from fully freely giving their consent. - See: Barański and Giermak, 2017, p. 208.
[215] Article 5.10. of the ILO CoP.

The ILO CoP also expresses the so-called "finality principle."[216] It means that personal data should be used only for the purposes for which they were originally collected.[217] Nevertheless, this principle is immediately balanced as, given the length of the employment relationship, in some cases, and the changing needs of the employer,[218] the CoP provides that when personal data are processed for different purposes than the original ones, for which they were collected, the employer is obliged to ensure that they are not used in a manner incompatible with the original purpose, and to take the necessary measures to avoid any misinterpretations.[219] However, in one case, a change of purpose is not allowed. If personal data is collected in connection with technical or organisational measures to ensure the security and proper functioning of automated information systems, it should not be used to control the behaviour of employees.[220]

The code opposes completely automated and mechanised decision-making and instead advocates individualised employee assessment.[221] It can even be said that it expresses the principle of the primacy of the human factor during the employee assessment process. Nevertheless, it does not entirely prohibit the use of automated data processing measures and electronic monitoring in decision-making and employee evaluation processes. The emphasis of Articles 5.5 and 5.6 of the CoP is on the phrases "solely" and "should not be the only factor", thus, it should be noted that the data processing and monitoring measures indicated should serve as measures and factors ancillary to others, in which the main role is played by a human being who is able to accurately and reasonably analyse and correct the decision or assessment.[222]

It is of utmost importance that the ILO CoP draws attention to the role of employees in the protection of personal data, especially its collective dimension. It states that employers, workers and their representatives should cooperate in protecting personal data and in developing privacy policies in accordance with the Code.[223] Furthermore, in order to comply with the principle of transparency, the employer is obliged to inform employees and their representatives of how

---

[216] De Hert and Lammerant (2013), p. 20.
[217] Article 5.2. of the ILO CoP.
[218] Commentary on the Code of Practice, 1997, Geneva: International Labour Office, p. 13.
[219] Article 5.3. of the ILO CoP.
[220] Article 5.4. of the ILO CoP; ILO, 1997, Commentary on the Code of Practice, p.13.
[221] "Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data." - Article 5.5. of the ILO CoP; "Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance." - Article 5.6. of the ILO CoP.
[222] ILO, 1997, Commentary on the Code of Practice, p. 14.
[223] Article 5.11. of the ILO CoP.

their data are processed and of their rights in this respect.[224][225] All parties with access to personal data should respect its confidentiality.[226]

Although the vast majority of the principles expressed in the Code are addressed to employers, as the actors most frequently processing employees' data, the Code also envisages a situation in which it is employees, e.g. because of their work and duties, who are involved in the processing of personal data. Such persons should receive regular training on the meaning and consequences of data processing, as well as the specific responsibilities they have for the correct application of the Code.[227]

Following the publication of the Code of Practice, the ILO has not relented in its efforts and continues to regularly raise the issue of the right to privacy at work, especially in the context of the digitalisation of workplaces. The Global Commission on the Future of Work, in its report "Work for a Brighter Future", in which it calls for the use of technology in support of decent work and emphasises a human-in-command approach to technology, it also asks governments, employers and workers' organisations to monitor the effects of technological change on work, to guide its development in ways that uphold workers' dignity, and to consider the adoption of new regulatory measures accordingly.[228]

Moreover, in 2022, the ILO published a Working Paper on the protection of workers' personal data. The main purpose of the paper was to present an overview of legal standards concerning the protection of workers' personal data and to examine, from both global and regional perspectives, the emerging trends, guiding principles and examples of good practice in this field.[229] In the paper, Hendrickx points out that the future of work is inseparable from the right to privacy. Technological developments, ranging from digital communication tools designed for telework, AI, and robotics, are reshaping work-life boundaries and redefining the

[224] Article 5.8. of the ILO CoP; De Hert, P. and Lammerant, H., 2013, p. 20.
[225] The content of the information obligation is further developed in Article 6.14. of the ILO CoP. In this provision, the Code sets out two conditions that an employer must fulfil in order for monitoring to be considered permissible. First of all, workers which are subjected to monitoring should be informed in advance of the reasons, length, the methods of data collection during monitoring. Secondly, the employers are obliged to minimise the interference with the privacy of workers, which in practice means, that they should use the least intrusive monitoring measures possible to achieve their objectives. In addition, the regulation restricts secret and continuous monitoring only to specific cases, as monitoring containing these traits can by extremely burdensome for physical and mental health of employees. The secret monitoring is possible only when it is allowed by national legislation or when it is used in investigation against criminal activity or other serious wrongdoing (suspicion of such activities should be based on reasonable grounds). On the other hand, the continuous monitoring can be used only if it is necessary for health and safety or property protection reasons. See also: ILO, 1997, pp. 18-19.
[226] Article 5.12. of the ILO CoP.
[227] Article 5.9. of the ILO CoP.
[228] Global Commission on the Future of Work, 2019, pp. 43-44.
[229] Hendrickx, 2022, p. 5.

very nature of work. Thus, the protection of workers' personal data must be viewed within the broader context of safeguarding privacy as part of a human-centred legal framework.[230]

Despite the fact that, contrary to e.g. the EU, activity on the part of the ILO is limited to soft-law instruments, this approach is to be, to a certain extent, valued, as it represents a very important contribution to the discussion on employees' personal data protection and monitoring. The current changes in the working environment are so dynamic, and the approaches of specific countries are so different, that an attempt to include these issues in a convention could end in failure, preceded by a process of long negotiations. It appears that, at this point, it is much more effective to work towards regional or national regulations covering this topic. The ILO, on the other hand, as a kind of forum for discussion, allows, in this context, for the exchange of experiences between states and for putting forward proposals on the protection of personal data which do not require consensus.

4. National regulations

4.1. Hungarian Regulation on Workplace Monitoring

Hungarian labour law until 2012 dealt very residually with the issues of data protection, privacy and the possibility of monitoring in the workplace. The regulation of these issues was reduced to a few provisions contained in the 1992 Hungarian Labour Code.[231][232] Firstly, this Code, in the first sentence of Section 3 Subsection 4, provided that: "employers may only disclose facts, data and opinions concerning an employee to third persons in the cases specified by law or with the employee's consent." The second provision relating to the issue at hand was Section 77 Subsection 1, which indicated that: "an employee shall only be requested to make a statement, fill out a data sheet, or take an aptitude test if it does not violate his personal rights and which essentially provides information considered substantive for the purposes of entering into an employment relationship." Nevertheless, it is interesting to note that the Code contained additional regulations related to the control of remote working (teleworking). According to Section 192/G Subsection 3: "in justified cases the employer shall be entitled to inspect completion of the work assignment by the person employed in teleworking. This inspection shall not constitute any right for the employer to inspect any information stored on the computer

[230] Hendrickx, 2022, p. 50.
[231] Act XXII of 1992 on the Labour Code.
[232] Balogh et al., 2012, p. 99.

or other information technology equipment of the person employed in teleworking used for working, which are not related to the rights and obligations arising from the employment relationship”. Moreover, unless there is an agreement to the contrary, the employer shall determine the type of inspection and the shortest period of time between the notification and commencement of the inspection if conducted in a property designated as the place of work. The inspection may not bring any unjustified and unreasonable hardship on the person employed in teleworking with a view to his personal, family and other circumstances, or on any other person who is also using the property designated as the place of work.[233]

The legal situation changed significantly on 6 January 2012 with the entry into force of the new Hungarian Labour Code. Namely, the new regulation introduced a separate title on protection of personal rights, consisting of three sections – Section 9 devoted to the protection of personality rights; Section 10 regulating the question of the disclosure of worker’s information and Section 11 establishing the employer’s right to monitor workers; however, only to the extent pertaining to the employment relationship.[234]

However, the most significant, from the point of view of the issue of workplace monitoring, changes have been triggered by the entry into force of 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). In order to bring the Hungarian data protection legal system in line with the GDPR, the Hungarian legislator adopted Act XXXIV of 2019 on the amendments necessary for the implementation of the European Union reform on data protection in April 2019.[235] The Enforcing Act amended more than 80 laws, including with regard to Article 88 of the GDPR, the Hungarian Labour Code of 2012, introducing, among other things, Title 5/A: Data management.[236][237]

The new Title consists of three sections: Section 10, Section 11 and Section 11/A. However, not all of these are entirely new provisions. Section 10, under which the issue of information disclosure and aptitude tests is regulated, and Section 11/A (former Section 11), which sets out the rules for workplace monitoring, already existed; however, they have been amended and

233 Section 192/G Subsection 4 of the Act XXII of 1992 on the Labour Code.
234 Title 5: Protection of Personal Rights of Act I of 2012 on the Labor Code (version before amendment of 2019 Act XXXIV on the amendments necessary for the implementation of the European Union reform on data protection).
235 Act XXXIV of 2019 on the amendments necessary for the implementation of the European Union reform on data protection (hereinafter: Enforcing Act).
236 Title 5/A: Data management of Act I of 2012 on the Labor Code.
237 Lukács, 2021, p. 108.

expanded through the Enforcing Act.[238] Completely new is Section 11, dealing with the processing of employee's biometric and criminal personal data.[239]

When it comes to the changes in Section 10 from the perspective of broadly understood workplace monitoring, Subsection 4, enabling employers to organise aptitude tests for employees, is significant. As aptitude tests, we can certainly consider all kinds of tests aimed at checking the employee's skills and attitude to a particular position[240]; however, according to Gyulavári, such tests should also include medical testing.[241] Given that sensitive employee data, such as medical and mental data[242], may be disclosed during such tests, the Hungarian legislator allows them only under two conditions: when they are required by employment regulations or when they are necessary to exercise rights or fulfil an obligation stated in the employment regulations.[243]

Given the dissertation topic, the most important thing is the new wording of Section 11/A. Subsection 1 of Section 11/A states the employer's right[244] to monitor employees' behaviour related to the employment relationship. Under this provision, the employer may monitor all aspects of the employee's daily activity associated with the employment relationship, including the employee's location, working time, number of breaks, etc.[245] For the purpose of the monitoring, unless it is contrary to the regulations of the different agreement, the employer may use technical devices. Employees need to be informed about the application of monitoring in advance in writing; thus, it should be considered that, in principle, covert monitoring is not allowed.[246] However, as the Hungarian Supreme Court indicated in its decision, a video recording made with a covert camera can be used as evidence in criminal proceedings, but in civil proceedings, it can be decided whether the recording violates someone's personal rights.[247]

Current wording of Subsection 1 of Section 11/A, because of its vagueness and lack of specific rules on the conduct of employee monitoring, should be rather considered as a general

[238] Lukács, 2021, p. 112.
[239] Section 11 of Act I of 2012 on the Labor Code.
[240] McCartney, 1994, p. 860.
[241] Gyulavári, 2023, p. 295.
[242] According to Ienca and Malgieri, the term "mental data" should be defined as "*any data that can be organised and processed to deduce an individual's mental states, including their cognitive, affective and conative states*" – Ienca and Malgieri, 2022, p. 4.
[243] Section 10 Subsection 4 of Act I of 2012 on the Labor Code.
[244] Some authors claim that it is not only a right but an obligation of the employer deriving from the employer's obligation to ensure safety at work. - See more: Lőrincz, 2025, Commentary on Section 11/A in Petrovics Z. (ed.) *A Munka Törvénykönyvének magyarázata*. Budapest: ORAC Kiadó; Lukács, 2021, p. 113.
[245] Gyulavári, 2023, p. 298.
[246] Gyulavári, 2023, p. 298.
[247] The Hungarian Supreme Court decision (Kúria/Curia), EBH2000. 296.

regulation, which requires clarification through doctrine, case law and the instructions of the Hungarian Data Protection Authority. It is interesting to note that, before the amendments introduced by the Enforcement Act, the Hungarian Labour Code featured two additional prerequisites for monitoring. It stated that the means and methods of monitoring should not violate human dignity and the private lives of the employees.[248] In the process of changes, the legislator decided to remove these two prerequisites, pointing out that the protection of human dignity and private life does not relate only to the monitoring activities, but to all aspects of the employment relationship. Moreover, protection of these two values can be derived from the general rules of labour law.[249]

Due to the residual nature of the Hungarian regulation on employee monitoring, the Data Protection Authority has prepared a practical guide on data processing at work. Although the guide was issued before the changes related to the entry into force of the GDPR, some parts of it, especially those concerning monitoring, may be applicable to the current legal situation. The guide, among other things, pointed out that camera monitoring may not be operated only to monitor employees and their activities. Moreover, the use of electronic surveillance for the purpose, even if not declarative, of influencing the behaviour of employees in the workplace may be considered unlawful. The cameras used for monitoring may not be placed in the areas where they would violate human dignity, especially in changing rooms, showers, toilets and e.g. medical rooms.[250] The Hungarian Data Protection Authority also stated that the monitoring of employee's geolocation by GPS is permissible only within working hours.[251] The guide is highly acknowledged by Hungarian doctrine, e.g. Lukács, when analysing the principles according to which monitoring can be carried out, referred to this guide.[252] He indicated that the methods of monitoring should be suitable for achieving the objective, i.e. the interest of the employer and the rights which are to be protected through monitoring.[253] Monitoring should be conducted in accordance with the rules of necessity and proportionality, and in every case, it should take into consideration the value of the employee's dignity.[254] Lukács also points out that, according to Section 7 Subsection 1 of the Hungarian Labour Code of 2012, the right to

---

[248] Section 11 Subsection 1 of Act I of 2012 on the Labor Code (version before amendment of 2019 Act XXXIV on the amendments necessary for the implementation of the European Union reform on data protection).
[249] T/4479. számú törvényjavaslat az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról, 2019, p. 102.
[250] A Nemzeti Adatvédelmi és Információszabadság Hatóság (hereinafter: NAIH), 2016, pp. 23 - 24.
[251] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 34.
[252] Lukács, 2021, p. 113.
[253] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 6.
[254] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 6.

monitoring may not be performed in a way that would violate the rights of the employees or prevent them from expressing their opinions.[255]

New regulation introduced to the Hungarian Labour Code of 2012 by the amendments of the Enforcing Act is Subsection 2 of Section 11/A. The provision stipulates that, unless parties of the employment relationship agree differently, the employee may use electronic devices provided by the employer only for the purpose of performing work within the realms of the employment relationship. For the purpose of the inspection, whether the employee uses the devices in compliance with the agreement or the rule stated by Subsection 2 of Section 11/A, the employer may monitor only data which is related to the employment relationship.[256] Therefore, it should be concluded that the scope of the employer's inspection is closely linked to the question of whether and, if so, to what extent it is allowed to use the electronic devices provided by the employer for private purposes. As Kajtár states, the employer has a choice between three models: banning, restricting and regulating the use of electronic equipment for private reasons.[257]

If the usage is regulated by the parties in such a way that the personal use of the devices is allowed, the employer may monitor only data related to the employment relationship and check whether the conditions associated with private use are complied with.[258] Given that the employer cannot monitor an employee's private data, it is good practice in this context for any private data of an employee to be marked and stored separately on such a device, so that the employer is not in doubt as to which data is private and which data is connected to the employment relationship. However, what about the situation where it is prohibited to use equipment provided by the employer for private purposes and yet the employee used the equipment for such purposes? In such a situation, can the employer gain access to the employee's private data? The answer to that question is not so obvious. According to Subsection 4 of Section 11/A, the data, which is required to check compliance with the prohibition stated in Subsection 2 of Section 11/A, should be considered as data related to the employment relationship. Thus, considering the wording of this provision, we might have the impression that *de facto* private data can also be considered as data related to the employment relationship and will be subject to monitoring by the employer. Nevertheless, such an

[255] Section 7 Subsection 1 of Act I of 2012 on the Labor Code (version before amendment of 2019 Act XXXIV on the amendments necessary for the implementation of the European Union reform on data protection); Lukács, 2021, p. 113.
[256] Section 11/A Subsection 3 of Act I of 2012 on the Labor Code.
[257] In principle, Kajtár refers in this context only to the use of the internet by employees, but her conclusions may apply to all devices referred to in Section 11/A Subsection 2 - See: Kajtár, 2016, pp. 119.
[258] Lukács, 2021, p. 216.

interpretation must be regarded as erroneous. As indicated by the legislative material on the necessary legal amendments to implement data protection reform in the European Union, when personal use is prohibited, the employer may access the data stored on the provided device only to the extent necessary to decide whether the data is private or professional.[259]

The provisions indicated in Subsections 2 and 3 of Section 11/A illustrate a certain change of emphasis in the Hungarian Labour Code of 2012. By introducing it, the Hungarian legislator decided to replace the previously existing prohibition on monitoring an employee's private life.[260] Such a solution gives more freedom to the parties of the employment relationship, but may cause significant risks to the employee's privacy, especially since the provision stated in Subsection 3 applies even when employees use their own equipment to carry out the work.[261]

4.1.1. Monitoring Outside of Working Hours as a Characteristic Element of the Hungarian Workplace Monitoring Model

The characteristic feature of Hungarian regulation of employee monitoring is that it not only affects employees during working hours but may also occur outside them.[262] Section 8 of the Hungarian Labour Code states that even outside of working hours, an employee should not be involved in any conduct which, especially considering the nature of the employee's job and his or her position in the employer's hierarchy, may directly and effectively endanger the employer's good reputation, legitimate economic interest, or the purpose of the employment relationship.[263] Moreover, the employee's right to express an opinion is *de facto* limited as it cannot cause serious harm or damage to the employer's reputation, legitimate economic or organisational interest.[264][265]

Section 8 of the Hungarian Labour Code shall not be perceived as a regulation enabling a subjective and unlimited restriction of the employee's freedom of expression by the employer because the employee's personal rights may only be restricted if it is essential for a legitimate purpose directly connected to the employment relationship and is proportionate to achieving

[259] T/4479. számú törvényjavaslat az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról (2019), p. 102.
[260] Varga, 2019, p. 88.
[261] Section 11/A (5) of Act I of 2012 on the Labor Code.
[262] Cséffán, 2024, p. 49.
[263] Section 8 Subsection 2 of Act I of 2012 on the Labor Code.
[264] Section 8 Subsection 3 of Act I of 2012 on the Labor Code.
[265] A different view on the subject is expressed by András Koltay, who states that this provision actually gives the employer a free hand to take actions against employees' freedom of expression - See: Koltay, 2022, p. 334.

that objective.[266] The restriction is accompanied by the information obligation – the employee should receive written information about that in advance.[267]

However, due to its nature, Section 8 has caused a lot of controversy and discussion in Hungarian labour law doctrine, especially on how to reconcile this provision with the general prohibition of violation of an employee's private life. Examining this issue, Pók points out that although Section 8 Subsection 2, under certain conditions, allows for the restriction of the employee's conduct outside working hours, such conduct should be considered as a part of the employee's private life, which should not be subjected to the employer's monitoring. The author notes that the monitoring of employees' Internet activity, which took place via their own devices outside working hours, is, in fact, unacceptable. In such situations, information about an undesirable opinion about an employer in the online sphere can only be acquired by him or her accidentally.[268] Mélypataki and Rácz, in general, take a similar position to that expressed by Pók; however, they approach this conflict from a slightly different angle. They differentiate two rights of an employer – the right to indirect control stated by Section 8 and the right to monitoring indicated currently in Section 11/A of the Hungarian Labour Code.[269] The authors point out that Subsection 2 of Section 8, unlike Section 11/A, does not provide an employer with a right to direct control through monitoring of employees, but rather enables an employer to sanction the behaviour of the employee, which should be considered as an indirect form of control.[270]

A dissenting and seemingly more accurate view is articulated by Kajtár and Rácz. Kajtár writes that according to the provisions of the Hungarian Labour Code[271], the monitoring of the employees' behaviour outside working hours is, in principle, not forbidden as long as such behaviour is related to the employment relationship.[272] Moreover, on the basis of the previous state of the law, Kajtár rightly points out that the provision of the Hungarian Labour Code did not indicate that employee privacy cannot be subject to monitoring. Former Subsection 1 of Section 11 only indicated that an employee's private life could not be violated.[273] Therefore, it should be concluded that, if all statutory requirements are met, the monitoring of employees'

[266] Section 8 Subsection 2 in conjunction with Section 9 Subsection 2 of Act I of 2012 on the Labor Code.
[267] Section 8 Subsection 2 of Act I of 2012 on the Labor Code.
[268] Pók, 2012, pp. 160–165.
[269] In their chapter Mélypataki and Rácz refered to the right to monitoring stated at the time in Section 11. Later, the Enforcement Act od 2019 moved regulation on monitoring to the new Section 11/A. However, the conclusion drawn by the authors can also be applied to the currecnt legal state.
[270] Mélypataki and Rácz, 2018, p. 679, 682.
[271] At that time Section 11, currently Section 11/A of the Hungarian Labour Code of 2012.
[272] Kajtár, 2015, pp. 203.
[273] Kajtár, 2015, p. 203.

behaviour outside working hours has to be considered legal. A convergent view is expressed by Rácz. She states that under Section 8 of the Hungarian Labour Code, monitoring of employees' behaviour outside working hours is permissible. However, Rácz draws attention to the very limited scope of this monitoring. It should be carried out methodically and under certain conditions expressed in the Labour Code.[274]

The conclusions expressed by Kajtár and Rácz take on even greater significance in the light of the actual wording of Section 11/A of the Hungarian Labour Code, which has been stripped of the provision expressing the protection of human dignity and privacy of the employee from overly severe employer monitoring. However, this does not mean that, because of the amendment in the Labour Code in 2019, employers are now entitled to monitor the private lives of employees without any restrictions. Firstly, just as before the changes, the regulations stipulate that the monitored employee's behaviour must be related to the employment relationship, and secondly, as already indicated before, the Hungarian legislator decided to remove the provision on dignity and privacy, as it recognised that the protection of human dignity and employee's privacy derives from the general principles of labour law and both values must be protected in every situation, not only in case of monitoring. Therefore, the view expressed by Kajtár and Rácz should be considered valid and applicable to the current regulation of employee monitoring in Hungary.

The question of monitoring outside working hours is not only theoretical, but also a practical issue. In 2013, the Hungarian Supreme Court heard the case of an employee who was dismissed owing to his social media activity.[275] The dismissed employee published a post on his Facebook profile in which he threatened and insulted the employer and exhorted other employees to organise. From the information available on the employee's profile, it was possible to identify who his employer was. Kúria agreed with the judgments of the court of the first and the second instance and ruled that, considering the circumstances of the case, the employer could legitimately consider the employee's action as conduct that made it impossible to maintain the employment relationship, thus the termination of the employment relationship by extraordinary termination was lawful. Justifying its decision, the Court indicated that the threats and abusive language used by the employee constituted a violation of freedom of speech, as it could lead to damage to the reputation of the employer and the management.

Another case of termination of employment relationship due to social media activity outside of working hours that has received publicity in Hungary is that of a prosecutor who was

[274] Rácz, 2015, pp. 284-285.
[275] Judgement of Kúria (Curia, Supreme Court of Hungary), Mfv. 10.469/2013/4.

disciplinary dismissed because of the published posts on his Facebook profile. The posts were published in the context of parliamentary elections, which were to be organised on 8 April, and were politically tinged. The court of the first instance ruled that two of the prosecutor's posts stated the expression of his freedom of speech, and only the third one could be considered a disciplinary offence.[276] However, the court stated that the dismissal was excessive and ruled only to reduce the prosecutor's remuneration. Despite the appeal of the prosecutor's office, the court of the second instance made the same statement as the court of the first instance.[277]

While a direct comparison between the two cases is not entirely conclusive due to differences in their factual background, a tentative conclusion can still be drawn. Given the prosecutor's duty to remain apolitical and independent, and the importance of his public role, his actions arguably caused greater harm, especially to the public sphere, than the offensive Facebook post of a private company's employee, who was dismissed on disciplinary grounds. In this context, the core issue concerns the conceptual boundaries of the notion "freedom of speech" linked to the employment relation, which appears to be applied inconsistently by the Hungarian judiciary.

4.2. Polish Regulation on Workplace Monitoring[278]

The Polish model of workplace surveillance differs from the Hungarian, Czech and Slovak models. It is a more closed and precise system, defined by three areas of surveillance: video, e-mail and other forms of monitoring, with clearly defined objectives for each surveillance measure. This model seems to be more in line with current standards on privacy in the workplace and is more understandable to the parties of the employment relationship, as it clearly addresses certain issues that are not directly regulated by the Labour Code in other models. This is partly due to the fact that the Polish regulation establishing a workplace monitoring model is the most recent regulation in the Visegrad Group countries after the Hungarian regulation, 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

[276] The third post concerend a publically known political person who could potentially have been involved in the fraud affair. The prosecutor shered a link to an article and added his comment "well, every 'accused' chooses his own defence, we will laugh at him at most. Go ahead... Oh, and April 8".

[277] Német, 2019, https://index.hu/belfold/2019/05/10/facebook_per_ugyesz_ugyeszseg_kirugas_itelet/?token=ec537fc4771e0f1a5fac51a7cefc3b19 (Accessed: 2 May 2026).

[278] Based on this fragment, an article was prepared and published: Mirosławski, T. (2025) 'Between Casuistry and Vagueness – A Comparative Legal Analysis of Employer Surveillance of Employee Tasks under Polish and Czech Legislation', Central European Academy Law Review, 2(1), pp. 191-216.

and implicit way.[279] Some of the principles were derived from the Constitution,[280] some were interpreted from the Labour Code,[281] and some had their source in the Act of 29 August 1997 on the protection of personal data.[282] 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,[283] regulating the conditions and scope of admissible workplace monitoring.

These provisions explicitly state that, under the Polish model of workplace monitoring, employers may apply two main forms of monitoring – video monitoring and monitoring of employees' business email – provided that their use is conditional on the existence of specific needs arising in the workplace. These needs are set out in the regulations. Nevertheless, pursuant to Article 22^3 §4 of the PLC, the catalogue of admissible forms of surveillance within the workplace has been extended, as under certain conditions, it enables the use of other forms of monitoring than video and business email monitoring. However, for other forms of monitoring, the provisions regarding the monitoring of an employee's business email should apply *mutatis mutandis*.[284] 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,[285] and many others, depending on the target of monitoring and the nature of the activity of the employer.

Concluding, it should be noted that 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.[286]

---

[279] Otto, 2023, p. 393.
[280] 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.
[281] Art. 11^1 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (hereinafter: PLC).
[282] 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.
[283] Art. 111 of the Act of 10th May 2018 item 1781 on personal data protection.
[284] Art. 22^3 §4 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
[285] Otto, 2023, pp. 409-410; Dąbrowska, 2019, p. 19.
[286] See: Kuba, 2014, pp. 561, 569.

4.3. Czech Regulation on Workplace Monitoring[287]

The question of monitoring 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 dissertation, as they touch upon the issue of workplace monitoring measures. 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.[288]

There is a certain duality between Paragraphs 1-3 of Section 316, as they can be divided into two groups.[289] 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.[290] 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.[291] However, in contrast to the first paragraph, Paragraph 2 points out the means of possible workplace surveillance, which, under certain conditions[292], will constitute an admissible

[287] Based on this fragment, an article was prepared and published: Mirosławski, T. (2025) 'Between Casuistry and Vagueness – A Comparative Legal Analysis of Employer Surveillance of Employee Tasks under Polish and Czech Legislation', Central European Academy Law Review, 2(1), pp. 191-216.

[288] Section 316 (4) of LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce" (hereinafter: CLC) - The employer may not require from an employee information that does not directly relate to performance of work and to basic labour relationship pursuant to section 3. The employer may not require in particular the information on: (a) pregnancy, (b) family and property situation, (c) sexual orientation, (d) origin, (e) trade union organization membership, (f) membership of political parties or movements, (g) religion or confession, (h) unimpeachability (clean criminal record), but the above shall not apply [thereby still excluding the information pursuant to (c), (d), (e), (f) and (g)] where there is a cause for it consisting in the nature of work to be performed provided that the requirement is adequate, or in the cases where it is laid down in this Code or in another Act. The said information may not be obtained by the employer even through third parties.

[289] Šmejkal, 2019, p. 58.

[290] Section 316 (1) of 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.

[291] Section 316 (3) of 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.

[292] 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.

infringement of the employee's privacy.[293] 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.

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 touches upon the issue of the employer's property, while the second and third paragraphs cover the protection of employees' privacy.[294] 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. On this ground, 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 to this question illustrates the complexity of the Czech workplace monitoring system and will be addressed in the second chapter of the thesis.

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? This topic will be explored further in the second chapter of this work.

In Czech labour law doctrine, there is an approach that aims to clarify the interpretative ambiguities arising from Paragraphs 1 and 2 of Section 316 of the CLC. This approach, recommended by Štefko, addresses both paragraphs holistically 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.[295] Štefko also

[293] Section 316 (2) of 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.
[294] Judgement of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011; Judgement of the Czech Supreme Court of 07 August 2014, 21 Cdo 747/2013.
[295] Štefko, 2016, p. 15; Štefko, 2017, p. 153; Štefko, 2023, p. 153.

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.[296] 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 the employer.[297] This pressure does not necessarily have to be direct but can often involve a limitation of future employment prospects (such as promotion, etc.).[298] 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.

4.4. Slovak Regulation on Workplace Monitoring

Similar to other countries in the Visegrad Group, the issue of workplace monitoring has been regulated under Slovakian legislation primarily in the Labour Code[299], which serves as *lex specialis* to the Personal Data Act[300], considered in this context as *lex generalis.*

Analysing the question of workplace monitoring from the perspective of Slovak legislation, it should be mentioned that the Code distinguishes 11 basic principles of labour law, which constitute a sort of introduction or even, one might say, preamble to the Labour Code. The last of these principles, indicated in Article 11, gives expression to the protection of an employee's personal data. The article states that "Employers may collect personal data on employees only when these relate to the qualifications and professional experience of employees and data that may be significant for the work that employees are expected to carry out, carry out, or have carried out."[301] This article represents the significance that the Slovak legislator has given to the protection of personal data that may be processed in connection with an employment relationship, and is also the basic provision regulating this issue in the Slovak labour law

[296] Štefko, 2023, p. 153; Jouza, 2022.
[297] Otto, 2016, p. 86.
[298] Morris, 2001, pp. 53-54.
[299] Act 311/2001 Coll. (hereinafter: Slovak Labour Code/SLC).
[300] Act 18/2018 Coll. (hereinafter: Personal Data Act).
[301] Article 11 of the Slovak Labour Code.

system. Moreover, in the doctrine, it is pointed out that this article follows three fundamental principles which apply to any situation, including situations concerning employment, of interference or breach of the right to respect for private life as expressed primarily in Article 8 of the European Convention on Human Rights. Such interference may be considered lawful and justified if it complies with the principles of legality, legitimacy and proportionality.[302] This view was also articulated by the Constitutional Court of the Slovak Republic, which in its judicial decision from 4 February 2009 referred to the jurisprudence of the European Court of Human Rights.[303]

In accordance with the principle of legality, the interference with the right to private life is possible only if there is a clear legal basis for it. Thus, the legality of the interference is examined in terms of whether it was carried out in compliance with the applicable legal provisions, taking into account whether the provisions were published and therefore available, and whether their effects were foreseeable. Consequently, the quality of the legal regulation underlying the possibility for interference with the right to private life should also be examined.[304] Taking into account the abovementioned criteria of the principle of legality, Article 11 of the Slovak Labour Code shall be considered to be in compliance with this principle, as the provision is available to the public, specific, and its effects can be foreseen.[305]

In addition to the fact that an interference in private life will have a proper legal basis, it must also have a legitimate purpose. The emanation of the need to express such a purpose is the principle of legitimacy. The Slovak Constitutional Court points out that the legitimacy of interference with the right to privacy derives from Article 8 (2) of the ECHR. It means that the right to privacy may only be interfered with when it is essential for the interest of the State for reasons of national security, public safety, prevention of disorder or crime. The interference is also legitimate when it takes place in the interests of society for reasons of health and morality, to ensure the economic well-being of the country and in the interests of individuals for the protection of their rights and freedoms.[306]

In the labour relations context, it should be mentioned that the employer's economic interest may also be considered as a legitimate aim of interfering with the employee's private life; however, this will not be the case in every situation. Barancová indicates that the recognition of the employer's economic interest as a legitimate aim of interference will depend on the

[302] Barancová, 2019, pp. 147-149; Mesarčík and Poruban, 2023, p. 458.
[303] Judicial decision of the Constitutional Court of the Slovak Republic, I. ÚS 117/07 of 4 February 2009.
[304] Judicial decision of the Constitutional Court of the Slovak Republic, I. ÚS 117/07 of 4 February 2009.
[305] Mesarčík and Poruban, 2023, p. 458.
[306] Judicial decision of the Constitutional Court of the Slovak Republic, I. ÚS 117/07 of 4 February 2009.

circumstances of the specific case, in particular, the character and object of the employer's activities, and on an assessment of the binding nature of the legal consequences in the case of a threat or violation of the employer's entitlements. Furthermore, the employer's conduct must be based on the appropriate legal basis and be characterised by proportionality.[307] Therefore, under Article 11 of the Slovak Labour Code, employers should take into consideration the specific nature of their economic activity and collect only the data related to a serious and clearly defined reason.[308]

In practice, determining the level of working time usage and examining the quality of work performance are identified as frequent rationales for employers to monitor employees during working time. Another reason, which is of great importance, is the employer's intention to prevent damage to his/her property. In order to prevent such damage, employers focus on verifying compliance with work discipline or checking for information leaks to third parties.[309]

The last principle, which is the principle of proportionality, means that the right to privacy may only be interfered with when it is necessary. In practice, this implies that, under the given circumstances, it was not possible to use other, less severe measures to achieve the legitimate aim.[310] When analysing the requirement of necessity, it should be noted that it will not be met if the interference took place due to need or usefulness.[311]

The interference should also be in accordance with the standards of a democratic society. The notion of "the standards of a democratic society" is related to the "democratic necessity test" shaped by the jurisprudence of the European Court of Human Rights[312].[313] In its practice, the ECtHR stated that the key feature of the European public order is not only political democracy, but the European Convention of Human Rights was established to uphold and advance the principles and values of a democratic society.[314] When referring to the notion of "democratic society", the Court points out that its main characteristics can be indicated: pluralism, tolerance and broadmindedness. Similar to the ECtHR, the Slovak Constitutional Court also attempted to define a "democratic society." The first two features of a "democratic society" mentioned by it are also pluralism and tolerance. However, when pointing out the third feature, the Slovak Constitutional Court used a different term. It pointed out that a

[307] Barancová, 2019, pp. 148-149.
[308] Mesarčík and Poruban, 2023, p. 458.
[309] Barancová, 2017, p. 256, cited in Horňák, 2017, p. 197.
[310] Judicial decision of the Constitutional Court of the Slovak Republic, I. ÚS 117/07 of 4 February 2009.
[311] Barancová, 2019, p. 149.
[312] Hereinafter: ECtHR.
[313] Trykhlib, 2020, p. 134.
[314] ECtHR judgment in Gorzelik and Others v. Poland from 17 February 2004 (Application no. 44158/98).

“democratic society” is also characterised by a free spirit (*voľný duch*),[315][316] which may be similar in some aspects to “broadmindedness”, but is characterised by greater depth, emotionality, abstraction and attachment to freedom in the broad sense.[317]

Taking the above into account, the principle of proportionality can be reduced to the so-called necessity test, which must consider the mentioned criteria. According to the practice of the ECtHR, there are two types of necessity tests: the absolute test and the persuasive test. In the case of the interference with the right to private life, the latter will apply, as it is more general, since it is based on the wider margin of appreciation.[318] The test is based on striking a balance between the right to private life and the interests of other stakeholders, and on assessing whether the means and the reason for the interference are sufficiently persuasive.[319]

Moreover, as Barancová indicates, in the context of employment relations, it is crucial that any interference with an employee’s right to privacy is conducted with full respect for the employee’s human dignity.[320]

Besides Article 11 of the Slovak Labour Code, which positions the protection of an employee’s personal data and respect for their private life as one of the basic principles of Slovak labour law, further on in the Labour Code, namely in §13 (4), the Slovak legislator indirectly indicated cases where employer interference in an employee’s privacy may be justified, thus creating the Slovak model of employee monitoring. Section 13 (4) reads: “An employer shall not, without serious reasons based on the specific nature of the employer's activities, invade the privacy of an employee at the workplace and in the common areas of the employer by monitoring the employee, recording telephone calls made by the employer's technical work equipment, and checking electronic mail sent from and delivered to the employee's work e-mail address without prior notice to the employee. Where an employer introduces a control mechanism, it shall discuss with the employees' representatives the scope of the control, the manner in which it is to be carried out and the duration of the control, and shall inform the employees of the scope of the control, the manner in which it is to be carried out and the duration of the control.”

Therefore, the regulation explicitly names two forms of monitoring, which might be applied by the employer: recording telephone calls made by the employer's technical work equipment,

[315] Judicial decision of the Constitutional Court of the Slovak Republic, I. ÚS 117/07 of 4 February 2009.
[316] Judicial decision of the Constitutional Court of the Slovak Republic, I. ÚS 274/05 of 14 June 2006.
[317] Free spirit or freedom of spirit is in fact a philosophical concept, present primarily in the Hegel’s concept of law - See more: Wilejczyk, 2009, pp. 11-21.
[318] Trykhlib, 2020, p. 134.
[319] See: ECtHR judgment in Odièvre v. France from 13 February 2003 (Application no. 42326/98).
[320] Barancová, 2019, p. 149.

and checking electronic mail sent from and delivered to the employee's work e-mail address. However, owing to the open term “monitoring of the employee” used in the provision, the scope of its application has been extended to forms that are not explicitly mentioned in it, such as camera surveillance, monitoring through the Global Positioning System (GPS), rankings of employees, some types of psychological testing, etc.[321]

Finally, when analysing the above regulation, it appears to be particularly vital to define the concept of “the serious reasons based on the specific nature of the employer’s activities,” as they are “the gateway” for the employer’s interference in the employee’s privacy. However, neither the Slovak Labour Code nor the Slovak courts, through their jurisprudence, define this notion. In practice, it is up to the employers themselves to decide what serious reasons, which are based on the specific nature of their activity, constitute a valid reason for introducing employee monitoring measures. Given how important the link between the serious reason and the specific nature of the employer’s activity is, it is necessary to consider how to interpret the concept of the employer’s activity, and more precisely, its specific nature. An extended analysis of this issue will take place in the second chapter of the thesis.

[321] Mesarčík and Poruban, 2023, pp. 458-459.

Chapter II. Objectives and Forms of Employee Monitoring

1. Employee Tasks

1.1. The Employer's General Right to Monitor the Usage of the Means of Production Under the Czech and Hungarian Workplace Monitoring Models[322]

When conducting a comparative legal analysis of workplace monitoring models implemented by the countries of the Visegrad group, with regard to the surveillance of tasks performed by employees during work, two very distinctive regulations emerge – Section 316 (1) of the Czech Labour Code[323] and Section 11/A (2) and (3) of the Hungarian Labour Code[324].

Section 316 (1) of the CLC states that "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 authorised to check compliance with the prohibition laid down in the first sentence in an appropriate way."[325] In turn, Section 11/A (2) of HLC provides as follows: "In the absence of a different agreement, the employee may use the information technology or computer technology device or system provided by the employer for work (hereinafter: computer technology device) exclusively for the purpose of fulfilling the employment relationship."[326] Moreover, Paragraph 3 of Section 11/A of HLC indicates that "During the inspection, the employer may look into data related to the employment relationship stored on the computing device used for the performance of the employment relationship."[327] Both regulations are remarkably similar and have the same effect, namely, they introduce a general right of the employer to check compliance with the established rule that, in the absence of the employer's consent or other agreement, employees may not use the means of production and other equipment belonging to the employer, provided to employees for the performance of their work, for private purposes.

---

[322] Based on this fragment, an article was prepared and published: Mirosławski, T. (2025) 'Between Casuistry and Vagueness – A Comparative Legal Analysis of Employer Surveillance of Employee Tasks under Polish and Czech Legislation', Central European Academy Law Review, 2(1), pp. 191-216.
[323] Hereinafter: CLC.
[324] Hereinafter HLC.
[325] Section 316 (1) of LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce" (Czech Labour Code).
[326] Section 11/A (2) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[327] Section 11/A (3) of Act of 2012 on the Labor Code (Hungarian Labour Code).

At first glance, it may seem that these provisions primarily serve to protect the employer's property, and that it is the property that will be the object of monitoring, rather than the tasks performed by employees.[328] Nevertheless, they should be viewed in a broader context in order to discover what effects they have in practice.

The Czech Supreme Court, in two of its judgments – of 16 August 2012 and of 7 August 2014 - in which it considered the nature of Czech regulations on employee monitoring, drew attention to a very important issue. First of all, it indicated that the first paragraph of section 316 of the Czech Labour Code concerns mainly the issue of the employer's property, while the second[329] and third paragraphs[330] touch on the protection of employees' privacy.[331] Following the position of the Supreme Court, Šmejkal stated that an employer's "check" – according to Paragraph 1 – does not constitute an infringement of the employees' privacy.[332] Nevertheless, this statement should be considered controversial, especially in light of the author's other considerations. Šmejkal indicates, that the monitoring under Paragraph 1 of the Section 316, 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.[333] Therefore, taking into account the court's findings and doctrinal considerations, it can be said that, in practice, Paragraph 1 of Section 316 of CLC serves primarily as a basis for the employer's surveillance of employee tasks. The same can be stated in the case of Hungarian regulation (Section 11/A (2) and (3) of the HLC), especially since there is no doubt that a correctly performed task should not involve misuse of the employer's property, which has been entrusted to carry out a specific work.

---

[328] Vobořil notes that and excessive emphasis on the protection of employer's property may lead to undesirable abuses. In many cases, the employer's genuine intention to monitor and emploee's personal information is concealed behind the argument of his or her property protection - See: Vobořil, 2012.
[329] Section 316 (2) of the CLC reads as follows: "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."
[330] Section 316 (3) of the CLC reads as follows: "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."
[331] Judgement of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011; Judgement of the Czech Supreme Court of 07 August 2014, 21 Cdo 747/2013.
[332] Šmejkal, 2019, p. 60.
[333] Šmejkal, 2019, p. 60.

1.1.1. The Employer's General Right to Monitor the Usage of the Means of Production Under the Czech and Hungarian Workplace Monitoring Models: Forms of Monitoring

If it has been established that Section 316 (1) of CLC and Section 11/A (2) in conjunction with Section 11/A (3) may constitute the basis for monitoring employees' tasks, it should be considered what form of monitoring Czech and Hungarian employers may use to monitor the performance of tasks by their employees, and what principles such form should comply with.

The very wording of Section 11/A (2) and (3) of the HLC indicates that forms of monitoring will be limited to so-called "communication monitoring"[334], i.e. how information technology or computer devices entrusted to or used by an employee for work are used, by checking data stored on computers, phones and other devices; checking the employees' internet activity, including the use of social media, checking the list of calls made from the working phones and monitoring work-related email.

On the other hand, the situation is significantly different in the case of Czech regulations. Section 316 (1) of CLC is very broad and, unlike the Hungarian regulation, does not implicitly restrict the forms of monitoring employees tasks by precisely specifying which devices employees may not use for their own purposes without the employer's consent, but only stating that this applies to all of the employer's means of production and other means necessary for the performance of work, including computer and telecommunication technology. Therefore, using a literal interpretation of the provision, it may seem that any form of monitoring aimed at determining in which manner employees performed tasks and whether this manner complied with the standard established by Section 316 (1) of CLC would be permissible. Nevertheless, due to the interpretative efforts made by the Supreme Court and the doctrine, this conclusion does not appear to be complete.

Regarding the Supreme Court's case law, the aforementioned judgment of 16 August 2012[335] issued 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,[336] is of key importance in the context

[334] Gyulavári, 2023, pp. 297-298.
[335] Judgement of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011.
[336] In a case, as a result of 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 (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

of considerations on the permissible forms of monitoring tasks performed by employees. In the judgment, the Court ruled that, contrary to the claimant's assertions, the monitoring carried out by the employer did not fall within the scope of Section 316 (2) of CLC and therefore could not have breached the information obligation established in Section 316 (3). Justifying its statement, the Court indicated that the employer did not intercept the employee's phone calls or check his emails and text messages (the measures designated in Paragraphs 2-3) during his inspection, but limited itself to checking whether the employee browsed websites not related to his work. The purpose of the employer's monitoring was solely to determine whether the employee complied (and if not, to what extent) with the prohibition on using the employer's computer and telecommunications equipment, for personal purposes, resulting from the law, considering the rules derived from the work regulations stating that "it is prohibited to use websites with dubious or sensitive content, as well as online news services, watching television via the Internet or listening to the radio via the Internet, which may overload the computer network and are not related to the performance of the agreed work".[337][338]

Following the jurisprudence, the doctrine indicated that one of the conditions for a given form of monitoring to be considered as pursuing the objective of Section 316 (1) of CLC and not exceeding the requirement of "appropriateness" is that the employer should refrain from using the monitoring measures listed in Section 316 (2) of CLC.[339] Nevertheless, this condition and the relationship between the first and second paragraphs of Section 316 of CLC provoke discussion. Morávek points out that 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, only this provision should apply if a method of surveillance other than those listed in Paragraph 2 (open or concealed monitoring, interception, and recording of telephone calls, checking of electronic mail or postal consignments addressed

qualification of the surveillance, whether it should fall under Section 316 (1) or (2) of CLC, and the legality of the dismissal became a matter of dispute.

[337] Judgement of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011.

[338] Moreover, the Supreme Court expanded its argument by point out that: "The aforementioned provision (Section 316 (2) of the CLC) applies primarily to cases of a specific nature of the employer's activity, and furthermore, it applies only to situations where the employee either uses the employer's production and work equipment for his or her personal needs with the employer's consent, or for some reason uses their own production and work equipment, including computer technology or telecommunications equipment (their own PC, laptop, mobile phone, typewriter, etc.) at the employer's premises, and to all items and actions (of a private nature) of the employee. In the case in question, the aim was to verify compliance with the prohibition set out in Section 316(1) of the Czech Labour Code, to which employer is entitled by law, rather than to monitor the employee's private activities." – See: Judgement of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011.

[339] Šmejkal, 2019, p. 61.

to employees) has been chosen. As an example of this type of monitoring, the author cites, *inter alia*, random checks carried out in real-time in ad-hoc cases.[340]

However, the above interpretation raises certain doubts, as it may lead to the conclusion that, since the list of monitoring measures listed in Paragraph 2 is exhaustive, an employer using other monitoring methods has absolute freedom to interfere with an employee's privacy. Such a conclusion must be considered incorrect, as its acceptance could lead to a disruption of the entire logical structure of the Section, the main pillar of which is the presumption that when monitoring is carried out within the framework established by Paragraph 1 of Section 316, an infringement of an employee's privacy cannot actually take place.[341]

We can therefore see that the catalogue of forms of monitoring tasks performed by employees falling under Section 316 (1) can be broad and depends largely on the specific situation. In the case of Hungary, this list has been limited by specifying the categories of devices and systems used to perform work,[342] and by specifying that monitoring should be limited to the inspection of data related to the employment relationship that is stored on these devices.[343]

1.1.2. The Employer's General Right to Monitor the Usage of the Means of Production Under the Czech and Hungarian Workplace Monitoring Models: General Principles

Nevertheless, in the case of both the Czech Republic and Hungary, in order to determine in detail what forms of employee monitoring are permissible, it is necessary to consider what general principles they should comply with. In both countries, such rules stem more from doctrinal considerations, jurisprudence, or guidelines issued by national data protection authorities than from explicit legislative provisions.

In the case of Hungary, what should be noted first is that, in connection with Section 11/A (3) of HLC, the legislator decided to define the notion of "data related to the employment relationship" in a specific way. Namely, it stated that it should be considered data necessary to check compliance with the rules on using equipment dedicated to performing work, established on the basis of Section 11/A (2) of HLC.[344] Thus, the scope of monitoring depends on what is

[340] Morávek, 2017, p. 578.
[341] Šmejkal, 2019, p. 62.
[342] Section 11/A (2) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[343] Section 11/A (3) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[344] Section 11/A (4) of Act I of 2012 on the Labor Code (Hungarian Labour Code).

specified in these rules. If the employer and the employee have reached an agreement that the employee may use specific devices belonging to the employer and used for work for private purposes, then the limit of monitoring is to determine whether the employee complied with the provisions of the agreement.[345] This finding takes on particular significance in the context of the fact that an employer may also conduct the monitoring of communications when, in accordance with a relevant agreement between the employer and the employee, the employee uses his or her private equipment for work.[346] On the other hand, if no agreement regarding the private use of working equipment has been concluded and private use is therefore prohibited, the employer may monitor the data stored on a specific IT/computer device, but only to the extent that allows them to determine whether the data is of a private or professional nature.[347]

Further and more detailed information about the principles of how communication monitoring, and consequently, employee task monitoring, should be carried out is provided by guidelines and case-law of the Hungarian DPA[348].[349] Regarding this issue, NAIH published two documents of significant value: 1. Recommendation on the Basic Requirements for Electronic Monitoring Systems Used in the Workplace, and 2. Information on the Basic Requirements for Data Processing in the Workplace. The former document primarily concerns video monitoring (conducted by CCTV cameras) and was issued in 2013, while the latter refers to an extensive catalogue of the means of monitoring, including video monitoring, monitoring of employees' e-mail and internet use, monitoring of the use of company mobile phones, GPS monitoring, and even monitoring conducted through the biometric systems, and dates from 2016. Given the subject matter of this section, particular attention should be paid to the second document.

In the Information on the Basic Requirements for Data Processing in the Workplace, NAIH emphasises that the development of the technology has influenced the evolution of employee monitoring, expanding it with new technical means and serves as a guide for employees and employers to help them understand what kind of requirements and principles should apply to

---

[345] Lukács, 2021, p. 216.
[346] Section 11/A (5) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[347] T/4479. számú törvényjavaslat az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról (2019), p. 102.
[348] A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH).
[349] The case law of Hungarian courts in cases concerning workplace monitoring is not very extensive. Therefore the doctrine is based primarily on practice, guidelines and recommendations of the Hungarian DPA. – See: Bankó and Szőke, 2016, pp. 53–69; In 2005, Szabó and Székely pointed out that the low number of judgments in this area may be due to employees' concerns about the costs, length, and unpredictability of court rulings, which is why they prefer to turn to the DPA to protect their rights. Despite the passing of more than two decades, the situation has not changed much, and it is still the DPA that plays the main role in resolving issues realted to the protection of employees' personal data - See: Szabó and Székely, 2005, p. 119.

data processing related to work, especially to employer control.[350] According to the NAIH, the principles that apply to the monitoring of communications are primarily the principles of purpose limitation, necessity and proportionality, as well as the principle of transparency, which is not directly indicated but derives from the content of the document.

The principle of purpose limitation is set out in Section 10 (1) of HLC. According to this principle, an employer may only process employee data that is necessary for the establishment, performance or termination of the employment relationship.[351] The practical implication of this principle is that the employer must clearly and unambiguously specify the purpose of data processing before the data is recorded. The purpose should be specified sufficiently to indicate what kind of data processing operations must be undertaken to achieve it. In this regard, the employer is obliged to specify in advance the scope of data requested from employees and inform them about it. When data that is not necessary to achieve a specific purpose (one of the three indicated in Section 10 (1) of HLC) is requested from employees, this situation constitutes an unjustified infringement of their privacy and their right to freely dispose of their personal data. Furthermore, if processed for different purposes, each of these purposes must be defined individually, and if the purpose changes during processing, it must be redefined.[352] Therefore, if the original purpose of processing employees' data was to monitor their tasks, and subsequently the employer wants to use this data to compile statistics and analytical data and present them, for example, during the training sessions, this purpose must be clearly defined before commencing monitoring.

The principle of limited purpose is related to the principle of transparency. The NAIH points out that in the context of communication monitoring (within which the Hungarian DPA distinguishes: monitoring of company e-mail, monitoring of work computers, monitoring of internet usage and monitoring of work mobile phones), the first step an employer should take is to develop an appropriate internal policy on the use of devices made available to employees for work purposes.[353] Such internal regulations should specify the rules for using the work equipment (whether it is allowed to use a specific device for private purposes, and are useful means of informing the employees about their obligations, the rules for potential monitoring, and the purpose of data processing.

---

[350] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 1.

[351] The employer may require the employee to make a statement or disclose personal data that is relevant to the establishment, performance, termination (cancellation) of the employment relationship or the enforcement of claims arising from this Act – Section 10 (1) of Act I of 2012 on the Labor Code (Hungarian Labour Code).

[352] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, pp. 4-5.

[353] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 25, 28, 30, 31.

A well-designed policy on the use of work devices and workplace monitoring serves as a preventive measure, which can protect employees from monitoring and excessive interference in their privacy, and protect employers from disputes with employees.[354] The NAIH, as a good practice against misuse of information and computer equipment entrusted to employees, recommends regular reminders about the rules for using work devices, e.g. in the context of a company e-mail, these could be notifications informing employees not to send private messages from a professional account.[355] Similarly, with regard to phones and computers, the employer could use pop-up windows indicating that the use of certain types of applications, programmes or downloading private files is not permitted. When it comes to internet use, reminders about websites that employees should not visit can certainly be beneficial, but the most effective method would be to block such websites within the WiFi network at work or on a specific device, so that employees cannot physically access them.

Policies will vary to a certain extent depending on the type of device and, consequently, the form of monitoring. In the case of company e-mails and computers, the policies should also regulate the creation and retention of backup copies of the e-mail account and data saved on the computer. It should also cover the issue of permanent deletion of messages and data.[356] When it comes to the usage of the Internet by employees, the employer's internal regulation should, *inter alia*, indicate which websites are prohibited from browsing at work.[357]

However, given the negligible practice of employers introducing appropriate internal regulations[358] and the rather frequent cases of employees failing to comply with specific rules for using computer and information equipment at work, it is extremely important to develop an appropriate mechanism for monitoring how employees perform their tasks, primarily because such monitoring involves the processing of personal data.

First of all, it should be stated that monitoring measures have their limits, determined primarily by the principle of proportionality. As indicated by the practice of the ECtHR, the principle of proportionality is arguably the most important principle in the context of analysing workplace monitoring, as it allows to understand its exact form, how it should be carried out, what is permitted within its framework, and what is not.[359] The principle means that monitoring measures used must be proportionate to the intended objective, i.e. they may only be used if

[354] Kártyás, Répáczki and Takács, 2016, p. 67.
[355] The NAIH refers to such measures in realtion to company e-mail, but there is no obstace to extending similar solutions to other equipment - See: A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 26.
[356] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 26, 28.
[357] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 30.
[358] Kártyás, Répáczki and Takács, 2016, p. 67.
[359] See more in: Barański and Mirosławski, 2025, pp. 177-204.

they actually enable the protection of the employer's interests and rights at risk. In addition, the scope of data covered by monitoring should be as limited as possible. Due to the fact that the private life of employees is not limited only to the non-work sphere but also extends to the workplace and professional activities,[360] the employer should take this into account when conducting monitoring and limit it only to controlling activities and data closely related to the work performed. Monitoring must be carried out with respect for human dignity and must not be intended to intimidate, humiliate or harass employees, nor may any of these actions result from it.[361] In a nutshell, it can be said that monitoring must be applied in such a way as to properly balance the interests and rights of the employer and the employee.

The NAIH points out that in order for personal data protection to be properly enforced and for monitoring to interfere with employees' privacy to the least extent possible, the workplace monitoring system should be designed in a gradual manner. In practice, it means that, for example, in the case of monitoring of company email, the initial focus should be put on the e-mail address of the addressee or the sender and on the subject title of the message. Sometimes, only this amount of information allows to decide whether the email was used for private purposes against the rules, without the need to enter the content of the email. In order to impose consequences under labour law, further investigations are usually not necessary. This is particularly important in situations where private use is permitted either completely or under specific conditions.[362] It should be stressed that, irrespective of whether an employee has been permitted to use company email for private purposes and informed in advance about possible monitoring, employers are not entitled to access private messages. Such correspondence remains protected under the rights to privacy, personal data protection, and the confidentiality of communications - safeguards which extend not only to employees but also to third parties.[363]

The Hungarian DPA expresses a corresponding analogous position also in the case of other forms of monitoring of employees' tasks. For instance, in the case of Internet use monitoring, if the employer has restricted access to specific websites and wishes to verify whether the employee has performed his or her duties properly, without misusing working time and in accordance with the established rules, it is sufficient for the employer to familiarise with the URLs of the websites, rather than conducting a thorough investigation of what the employee

[360] This view was first expressed by the ECtHR in its judgment from 16 December 1992 in Niemietz v. Germany (Application no. 13710/88) and contributed to a fundamental change in the understanding of employees' right to privacy, particularly with regard to workplace monitoring.
[361] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 6.
[362] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 26.
[363] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 27.

was doing on those website.[364] The NAIH's position should be considered valid, as such detailed monitoring could lead to the acquisition by the employer sensitive data about the employee, such as information about their political views, religious beliefs, health status or sexual orientation. Moreover, guidelines regarding Internet monitoring have a significant practical implication, as cases concerning this issue have already been heard by Hungarian courts. In one such case, an employee was using his and his colleague's office computer to visit pornographic websites during working hours. Based on his actions, he was dismissed from work on disciplinary grounds. The Hungarian Supreme Court adjudicated in that case that the extraordinary termination of the employment relationship was lawful, because, as the employee who held an important position, his conduct violated essential obligations, thereby exposing his employer to damage.[365]

With regard to the computers used by employees, the employer may only note that the employee has stored his or her private data or files on the computer, contrary to the prior agreements made between the parties to the employment relationship. The employer should not open the files and monitor their exact content. In a situation where a laptop may be used for private purposes, private files should be clearly separated from work data, e.g. by creating appropriate folders or partitions on the hard drive.[366]

A similar solution may be applied in the case of an employee using a telephone provided to him or her by the employer. If the employer agrees that the telephone may also be used for private purposes, NAIH recommends, as a good practice, the use of two numbers, one for business calls and the other for private ones. This allows the employer to access data on the business calls without endangering the employee's privacy.[367] The employer is also entitled to obtain billing records from the telephone service provider containing details of calls made from the telephone. However, private numbers should be concealed on such documents so that the employer cannot acquire information about who the employee called for private reasons, for what purpose and when.[368]

Once the employer has identified the professional data, thereby ensuring the employee's privacy, the employer can proceed to a more detailed analysis. Nevertheless, in accordance with the principle of proportionality, monitoring should also apply in this situation to the narrowest

[364] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 31.
[365] Decision of Kúria (Curia, Supreme Court of Hungary), BH2006.64. See also: Kártyás, Répáczki, Takács, 2016, p. 67; Ásványi, 2022, p. 271; Petrovics, 2021, pp. 46-61.
[366] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 28-29.
[367] Such solutions are no available due to, among other things, the development of e-SIM card technology.
[368] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 32.

possible group of data related to an employee's potential specific misconduct.[369] For example, data monitoring should be limited only to internet browsing history, telephone calls or messages sent during a particular period of time, or only to files related to a concrete client or project.

It should also be remembered that the lawfulness of monitoring depends on the employer fulfilling his or her information obligation, according to which, prior to the commencement of monitoring, the employer must inform the employee about:

- the purpose and interest of the employer in relation to which a specific form of monitoring is carried out;
- which entity or person is authorised to carry out the monitoring on behalf of the employer;
- a precise monitoring procedure developed in accordance with the requirements of "graduality";
- what rights and remedies are available to employees in relation to monitoring.[370]

Interestingly, the DPA has not recommended any form of communicating the above information to employees, so it can be assumed that this may be a customary practice adopted at a given employer. On the other hand, considering the wording of Section 11/A (1) of HLC, in which the legislator specified the written form of information provided to an employee in connection with the monitoring of his or her behaviour related to the employment relationship by technical device, and the desire to maintain consistent model of monitoring in the workplace, and also taking into account the effects of monitoring on individual employees, it should be highly recommended that the information provided in connection with Section 11/A (2) and monitoring of employee tasks also be in written form. In addition, efforts should be made to ensure that the employee understands that their actions undertaken in the realm of performing employment relationship may be monitored and on what terms this will take place, as only under this condition, the actual objective set by the principle of transparency might be achieved. Nevertheless, achieving complete understanding is exceedingly challenging due to the complexity of the information, especially in the case of more advanced forms of monitoring, and due to the competencies of the employee, which in many cases do not strictly cover the technical and legal knowledge about the subject of surveillance and processing of personal data.[371]

---

[369] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 27.
[370] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 27, 30, 31, 32.
[371] More on transparency in the context of workplace monitoring and different appraoches to this principle (contextual and universal), in: Molè, 2022, p. 92-99.

The final requirement that NAIH points out when establishing the entire monitoring procedure is to guarantee the presence of an employee during monitoring, if specific circumstances allow it.[372] This requirement is to a certain extent justified by the fact that Hungarian labour law does not apply the presumption that correspondence in a company email account or files stored on a company computer does not contain private information about the employee or third parties.[373] Therefore, the presence of the employee and their prior review of messages, files, websites or other types of data before the employer accesses them may protect the employer from violating the privacy of the employee and third parties.[374]

An extraordinarily important and distinctive feature of Hungarian regulation on workplace monitoring, setting it apart from other Visegrad Group countries, is that it directly addresses the increasingly common trend in the workplaces known as “Bring Your Own Device”[375][376]. This trend is often presented as positive for employees, as it can lead to increased mobility and flexibility, which in turn contributes to greater productivity and job satisfaction.[377] It is also beneficial for employers, as it shifts the burden of purchasing and maintaining equipment onto employees, which is reflected in significant cost savings. As indicated by research conducted by Kártyás, Répáczki and Takács, the use of personal devices for work purposes is relatively widespread in Hungary.[378] On the other hand, it should be stated that the BYOD phenomenon, sometimes referred to as a strategy,[379] which better reflects its nature, also carries significant risks. From the employer’s point of view, the main challenge is security and protection of business-critical data. This type of data, stored on employees’ private devices, can easily be disclosed or transferred to competitors; moreover, the devices themselves can get lost or stolen. Therefore, employers should implement appropriate internal policies to protect devices and the data they contain.[380] When introducing a BYOD strategy in a company, a key element should be the implementation of a Mobile Device Management[381] system, which enables remote

[372] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 10.
[373] Lukács, 2021, p. 216, 219.
[374] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 27.
[375] Hereinafter: BYOD.
[376] BYOD can be considered as a philospohy that allows employees to use their own IT and computer devices for work purposes and submit them to monitoring by the IT department or, more generally, their employer - See: Chountalas and Karagiorgos, 2015, p. 2.
[377] Bankó and Szőke, 2016, p. 26; Chountalas and Karagiorgos, 2015, p. 3.
[378] According to research by Kártyás, Répáczki and Takács, 45% of respondents indicated that they use their own digital devices for work purposes. When asked about the type of devices they use, employees most often mentioned smartphones (46,8%), computers (39,6 %) and mobile phones (34%) - See: Kártyás, Répáczki and Takács, 2016, p. 68.
[379] See, e.g.: https://belltechlogix.com/bring-your-own-device-strategy/ (Accessed: 3 May 2026).
[380] Chountalas and Karagiorgos, 2015, p. 4.
[381] Hereinafter: MDM.

control over devices, their monitoring and the wiping of sensitive data in the event of their loss.[382] On the other hand, this strategy also entails enormous risks for employees, specifically for their privacy. BYOD contributes to blurring the line between private and professional life.[383] Private and professional data blend and become increasingly difficult to separate, which, in the event of monitoring, may result in numerous misconducts and excessive interference with the privacy of employees and third parties.[384] The described issue is visible and becomes relevant in the context of Section 11/A (5) of HLC, which states that employer monitoring also applies to private devices belonging to employees if, based on an agreement with the employer, such devices are used to perform work.[385] Nevertheless, the problem is not merely theoretical, as it has been addressed in the jurisprudence of the Hungarian Supreme Court, which, in its judgement of 5 June 2020, drew attention to the requirements that must be met for such monitoring to be considered lawful. The judgment was issued in a case concerning the employer's monitoring of personal data, including text messages and emails, stored on the mobile phone, which was the employee's private property. The employer based its monitoring entitlement on the fact that the phone was equipped with a SIM card belonging to the employer and that the employee gave consent to hand over the phone to the employer. The Supreme Court ruled that the processing of the employee's private data by the employer was against the law. The Court justified its decision by stating that the employer should have provided the employee with detailed information on the technical measures which are going to be used during the monitoring of data stored on the mobile phone. Only after receiving such information can an employee give fully conscious and valid consent. If the employer considers that it is necessary to gain access to private data as well, it first has to explain to the employee the relationship between these data and the employment relationship. It is important to note that the methods of monitoring must always be proportionate to their aim, and employees should be provided with adequate safeguards against abuse.[386]

In the case of the Czech model of employee tasks monitoring and general rules with which the monitoring should comply, the aforementioned Supreme Court judgment of 16 August 2012 should be referred to again, in which the Court expressed an immensely important position, paving the way for the interpretation of Paragraph 1 of Section 316 of CLC. Namely, it stated that monitoring cannot be exercised by the employer in a completely arbitrary manner, since

[382] Sarzyński, 2016, p. 72; Gajar, P. K., Gosh, A. and Rai, S., 2013, p. 66.
[383] Kártyás, Répáczki and Takács, 2016, p. 72.
[384] Bankó and Szőke, 2016, p. 27.
[385] Section 11/A (5) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[386] Judgment of Kúria (Curia, Supreme Court of Hungary), Mfv. 10.397/2018/2., BH 2020. 48.

the employer is entitled to exercise such control only in an "appropriate way".[387] In this position, the Court referred to the literal wording of the provision under discussion, in which the Czech legislator, unlike the Hungarian one, decided to define the frames of permissible monitoring not by designating categories of data that may be the object of monitoring (in the Hungarian Labour Code, these are data related to the employment relationship stored on the computing device used for the performance of the employment relationship[388]), but by generally defining the manner in which monitoring should be carried out as "appropriate". Nevertheless, "appropriateness" carries with it an element of significant subjectivity, which in the context of monitoring still involves a risk of arbitrariness, resulting in a possible violation of employees' privacy. Therefore, it would seem logical for the legislator to define the notion of "appropriate way" or specify the characteristics that would make monitoring "appropriate". However, the Czech legislator refrained from doing so, which resulted in action on the part of the judiciary. The Supreme Court noted that the lack of a legal definition of the term "appropriate way" makes Paragraph 1 of Section 316 of the CLC a legal norm with a vague and abstract hypothesis. It means that the task of defining the hypothesis has been left to the courts, which should do this on a case-by-case basis, at its own discretion, taking into account a wide and, so far, unrestricted range of circumstances. In most cases, the courts will examine "whether monitoring was continuous or subsequent, its duration, scope, whether and to what extent it restricted the employee in his or her activities, whether and to what extent it also violated his or her right to privacy, etc."[389] Moreover, the Court ruled that the object of the surveillance can only be to determine whether the employee has violated the absolute prohibition on the use of the employer's equipment for private purposes, as specified in the Labour Code, or, in the event of a different agreement with the employer, whether the employee complied with his obligations and rules specified therein. According to the Court, only monitoring conducted in such a manner can be considered appropriate and lawful under Czech labour law regulation.[390]

On the grounds of the analysed judgment, the doctrine, identifying the conditions which monitoring measures applied by the employer should meet in order to comply with the requirement of "appropriateness" under Section 316 (1) of CLC, defined, besides the aforementioned condition that the employer should refrain from using the employee surveillance measures specified in Section 316 (2) of CLC, as second such condition as "the

[387] Judgement of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011.
[388] Section 11/A (3) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[389] Judgement of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011.
[390] Judgement of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011.

restriction of the scope and extent of monitoring, including the exclusion of the possibility to check the exact content of non-work ‘activities’ undertaken by employees during work[391][392] (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.)

However, there is also a critical approach in the doctrine to the interpretation of workplace monitoring in light of Section 316 (1) of CLC presented by the Supreme Court. Vobořil argues that it is rather difficult to agree that limiting monitoring to only 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, etc. Moreover, it is questionable whether supervising internet activity is a proportional method of checking under Paragraph 1 of Section 316 of CLC. There are different and more adequate ways to check the performance of tasks entrusted to employees and 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.[393]

Considering the above, it should be pointed out that Paragraph 1 of Section 316 of CLC creates an extremely vague legal framework and can be interpreted in various ways. Under no circumstances does it constitute a safe harbour for Czech employers, as some authors label it,[394] but rather a seal full of hidden dangers. This is particularly illustrated by the view expressed by the Czech Supreme Court, according to which this provision states a norm with an abstract hypothesis, leaving its determination to judicial discretion.[395] This, in turn, creates a risk of excessive judicial activism, which in the context of employment relations and workplace monitoring is especially problematic, as it makes the rules less comprehensible for the average addressee and weakens legal certainty for both employers and employees.[396]

[391] Šmejkal, 2019, p. 61.
[392] See also: Štefko, 2016, p. 15.
[393] Vobořil, 2012.
[394] Šmejkal, 2019, p. 60.
[395] Judgement of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011.
[396] Morávek, 2017, p. 584.

1.2. The Employer's General Right to Monitor the Usage of the Means of Production Under the Slovak and Polish Workplace Monitoring Models[397]

In contrast to the Hungarian and Czech models of employee monitoring, provisions such as Section 11/A (2) and (3) of the HLC and Section 316 (1) of the CLC, which stipulate that, unless otherwise agreed between the parties of the employment relationship or unless the employer has given consent,[398] equipment made available to employees to perform work may not be used for private purposes, are not reflected in the Slovak and Polish models.[399]

However, looking at Article 11 of the Slovak Labour Code, one may consider whether this provision could be used to derive a general right for employers to check how employees use the items provided to them for work, similar to that expressed in the Hungarian and Czech models of monitoring. The provision states that "employers may collect personal data on employees only when these relate to the qualifications and professional experience of employees and data that may be significant for the work that employees are expected to carry out, carry out, or have carried out."[400] The article in question is subject to very broad doctrinal analysis, which combines the right to personal data protection expressed in the aforementioned regulation with the right to privacy of employees.[401] In defining privacy, Slovak doctrine follows the direction set out in the case law of the ECtHR, indicating that the right to privacy means "personal privacy (the personal sphere of the individual, i.e., data concerning gender identification, name, sexual orientation, and sex life), as well as the right of every human being to establish and develop relationships with other human beings (of a private and professional

[397] Based on this fragment, an article was prepared and published: Mirosławski, T. (2025) 'Between Casuistry and Vagueness – A Comparative Legal Analysis of Employer Surveillance of Employee Tasks under Polish and Czech Legislation', Central European Academy Law Review, 2(1), pp. 191-216.
[398] At this point, it is worth noting one more interesting issue arising from the Hungarian and Czech regulations referred to above. Namely, the nature of the norms contained therein. When considering Section 316(1) of the CLC, there is no doubt that the Czech legislator has given the norm resulting from this provision a semi-imperative character, as the employer, by giving his consent, can only improve the employee's situation by allowing him to use the entrusted equipment for private purposes, either partially or completely. However, there is a certain inconsistency in the Hungarian regulation. Provision 11/A (2) HLC allows the parties to conclude an agreement regulating the private use of equipment entrusted for work, which would indicate the dispositive nature of the norm. However, the later part of the provision states that in the absence of such an agreement, an employee may use the entrusted equipment solely for the purpose of fulfilling his or her employment relationship. This construction therefore leads to a situation in which an agreement between the parties can only lead to a more favourable regulation of the employee's situation by liberalising the prohibition on private use, which in turn indicates the rather semi-imperative nature of the norm. It should therefore be concluded that the norm resulting from provision 11/A (2) HLC, despite being formulated as a dispositive norm, through its practical effects corresponds rather to a semi-imperative norm.
[399] Barancová, 2016, p. 41.
[400] Article 11 of the Slovak Labour Code.
[401] Švec, Toman, Olšovská, Žuľová, et.al., 2023, Čl.11.

nature, i.e. a kind of zone of interaction between an employee and other persons)."[402] However, it should be remembered that an employee's right to privacy is not absolute, and its limits are determined by the professional activities performed for the employer. Therefore, when an employee is performing work-related tasks, the confidentiality of his or her correspondence or telephone conversations will be significantly limited. Within the framework of the employment relationship, a certain relationship arises between the rights of the employee and the interests and rights of the employer. On the one hand, there is the right of employees to protect their privacy, but on the other hand, this right is counterbalanced by the employer's right to monitor and control the employee's work performance and the right to ensure adequate protection of its own property.[403] As an example of limiting an employee's right to privacy, in a commentary by Švec, Toman, Olšovská, Žuľová, et.al. in the section devoted to Article 11 of the Slovak Labor Code,[404] reference is made to the judgment of the Slovak Supreme Court of 12 September 2016, in which the court ruled that in order to verify an employee's compliance with work discipline, the employer has the right to monitor private e-mails sent during working hours from a computer assigned to the employee for the purpose of performing work tasks.[405]

However, these considerations, although extremely detailed and accurate, cannot lead to the conclusion that Article 11 provides a legal basis for the employer's general right to check whether an employee is using the equipment entrusted to him for private purposes, as explicitly regulated in the Czech and Hungarian labour codes. This is primarily due to the character that the Slovak legislator gave to this article by placing it in the part of the code entitled "Fundamental Principles (*Základné Zásady*)." These principles cannot be treated as equivalent to the subsequent sections of the code, as they constitute the core foundation of Slovak labour law,[406] and their main purpose is to create an interpretative framework for resolving ambiguities arising from further provisions of the labour code.[407]

Therefore, Section 13 (4) of the Slovak Labour Code will be the legal basis for workplace monitoring of various sorts, including monitoring of employees' tasks. In addition to the rules embodied in this provision, monitoring should also comply with the principles of legality,

[402] Švec, Toman, Olšovská, Žuľová, et.al., 2023, Čl.11.
[403] Švec, Toman, Olšovská, Žuľová, et.al., 2023, Čl.11.
[404] Švec, Toman, Olšovská, Žuľová, et.al., 2023, Čl.11.
[405] Ruling of the Slovak Suprme of 12 September 2016, n. 3Cdo/233/2015.
[406] It can even be said that they constitute a specific axiology of Slovak labour law.
[407] Mesarčík and Poruban, 2023, p. 457.

legitimacy, and proportionality derived by doctrine and jurisprudence from Article 11 of the SLC.[408]

1.3. The Concept of Serious Reasons/Cause Arising From the Specific Nature of the Employer's Activity within the Slovak and Czech Workplace Monitoring Models[409]

Section 13 (4) of the SLC states that "an employer shall not, without serious reasons based on the specific nature of the employer's activities, invade the privacy of an employee at the workplace and in the common areas of the employer by monitoring the employee, recording telephone calls made by the employer's technical work equipment, and checking electronic mail sent from and delivered to the employee's work e-mail address without prior notice to the employee. Where an employer introduces a control mechanism, it shall discuss with the employees' representatives the scope of the control, the manner in which it is to be carried out and the duration of the control, and shall inform the employees of the scope of the control, the manner in which it is to be carried out and the duration of the control."[410] This section to a large extent resembles Section 316 (2) and (3) of the Czech Labour Code. However, they cannot be considered identical.

Both of the regulations as a condition for the employer to interfere with the employee's privacy through monitoring, identify serious reasons arising from the specific nature of the employer's activities.[411] However, unfortunately, neither of the labour codes defines what serious reasons are exactly and how to interpret the specific nature of the employer's activities. This leads to a situation where it is unclear which employers are authorised to introduce monitoring measures in the workplace – all of them, or only those who conduct particularly hazardous activities. Furthermore, many employers mistakenly assume that any serious reason for introducing employee monitoring is related to the specific nature of their activity.[412] Therefore, it is necessary to determine what content these notions encompass. Both Slovak and Czech legal doctrine have undertaken this task, albeit with slightly different approaches.

---

[408] Mesarčík and Poruban, 2023, pp. 458-459; Ruling of the Slovak Suprme of 12 September 2016, n. 3Cdo/233/2015; Švec, M., Toman, J., Olšovská, A., Žuľová, J., et.al. 2023, Čl.11.
[409] Based on this fragment, an article was prepared and published: Mirosławski, T. (2025) 'Between Casuistry and Vagueness – A Comparative Legal Analysis of Employer Surveillance of Employee Tasks under Polish and Czech Legislation', Central European Academy Law Review, 2(1), pp. 191-216.
[410] Section 13 (4) of the Slovak Labour Code.
[411] In Slovak: "*vážne dôvody spočívajúce v osobitnej povahe činností zamestnávateľa"* and in Czech: "závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele".
[412] Greguš, 2017, p. 233.

Within the realm of the Slovak doctrine of labour law, the main focus is on the concept of the activity of the employer, considering its broad and narrow dimensions. When it comes to the broad sense, it can be understood as the activity which appears in the relevant publicly available register or founding document of the employer. On the other hand, in a narrower sense, the employer's activities are specific activities carried out by the employer, employees, contractors, etc.[413] In the context of Section 13 (4) of the SLC, the employer's activity should be interpreted in the narrower sense, and its specific nature relates primarily to the specific work activities performed by employees.[414]

Once the interpretative framework for the notion of the specific nature of the employer's activity is set, it is desirable to look at the concept of a serious reason to be based on such activity. In the literature, the following are cited as serious reasons that may justify interference with employee privacy in the workplace through monitoring: protection of employer and employee property, control of the work performed by employees, optimisation of costs and taxes, streamlining of production and improvement of occupational health and safety.[415]

A position, to a certain extent, convergent with the interpretation of Slovak doctrine was expressed by Šimečková, referring to paragraph 2 of Section 316 of the CLC. The author indicates that Section 316 (2) of the CLC should not be interpreted in a way that only employers involved in specific hazardous activities may exercise the monitoring powers granted to them by law. She claims that the basis for implementing surveillance measures is to ensure compliance with health and safety rules, protect the life and health of employees, protect property belonging to the employer or employee, and monitor productivity. These grounds apply to every employer, and that is why every employer may find justification to use the measures listed in paragraph 2 of Section 316 of the CLC.[416]

Nevertheless, Czech doctrine is quite diverse and also includes views that are contrary to those expressed in Slovak labour law doctrine or by Šimečková. For instance, in one of its publications on the protection of employees' personal rights and the protection of the employer's property interests, the Czech State Labour Inspectorate[417] pointed out that "a serious reason/a serious cause" is generally not applicable in the production of ordinary products or the

[413] Beierová, 2017, p. 265.
[414] Greguš, 2017, p. 233.
[415] Greguš, 2017, p. 233.
[416] Šimečková, 2021, p. 95.
[417] Státní Úřad Inspekce Práce (hereinafter: SUIP).

supply of ordinary services.[418] Therefore, paragraph 2 of Section 316 of the CLC does not apply to all employers, regardless of their field of activity.

There is also a third approach presented by Šmejkal, critical toward the SUIP opinion - stating that such a straightforward answer does not provide good guidance for the doctrine – and towards Šimečkova – negating that Section 316 (2) of the CLC may apply to any employer. Drawing on the relevant literature[419] and the position of the Office for Personal Data Protection[420], Šmejkal argues in favour of adopting a "situational analysis," which, in his view, provides a more accurate framework for assessing circumstances that justify heightened or exceptional need for workplace monitoring.[421] Within this framework, he identifies several situations that may justify a proportionate interference with an employee's privacy: a) the processing of substantial amounts of cash; b) when workplaces are subject to special regulations, such as those involving highly sensitive or classified information[422]; c) the work is performed in the environments with an elevated risk of accidents, explosions, or similar hazards, for example, in the nuclear power plants, mines, steelworks, etc.[423]; d) there occurs a significant need to protect intellectual and industrial property rights, safeguard valuable knowledge and third-party personal data,[424] and to uphold equal treatment and non-discrimination.

When analysing the above positions, the interpretation expressed in Slovak literature on the subject and that presented by Šimečkova on the grounds of Czech labour law should definitely be endorsed. This conclusion is based on a comparative legal analysis of Section 13 (4) of the SLC and Section 316 (2) of the CLC, the wording and meaning of which are close. Considering that Section 13 (4) of the SLC is in practice the only basis in substantive law for the use of monitoring measures by Slovak employers, limiting this provision only to employers whose activities relate to areas of special hazard would be clearly inappropriate, as it would restrict most employers in the performance of their basic organisational function and the related control function, and in some cases also their obligations in the field of health and safety at work.

Although under Czech labour law, the provision in question does not constitute the sole basis for monitoring applied by employers, like in the case of Slovakia, its nature differs from

[418] Státní Úřad Inspekce Práce, 2019, p. 3.
[419] See: Zemanová Šimonová, 2016; Vych, 2015; Jouza, 2022.
[420] Hereinafter: UOOU.
[421] Šmejkal, 2019, p. 74.
[422] Zemanová Šimonová, 2016.
[423] Vych, 2015.
[424] Jouza, 2022.

that of the mentioned and described paragraph 1 of Section 316 of the CLC. Section 316 (2) of the CLC, as well as Section 13 (4) of the SLC, is primarily intended to enable monitoring that is appropriate to the activities carried out by a specific employer and justified by their needs arising from such activities. However, it should be noted that these needs must be serious and not every reason on the employer's side can justify monitoring. In most cases, according to the above considerations, serious reasons should therefore be classified as those that fall within the scope of the employer's organisational and controlling functions and their responsibilities to ensure adequate health and safety standards.

Furthermore, the Slovak doctrine also raises an extremely important and pertinent remark regarding the discussed issue. Namely, it states that, as the notion of "serious reasons" is not specified in the legal provisions, such reasons should be indicated in the employer's internal regulations, and employees should be informed about them. Thus, if one of the reasons occurs, employees can reasonably and foreseeably expect interference with their privacy, which in turn leads to the fulfilment of the duty to notify employees, which is one of the conditions for the permissibility of such interference.[425] Such action on the part of the employer may have a preventive effect, on the one hand protecting employees from excessive invasion of their privacy, and on the other hand limiting their actions that could be contrary to the employer's interests.

Although the observation was made on the basis of Slovak law, it can be treated as good practice in relation to both countries, given the close similarity between Section 13(4) of the SLC and Section 316(2) of the CLC. Moreover, in the Czech monitoring model, as in the Slovak one, the legislator also expressed an information obligation, which could be at least partially satisfied by regulating the issue of "serious reasons" in the employer's internal regulations.

Concluding the discussion on the concept of "serious reasons", it should be noted that the position expressed in Slovak labour law doctrine to include such reasons in employers' internal regulations is in line with the calls for employers to introduce internal polices on the use of electronic devices and workplace monitoring, which are present in international discussions[426] and strongly emphasised among the Visegrad Group countries by the Hungarian DPA[427] and labour law doctrine[428].

[425] Barancová, 2016, p. 47.
[426] See e.g.: Recommendation CM/Rec(2015)5.
[427] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 25, 28, 30, 31.
[428] Kártyás, Répáczki and Takács, 2016, p. 67.

1.4. Forms of Monitoring[429]

Further analysis of the compared regulations leads us to the forms of monitoring expressed in both provisions. Both regulations specify forms of monitoring that can be used to monitor employees. Some of these standards overlap, at least partially, while others do not. In the following section, the emphasis will be mainly on so-called communication monitoring, understood as the monitoring of telephone calls, company e-mail and other electronic communication, as this is mentioned in both monitoring models. At this point, Polish regulations should also be included in the comparative legal analysis, as one of the basic forms of monitoring on which the Polish model is based is the monitoring of an employee's company email. The Hungarian regulation on this subject, i.e. Section 11/A (2) and (3) HLC, was analysed at the beginning of the subchapter and compared with Section 316 (1) CLC, as the nature of both provisions expressing the so-called "general right of the employer to check" provided a much more appropriate basis for comparative legal research. The Hungarian regulation will be addressed again in the analysis covering the so-called "beyond communication"[430] forms of monitoring.

1.4.1. Communication Monitoring

Within the category of communication monitoring, commonly used by employers, the Polish model refers explicitly only to the monitoring of an employee's company e-mail account, unlike the Slovak or Czech models, which, in addition to monitoring of e-mail accounts, also provide for the monitoring of employees' telephone conversations. Before moving on to detailed considerations on the forms of monitoring, it is first necessary to draw attention to the element that distinguishes the Polish model from all four models of workplace monitoring adopted in the Visegrad Group countries. Namely, the Polish regulation defines in the most direct and, to a certain extent, clear manner the prerequisites that must be met for the monitoring of electronic mail to be considered lawful. While Slovak and Czech legislators set serious reasons arising from the specific nature of the employer's activities as a condition for employer interference

[429] Based on the sections of this fragment concerning Poland and the Czech Republic, an article was prepared and published: Mirosławski, T. (2025) 'Between Casuistry and Vagueness – A Comparative Legal Analysis of Employer Surveillance of Employee Tasks under Polish and Czech Legislation', Central European Academy Law Review, 2(1), pp. 191-216.
[430] The categorisation of communication monitoring and "beyond communication" forms of monitoring is used by Gyulavári – See: Gyulavári, 2023, p. 298.

with the privacy of employees, *inter alia,* through monitoring their e-mail accounts, which is an exceptionally open notion and problematic in terms of interpretation, as proven above, and on the other hand, on the basis of the Hungarian monitoring model, email monitoring falls under the so-called general right of the employer to check whether the equipment assigned to the employee is being used properly (for work and not for private purposes), the Polish legislator indicates that the employer may introduce monitoring of the employee's company email 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 work tools made available to the employee[431]. Considering that the conjunction "and" (pol. *i*) is used between the indicated prerequisites, they must be fulfilled cumulatively. The construction of this provision indicates the legislator's intention to ensure a high standard of protection of employee privacy against excessive interference by the employer.[432] The Personal Data Protection Office indicated that on this ground, the employer can control the activity of his employees while they are at his or her disposal at the workplace.[433]

Moving on to a detailed comparative legal analysis of employee email monitoring, the Slovak perspective will be addressed first.

Primarily, it is important to note that the reference in Section 13 (4) of the SLC to the employer's ability to monitor electronic mail sent from and delivered to the employee's work email address stems from the fact that an employee may not use resources entrusted to him or her by the employer for private purposes, such as paper or electronic correspondence.[434]

Slovak labour law doctrine places strong emphasis on distinguishing between work-related and private email correspondence. The prevailing view is that, as a rule, private correspondence has no place in the workplace and during working time, unless the employer has provided the employee with a "company" email account for private use. Authors such as Križan[435] and Siskovičová[436] refer to Morávek's statement that it can even be assumed that correspondence or e-mails received at work are primarily work-related, unless there are reasons to believe otherwise.[437] From this position, it can be concluded that the employer is entitled to open and

[431] Art. 22^3 §1 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[432] Otto, 2023, p. 409.
[433] Urząd Ochrony Danych Osobowych, 2018a, p. 34.
[434] This follows form Section 81 of the SLC, according to which employee is obliged to work responsibly and properly, and to follow the instructions of superiors issued in accordance with legal regulations; to utilise the working time for assigned work; to adhere to legal regulations and other regulations relating to the work he or she performs, if he or she was properly informed about them; and to properly manage the resources entrusted to him or her by the employer and to protect the employer's property against damage, loss, destruction and abuse, and not to act in contradiction to the justified interests of the employer. – Section 81 (a)(b)(c)(e) of Slovak Labour Code.
[435] Križan, 2016, p. 267.
[436] Siskovičová, 2015, p. 66.
[437] Morávek, 2013, 2.1.2.2 E-mail pro osobní potřebu.

check the content of "work-related" emails anytime.[438] However, this approach seems too far-reaching. Firstly, it ignores the changes currently taking place in the sphere of employment, which are leading to a blurring of the boundaries between the private and professional spheres.[439] Secondly, it does not take into account the concept of employee privacy, which has emerged from the case law of the ECtHR, which indicates that employee privacy may, in certain situations, also extend into the professional sphere and include the element of building a so-called social identity at work, i.e., the opportunity to establish contacts with other people.[440] Thirdly, and most importantly, it appears that this approach does not in any way refer to the employer's information obligation as set out in Section 13(4) of the SLC. Particularly questionable is the employer's virtually unrestricted access to the content of an employee's emails, even if they are of a business nature. In this regard, it is worth mentioning the valid position of the Hungarian DPA, which stated that due to the possibility of violating the employee's privacy, the content of the message should be opened in specific cases and only after ascertaining the nature of the message. The employer should first limit itself to checking the subject of the message, its sender and recipient, etc.[441] On the other hand, despite appearing to agree with Morávek's position, Slovak doctrine also indicates that if the characteristics of a message clearly indicate that it is private, the employer has no right to open and analyse it,[442] which seems to bring it closer to a more balanced solution.

Certainly, the situation may change significantly if the employee is not at the workplace and the employer has an urgent need to obtain information stored in the employee's company email account. In such circumstances, it should be considered that the employer is entitled to directly access the content of the messages in the mailbox, although if any of the messages turn out to be of a private nature, the employer should immediately stop reviewing them.[443]

At this point, it is worth mentioning the ruling of the Slovak Supreme Court of 12 September 2016, which was instrumental in setting legal standards covering the monitoring of employees' official[444] email correspondence.[445] In the ruling, the court adjudicated on the invalidity of the termination of employment. The analysis of the case should begin with a brief

[438] Križan, 2016, p. 267.
[439] This refers to phenomena and trends such as remote work and the use of personal devices for work purposes, known as "bring your own device."
[440] ECtHR judgement of the ECtHR in Bărbulescu v. Romania from 12 January 2016 (Application no. 61496/08), 70; ECtHR judgment in Niemietz v. Germany from 16 December 1992 (Application no. 13710/88), 29.
[441] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, pp. 26-27.
[442] Križan 2016, p. 268.
[443] Siskovičová, 2015, p. 67; Morávek, 2013, 2.1.2.2 E-mail pro osobní potřebu.
[444] "Offcial" means not private but belonging to a particular company or institution.
[445] Ruling of the Slovak Supreme Court of 12 September 2016, n. 3Cdo/233/2015.

overview of the facts of the case, according to which an employee who was a senior official at the Slovak Ministry of the Interior was dismissed on disciplinary grounds because he used his official computer, e-mail address, the name of the ministry and its symbols for private purposes and for his own benefit. Moreover, the employee was warned and knew that the employer’s internal regulation allows employees to use e-mails for performing their work and prohibits the use of work computers and official email addresses for private purposes. When adjudicating the case, the Supreme Court ruled in favour of the employer and indicated that the employer’s decision to dismiss the employee because of the serious breach of work discipline was justified. Nevertheless, due to the subject matter of the thesis, particular attention should be paid to the Supreme Court’s reasoning, in which it discusses the issue of email monitoring and refers to the question of privacy in the workplace.

The Court held that the employees’ right to privacy in the workplace takes on a slightly different character than the ordinary one expressed by the individual in the fully private sphere; however, even when employees are required to perform work tasks, they do not lose their right to privacy. In its ruling, the Supreme Court highlights the existence of the conflict between employees’ right to privacy and the employer’s interest, which is reflected in the entitlement to know how employees perform their work and duties, how they respect the specific prohibitions and restrictions, and how and for what purposes they use electronic communication using technology owned by the employer. According to the Court, it is obvious that if the employer prohibits employees from using assigned computer equipment for private purposes in internal regulations, he or she must have adequate means of checking compliance with such a prohibition, and in the event of a breach of the prohibition, they must be able to verify the extent of such a breach. The employer is also entitled to obtain evidence considering the employee’s behaviour against the prohibition. When conducting such a check, the employer may reasonably assume that e-mails which are received and sent by the employee from the official e-mail box are of a work-related nature. If the employer, during his monitoring activity, discovers that the employee’s electronic communication is of a private nature, this should be considered as a secondary infringement of the employee’s privacy.[446]

The Slovak Supreme Court's ruling was also greatly influenced by the case law of the ECtHR, specifically the case Bărbulescu v. Romania. However, it should be mentioned that the Supreme Court referred to the first decision in this case, which was later reviewed by the Grand Chamber and resulted in a contrasting judgment.

[446] Havrilla and Sanak, 2017, p. 91.

In the first judgment in the case Bărbulescu v. Romania, the ECtHR adjudicated that the monitoring of a particular employee's communications during working hours on a computer used for the performance of official duties, with respect for the principles of legality, legitimacy and proportionality, is not contrary to Article 8 of ECHR.[447] Therefore, the Slovak Supreme Court followed the interpretation of ECtHR and stated that

"For the purpose of verifying whether the employee is complying with work discipline, the employer, respecting the principles of legality, legitimacy and proportionality, is also entitled to monitor private electronic mail sent and received from the computer assigned to the employee for the performance of his/her work tasks. Moreover, while adhering to these principles, evidence submitted by the employer (e-mails) in proceedings concerning the invalidity of the termination of employment cannot be considered inadmissible."[448]

In the analysed case, the Slovak Supreme Court pointed out that the monitoring of the employee's e-mail was not continuous and covered the appropriate scope of correspondence necessary for the employer to determine how the employee used the working tool entrusted to him. It should therefore be concluded that the employer complied with the principle of proportionality. Furthermore, the employee was informed that the computer equipment entrusted to him, including email, could only be used for work purposes and that private use was prohibited. Additionally, it should be noted that a similar position regarding the monitoring of an employee's work-related email account was expressed by the Regional Court in Bratislava in case no. 6Co/203/2012.[449] In its judgment, the court rejected the claimant's allegation that the termination of his employment was unlawful because the defendant (employer) had violated the principles of privacy protection in the workplace by monitoring the employee's work-related email account without giving the employee adequate notice. In the court's opinion, the claimant used the laptop entrusted to him and the company email account not only for work and business communication, but also to send messages containing undesirable information about the employer to external parties, thereby exposing the employer to damage and breaching his duties. In justifying its position, the court pointed out that the very nature of a company laptop and email account means that they can only be used for work-related purposes; therefore, it is not necessary to inform employees about the prohibition on using them for private matters or

[447] ECtHR judgement in Bărbulescu v. Romania from 5 September 2017 (Application no. 61496/08).
[448] Ruling of the Slovak Supreme Court of 12 September 2016, n. 3Cdo/233/2015.
[449] Judgement of the Regional Court in Bratislava of 29 October 2012, n. 6Co/203/2012.

about the possibility of monitoring them. However, it seems that such a view is too far-reaching, especially from the present perspective.[450] Firstly, unlike the Czech and Hungarian workplace monitoring models, the Slovak one does not provide for a general prohibition on the use of equipment entrusted to employees for private purposes. Secondly, the current legal status imposes an information obligation on the employer as one of the conditions for lawful monitoring,[451] and thirdly, this position is contrary to the jurisprudence of the ECtHR. In *Copland v. UK*, the Strasbourg Court addressed the issue of an employee's expectation of privacy and explicitly stated that if an employee has not been warned that his or her telephone calls will be monitored, they have a reasonable expectation of privacy that such calls will not be monitored, and the same applies to emails and use of the internet.[452]

Considering the above and observing the current discussion on the admissibility and grounds for monitoring in the workplace, it is interesting to note that the Supreme Court did not indicate that one of the prerequisites for the admissibility of workplace monitoring is prior notification to the employee of the possibility of monitoring his or her conduct. However, it should be borne in mind that the significance of this prerequisite was only established by the Grand Chamber's judgment in the Bărbulescu v. Romania case. The Grand Chamber indicated that it is a necessary condition for the admissibility of employee monitoring, as it significantly affects the so-called reasonable expectation of privacy in the workplace. Among other things, due to the absence of this prerequisite, the ECtHR in its second judgment in the case ruled in favour of the employee.[453]

It should also be emphasised that the act regulating the employment relationship, which formed the basis of the case examined by the Slovak Supreme Court, was the State Service Act, which at that time was silent on the issue of monitoring in the workplace and the prerequisite of prior notice,[454] which was clearly reflected in the judgment. However, given the importance attached to the case law of ECtHR by the Slovak judiciary and labour law doctrine, it could be expected that, following the publication of the Grand Chamber judgment in the Bărbulescu v. Romania case, also the practice of the Slovak courts, especially the Supreme Court, would change. Unfortunately, at this point, there is no example we could use to analyse such a change, but nevertheless, the new approach is inevitable. As Beierová indicates, the Slovak courts,

[450] Barancová, 2016, pp. 50-51.
[451] Article 13 (4) of the Slovak Labour Code.
[452] ECtHR judgment in Copland v. the United Kingdom from 3 April 2007 (Application no. 62617/00), 42; ECtHR judgment in case Halford v. the United Kingdom from 25 June 1997 (Application no. 20605/92), 45.
[453] Grand Chamber of the ECtHR in Bărbulescu v. Romania from 5 September 2017 (Application no. 61496/08).
[454] Mesarčík and Poruban, 2023, pp. 464.

which will adjudicate on the issues of interference with an employee's privacy and the monitoring of electronic communications by employer, currently have a comprehensive legal basis provided by the European Convention on Human Rights, the case law of the ECtHR and the Constitutional Court of the Slovak Republic and when deciding should consider all the principles and criteria derived from the given legal norms and case law.[455]

In contrast to the approach apparent in the example of the Slovak model of monitoring of employees' email accounts, it seems that the interpretation developed by the national DPA and the doctrine for the purposes of Polish regulations covering email monitoring is more consistent with the standards set by the case law of the ECtHR.[456]

Firstly, it should be noted that email monitoring is a form of monitoring that constitutes a specific limitation of the freedom and privacy of communication. This is highly significant, as this value is protected at a constitutional level.[457] The Polish legislator, demonstrating this characteristic feature of this form of monitoring, indicated that its use should not violate the confidentiality of correspondence and other personal rights of employees.[458] The wording of the regulation entailed the need to define precise limits within which the monitoring of employees' email correspondence may take place.

On the basis of a literal interpretation of Article 22^3 of the PLC, which, in some respects, resembles Slovak regulation,[459] it should be noted that only company email accounts used by employees to perform their duties may be monitored, but under no circumstances may private inboxes be subject to monitoring.[460] According to the Polish Personal Data Protection Office, the control of private correspondence is completely prohibited;[461] thus, if a private message is found in a business email account, it cannot be checked. This kind of situation may occur in particular when an employer authorises an employee to use the company's email account for private purposes. The acquisition by the employer of data concerning the employee's private life as a result of monitoring such an email account will constitute a violation of employee informational privacy.[462]

Nevertheless, it is crucial to devote some attention to considerations regarding the nature of email monitoring, especially in the context of the adequacy of this form in relation to the

---

455 Beierová, 2017, p. 267.
456 Otto, 2023, p. 409.
457 Art. 49 of the Constitution of the Republic of Poland of 2nd April 1997, Dz. U. No. 78 Item 483.
458 Art. 22^3 §2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
459 Both regulations explicitly state that monitoring refers to "official" email accounts. Slovak legislation refers to "employee's work email address", while the Polish uses the term "employees' business electronic mail."
460 Kuba, 2019, p. 34.
461 Urząd Ochorny Danych Osobowych, 2018a, p. 35.
462 Otto, 2023, p. 409; Urząd Ochorny Danych Osobowych, 2018a, p. 35.

premises for its admissibility. Although these considerations are based on the Polish monitoring model, the conclusions drawn from them can be applied to all workplace monitoring models discussed in the thesis.

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).[463] 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.[464] This position should be considered justified, since business email is rarely the only tool for providing work, and its control involves a high risk of violating the employee's privacy. Therefore, the monitoring of it may be insufficient and, in some cases, even too severe to fulfil the premises of this form of surveillance.

Regarding the establishment of the objectives, the scope, the manner of use and the information obligation connected to email monitoring, the legislator has stated that the provisions of Article 22^{2} §6-10, originally belonging to the part regulating video monitoring, shall apply accordingly.[465] Therefore, their details will be discussed later in the chapter; however, it should be mentioned at this point that the considerations and conclusions made on the basis of these provisions in the context of camera surveillance will also apply to the monitoring of business emails.

Monitoring employees' company email accounts is also a frequently used form of workplace monitoring among Czech employers.[466] However, despite its widespread use, it appears that the level of employee privacy protection guaranteed by the provision regulating this monitoring measure is lower than in Poland or Slovakia. When introducing the possibility of monitoring electronic mail into the Labour Code, the Czech legislator did not refer, as the Polish legislator did, to the requirement to respect constitutional values such as the confidentiality of correspondence and respect for other personal rights,[467] nor did it explicitly state, as in the case under Slovak law, that only company email accounts used for work by employees may be monitored[468].

[463] Kuba, 2019, p. 31.
[464] Kuba, 2019, p. 31.
[465] Art. 22^{3} §3 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[466] Kolářová, 2017; Šmejkal, 2019, p. 82.
[467] Art. 22^{3} §2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[468] Section 13 (4) of the Slovak Labour Code.

Nevertheless, a literal interpretation of Section 316 (2) of the CLC,[469] which directly mentions the possibility of email monitoring (and also of traditional post), does not convey its full meaning, and in order to find it, it is necessary to depart from it, in favour of a systemic interpretation.

In the Charter of Fundamental Rights and Freedoms, which is part of the Czech constitutional system, Article 13 clearly states that both electronic and traditional correspondence are confidential.[470] However, this rule is not absolute. Derogations from it are possible if it is indicated in law. One such exception is the aforementioned Section 316 (2) of CLC, which permits the monitoring of electronic and paper mail addressed to an employee if it is necessary for important reasons related to the employer's nature of business activity. Nevertheless, this does not mean that the employer is entitled to conduct such monitoring in an absolutely arbitrary manner.[471]

The Czech Data Protection Authority, seeking to clarify how email monitoring in the workplace can be carried out, issued Standpoint No. 2/2009, in which it indicated that the key criterion for distinguishing between employees' private and work email accounts is the form of the email address.[472] This means that if an email address consists of the name of a specific department within the employer and the employer's domain, e.g. production@companyXYZ.cz, then such an email account should be considered a company account, which may be subject to employer surveillance (including viewing the content of messages contained in such a mailbox).[473] On the other hand, if the email address takes the form of a first name, surname and employer domain, e.g. jan_procházka@companyXYZ.cz, then it should be assumed that the emails stored in such an account are private, and therefore the employer cannot access their content. Instead, the employer may check the number of emails that have been received and sent from such an account, their titles and in exceptional cases, who the recipient of the email is.[474]

Recognising the form of an email address as a crucial factor in distinguishing between private and work-related messages in a given email inbox is an approach characteristic only of

[469] Section 316 (4) of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".
[470] Article 13 "Listina Základních Práv a Svobod" of the Czech Charter of Fundamental Rights and Freedoms of 16 December 1992 (Const. act No. 2/1993 Coll. as amended by constitutional act No. 162/1998 Coll.) reads as follows: "No one may violate the confidentiality of letters or other documents and records, whether kept privately or sent by mail or other means, except in cases and in the manner prescribed by law. The confidentiality of messages transmitted by telephone, telegraph, or other similar means is similarly guaranteed."
[471] Potyková, 2018/2019, p. 59.
[472] Úřad pro ochranu osobních údajů, 2009.
[473] Štěpánková, 2025, p. 329.
[474] Potyková, 2018/2019, p. 60.

the Czech personal data protection authority and has not been expressed in any of the other three national workplace monitoring models.

Although this approach is simply to apply in practice and considered by some authors to ensure a high level of protection of privacy[475] and confidentiality of employee correspondence, it has at one point been severely criticised as inflexible and incompatible with the development of employee privacy standards, primarily due to the extensive monitoring capabilities of company email accounts, which, despite the "top-down" assumption that they only contain work-related messages, may in practice also contain private messages to which the employer should not have access.[476]

As a result of growing criticism, the mentioned approach was rejected and replaced by a more balanced and complex one. The form of the email address itself ceased to be decisive, and instead of the entire inbox, the emphasis shifted to individual messages. The employer should assess the characteristics of a given message – whether it is work-related or private – based on its features that are visible without opening it, like subject, sender, and recipient. The form of the address itself took on a rather auxiliary function in relation to the features mentioned above.[477]

Furthermore, in the new approach, great importance began to be attached to the concept of serious reasons found in Section 316 (2) of CLC, indicating that the employer may only interfere with the content of the messages, open and read them, if the condition of the serious reasons consisting in the nature of the employer's activity is met.[478] Such a situation may arise when non-performance of a specific task could expose the employer to serious harm, e.g., when an employee falls ill, and a replacement is needed. However, it should be remembered that the employer's access to the employee's emails in the company mailbox should not last longer than is necessary.[479] In a situation where an email that did not initially appear to be private turns out to be private upon reading, the employer should immediately stop interference with it. Further reading or opening emails whose characteristics indicate their private nature constitutes a violation of the employee's privacy.[480]

In Czech doctrine, much like in Polish, certain concerns are expressed regarding email monitoring, primarily in relation to the principle of proportionality of intervention in employee

[475] Potyková, 2018/2019, p. 60.
[476] Štěpánková, 2025, p. 329.
[477] Morávek, 2012, pp. 178-179.
[478] Morávek, 2017, p. 583.
[479] Šmejkal, 2019, p. 82.
[480] Morávek, 2012, p. 178.

privacy. As in Poland, it has been pointed out that, in general, this form of monitoring can be very intrusive and does not necessarily fulfil its original purpose, whereas in the Czech Republic it is pointed out that in the event of an employee's absence from work, a better solution than reviewing all emails in his or her mailbox may be to set up an autoresponder that will provide the senders with all the necessary information about who the message should be forwarded to and inform them of the employee's absence without giving any further details. However, it should be noted that this approach also has its limitations, and there may still be situations where it is necessary to monitor and interact with emails stored in an employee's company mailbox.[481]

1.4.2. Beyond Communication Monitoring

When analysing the forms of monitoring that can be used by employers to oversee the tasks performed by employees, in addition to communication monitoring, forms of monitoring that go beyond communication should also be considered. In the context of monitoring employee tasks, the form of monitoring beyond communication that should be focused on is primarily camera monitoring, also known as video monitoring or CCTV[482] monitoring.

Video surveillance is present in each of the four workplace monitoring models in the Visegrad Group countries. Under the Polish model, the legal basis for such monitoring is Article 22^2 of the Polish Labour Code.[483] In the Czech Labour Code, the possibility of using this type of monitoring stems from Section 316 (2).[484] In turn, under the Slovak labour law, camera monitoring has not been explicitly mentioned in the law, but it falls within the broader catalogue of monitoring practices derived from Section 13 (4) of the Slovak Labour Code.[485] In the Hungarian model, this form of monitoring is also not explicitly mentioned, but the possibility of its use by the employer stems from Section 11/A (1) of the Hungarian Labour Code.[486]

A comparative legal analysis of camera surveillance should begin with general considerations regarding the premises for the use of such monitoring, as this form of surveillance, due to its nature, can be used not only to monitor the tasks performed by employees, but also for other purposes.

[481] Štěpánková, 2025, p. 330.
[482] Closed Circuit Television.
[483] Art. 22^2 §1 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[484] Section 316 (2) of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".
[485] Section 13 (4) of the Slovak Labour Code.
[486] Section 11/A Subsection 1of Act I of 2012 on the Labor Code (Hungarian Labour Code).

According to the Polish model of workplace monitoring, 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*.[487] 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. On the basis of the "production control 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.[488] In accordance with the principle of purpose limitation of data processing, expressed on the one hand in Article 5(1)(b) of the GDPR and on the other hand in Article 22^2 (3) of the Polish Labour Code, monitoring should only be used for the purposes specifically indicated in law. Therefore, when considering the premise of "production control", a narrower interpretation should be advocated, which has been, in fact, confirmed by the Polish DPA[489]. The purpose of video monitoring used for production control is primarily to identify irregularities in the production process and products, as this enables the employer to take appropriate corrective and preventive measures. Thus, it appears that camera monitoring cannot be used to monitor employees' behaviour, their interactions with customers, the way in which they perform their tasks, etc.[490]

In the realm of the Slovak workplace monitoring model, similarly to the rest of the analysed models, video monitoring has, at some point, emerged as a response to technological developments in the labour market that influence employment relations.

Nevertheless, in contrast to the Polish model, the Slovak legislator did not specify in labour law provisions the specific purposes for which camera monitoring should be introduced. It only indicated that the premise for introducing this form of monitoring is the existence of serious reasons based on the specific nature of the employer's activities, as discussed earlier. Slovak labour law doctrine identifies two groups of "serious reasons" that employers use to justify the use of CCTV monitoring. The first group focuses on monitoring employee performance and work efficiency. Monitoring is used to observe whether employees are fulfilling their tasks and duties, and how they are using their working time. This group also includes the possibility of

[487] Art. 22^2 §1 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[488] Dąbrowska, 2019, p. 16.
[489] Urząd Ochorny Danych Osobowtch, 2018b, p. 20.
[490] Miłosz and Świątek-Rudoman, 2019, p. 34.

monitoring whether employees comply with the prohibition on consuming alcohol and other psychoactive substances in the workplace. The second group, on the other hand, includes reasons such as protecting the employer's property and ensuring appropriate health and safety standards.[491] However, a common situation that appears in practice is that the employer, while actually pursuing the objectives indicated in the first group of "serious reasons", introduce and use video monitoring, referring to reasons belonging to the second group, thus concealing the real purpose of the monitoring,[492] which is contrary to the principle of purpose limitation under Article 5(1)(b) of the GDPR.[493] This situation aptly illustrates the dual, panoptic effect of video surveillance in the workplace. On the one hand, cameras are used for "protection," a purpose often portrayed as legitimate or even commendable; on the other hand, they function as tools of control and a subtle form of coercion over employees.[494]

Similar to the Polish model of workplace monitoring, where one of the premises for video monitoring is "production control", under the Slovak model, consideration is given to whether the employer's desire to check work performance is a sufficient rationale for using a CCTV system in the workplace. This issue has also been considered by the European Data Protection Supervisor[495]. EDPS, in its guidelines on video-surveillance, states that excessively intrusive monitoring systems may reinforce unnecessary stress among employees and undermine their trust towards the employer. Given this, it should be noted that the use of video monitoring to check how employees perform their work should, in principle, be avoided. However, there may be specific cases where the interest deriving from monitoring significantly outweighs the need to respect employees' privacy. Furthermore, the EDPS pointed out that objectives such as managing work efficiency, ensuring quality control, enforcing the internal policies or providing evidence for dispute resolution, should not, in themselves, be considered as grounds for justifying the use of video monitoring in the workplace.[496] The Slovak labour law doctrine follows the EDPS position and also indicates that monitoring employees with cameras solely for the purpose of checking work efficiency is impermissible, which is consistent with the

[491] Siskovičová, 2015, p. 58.
[492] Škvarková, M. (2017) 'KAMEROVÝ SYSTÉM NA PRACOVISKU VS. PRÁVO ZAMESTNANCA NA SÚKROMIE' in Barancová, H., Olšovská, A. (eds.), *Pracovné právo v digitálnej dobe*, Prague: Leges, p. 203.
[493] Art. 5 (1)(b) of the GDPR.
[494] The panoptic effect caused by video monitoring in the workplaces is only part of a wider phenomenon, having its roots primarily in the camera surveillance systems used by local and national authorities in public places – See also: Kovanič, 2020, p. 351-354.
[495] Hereinafter: EDPS
[496] European Data Protection Supervisor (2010), p. 22.

position expressed, e.g. by Miłosz and Świątek-Rudoman[497] within Polish labour law doctrine and by the Polish DPA[498].

In terms of objectives or prerequisites for video monitoring, the Czech model is remarkably similar to the Slovak one. Also, in contrast to the Polish provisions, it does not specify the purposes for introducing camera monitoring, but indicates that it depends on the emergence of a serious cause consisting of the employer's nature of activity.[499] Just like the Slovak legislator, the Czech legislator also has not defined what constitutes a serious cause consisting in the employer's nature of activity, which has led to extensive doctrinal considerations, which have already been resolved in an earlier section of this thesis.

However, it should be noted that, according to Morávek's position, the provision of Section 316 (2) of CLC, which forms the basis for CCTV monitoring, may be used to protect the employer's property and to monitor the performance of employees' tasks.[500] Nevertheless, the notion of "a serious cause consisting in the employer's nature of activity" essentially coincides with the so-called legitimate interest premise resulting from Article 6(1)(f) of the GDPR, which has significant practical implications. First and foremost, this means that before implementing camera monitoring, the employer must analyse the necessity of introducing this form of monitoring in relation to the intended monitoring objectives. In practice, this means that the employer must weigh up the importance of their interest related to the use of monitoring against the interests or rights of the persons who will be monitored. Camera monitoring may only be implemented if the employer's interests outweigh those of the employees.[501]

Given the need to conduct a proportionality test and the similarity between the Czech and Slovak CCTV monitoring models, it can be concluded that, in accordance with the position of the EDPS,[502] under Czech, as under Slovak labour law, the sole premise of monitoring only for the purpose of checking the performance of work performed by employees is, in principle, insufficient.

The Hungarian legislator, while regulating the issue of camera monitoring within the workplace, has taken a different path from those outlined in the previously discussed monitoring models and has indicated that employees may only be monitored in terms of their behaviour

---

[497] Miłosz and Świątek-Rudoman, 2019, p. 34.
[498] Urząd Ochorny Danych Osobowych, 2018b, p. 20.
[499] Section 316 (2) of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".
[500] Morávek, 2020), p. 20.
[501] Miłosz and Świątek-Rudoman, 2019, p. 34.
[502] European Data Protection Supervisor, 2010, p. 22.

related to the employment relationship.[503] The literature indicates that video monitoring aimed at employees' behaviour in relation to their employment primarily serves to protect and ensure the economic interest of the employer.[504] However, an employer's interest can be viewed in two ways.

Firstly, the employer's interest lies in monitoring the performance of work by employees. Such monitoring focuses primarily on checking whether employees perform their tasks and duties properly. The objectives pursued by the employer in the case of such monitoring are mainly the efficiency of the company's operations and its profitability. Such monitoring is treated as an employer's entitlement resulting from the nature of their business activities, as it enables the introduction of new solutions and technologies that improve performance and productivity.[505]

Secondly, the employer's interest is embodied in the protection of the property and individuals involved in the process of work. In order to achieve this objective, monitoring focuses on supervising employees' compliance with occupational health and safety standards. Such monitoring may also lead to the protection against crimes committed in the workplace.[506] This objective of monitoring stems, in a sense, from the employer's obligation to ensure appropriate working conditions.[507]

Given the above, we see a certain analogy between Hungarian, Czech and Slovak regulations. In all three models of camera surveillance, the specific objectives of this form of surveillance have not been explicitly specified. However, in the doctrinal considerations made on the basis of each of the three regulations mentioned, two main fields, which can also be perceived as objectives, emerge: 1. monitoring of tasks performed by employees and monitoring of property.

Furthermore, as in the case of Poland, Slovakia and the Czech Republic, questions also arise within the Hungarian workplace monitoring model regarding the scope of the employees' tasks monitoring premise.

Within the Hungarian monitoring model, immense importance is attributed to the value of human dignity, which sets a sort of boundary for the scope and permissible objectives of CCTV monitoring.[508] The interplay between respect for human dignity and camera monitoring was

---

[503] Section 11/A Subsection 1 of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[504] Lukács, 2017, p. 98.
[505] Lukács, 2017, p. 99.
[506] Miller and Weckert, 2000, p. 260.
[507] Lukács, 2017, pp. 99-100.
[508] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013), p. 5.

determined, among others, by the Hungarian Constitutional Court in its decision 36/2005.(X.5.). The Court stated that “the use of cameras as a technical means of protecting property is suitable for safeguarding property, but it can inevitably also be directed at individuals, human behaviour, habits, expressions, and even the human body itself. Electronic monitoring is therefore capable of invading privacy and recording intimate (sensitive) situations, even without the knowledge of the person concerned or without them being in a position to consider the permissibility of such recordings and their consequences. In addition to violating the right to privacy, such monitoring may also affect the right to human dignity in a broader and deeper sense. The essential conceptual element of privacy is precisely that others cannot intrude into it or look into it against the will of the person concerned. If unwanted intrusion does occur, not only the right to privacy itself, but also other elements of human dignity, such as the freedom of self-determination or the right to physical and personal integrity, may be violated.”[509]

In this regard, the Hungarian DPA pointed out that the installation of cameras whose sole purpose is to monitor employees is unacceptable. Furthermore, a monitoring system, the purpose of which, even if not its primary purpose, is to influence employees' behaviour at work, must be considered unlawful.[510] This position has also been confirmed by doctrine. Ásványi, following Hungarian case law, points out that CCTV monitoring which targets only one employee and his or her activities, and which violates human dignity, should be considered inadmissible in the workplace.[511] In turn, Gyulavári also emphasises that video monitoring must not violate human dignity and points out that the sole purpose of this form of surveillance can be to control the performance of work.[512]

When analysing the Hungarian model of camera monitoring and the position expressed by the Hungarian DPA and doctrine, it should be noted that, clearly, the purposes served by this form of monitoring play an important role in considerations regarding the admissibility of monitoring; however, the most important factor determining whether a particular case of CCTV monitoring is lawful is the manner in which it is applied and, above all, whether its application does not clash with human dignity.

1.4.3. Covert Monitoring

[509] Decision of Hungarian Constitutional Court (Alkotmánybíróság) 36/2005.(X.5.), par. III (2).
[510] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013, p. 5; A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 23-24.
[511] Ásványi, 2022, p. 273.
[512] Gyulavári, 2023, p. 299.

A major point of divergence between the workplace monitoring models in the Visegrad Group countries, specifically between the Czech model and the rest, is the issue of covert monitoring.

Under Polish, Slovak and Hungarian labour law, although some voices are calling for such a possibility to be introduced into the labour codes,[513] covert monitoring, regardless of its form, is currently inadmissible, primarily due to the employer's information obligation, which must be fulfilled before the launch of the monitoring. The argument that covert monitoring is unacceptable in the context of the three workplace monitoring models is confirmed both in the doctrine[514] and in jurisprudence[515].

The situation is radically different in the case of the Czech model of workplace monitoring. The Czech Labour Code explicitly expresses the possibility of the application of concealed monitoring by an employer.[516] However, such regulation raises the question of how to combine the possibility of using covert monitoring with the information obligation existing in the Czech model. The doctrine indicates that in such a situation, information obligation prior to the start of the monitoring is, as a rule, to a certain extent restricted.[517] Nevertheless, it should be completely fulfilled, but in an *ex-post* manner, after the monitoring was carried out.[518] It is also pointed out by some authors that the employer should inform employees of the possibility of monitoring before it begins; however, without providing any further details, including the method and timing.[519] This solution seems rather artificial owing to the fact that during any future conflict in the workplace, the employee will figure out that the collected evidence of his/her misconduct was an outcome of covert monitoring.[520]

1.4.4. Monitoring Principles

After discussing the fundamental issue of the premises/objectives of monitoring, further comparative analysis will focus on the territorial scope of monitoring, retention period, and

[513] Škvarková, 2017, p. 212-213.
[514] Barański, M. 2018, p. 48; Urząd Ochrony Danych Osobowych, 2018b, pp. 25-26; Škvarková, 2017, p. 212; Barancová, 2016, p. 54; Greguš, 2017, p. 243; Štefko, 2016, p. 15; A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 25.
[515] Judgement of the Polish Supreme Administrative Court of 13 February 2014, I OSK 2436/12.
[516] Section 316 (2) of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".
[517] Štěpánková, 2025, p. 324.
[518] Sehnálek, 2023, p. 260.
[519] Morávek, 2020, pp. 26; Štěpánková, 2025, p. 324.
[520] See more in: Šmejkal, 2019, p. 76.

information obligation. On the grounds of these aspects, even more differences between workplace monitoring models in the Visegrad Group countries will be revealed.

1.4.4.1. Territorial Scope of Monitoring

Beginning 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.[521]

Looking at the Polish regulation within the labour code, it can be considered that it complies with these principles. It defines the general area of monitoring, the sites that should be excluded from the video monitoring and regulates the possibility of derogating from the general prohibition in specific cases.[522]

The provisions regulating CCTV monitoring indicate that it may cover not only the workplace, but also the area surrounding it.[523] It can therefore be concluded that monitoring may cover places where work is not performed, but its surveillance remains closely related to the specific purposes for which it was introduced. Of course, in such a case, a thorough analysis should be carried out to determine the purpose of the monitored premises and the impact of such monitoring on the privacy of employees.[524] With regard to places that, as a rule, should not be monitored, the legislator decided to divide their catalogue into two provisions. The first provision is §1^1 of Article 22^2 of the PLC, which states that monitoring shall not cover areas made available to the company trade union organisation.[525] In turn, according to the second of the mentioned provisions (Art. 22^2 §2 of the PLC), monitoring shall not cover sanitary rooms, locker rooms, canteens[526], or smoking rooms.[527] However, with regard to the second part of the catalogue of sites excluded from monitoring, the law provides an exception to this general

[521] See the principle of data minimisation - Art. 5 (1)(c) of the GDPR.
[522] Art. 22^2 §1-2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[523] Art. 22^2 §1 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[524] Miłosz and Świątek-Rudoman, 2019, p. 34.
[525] Art. 22^2 §1^1 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[526] There are certain interpretative uncertainties regarding the notion of a "canteens", mainly due to the fact that canteens as places of collective consumption of food are only found at large employers. However, according to Świątek-Rudoman and Miłosz, this concept should be understood broadly as any room dedicated to the consumption of meals by employees and as a dining room within the meaning of the Regulation of the Minister of Labour and Social Policy of 26 September 1997 on general occupational health and safety regulations (Dz.U. 1997 nr 129 poz. 844) – See: Miłosz and Świątek-Rudoman, 2019, p. 35.
[527] Art. 22^2 §2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).

restriction. Namely, these 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.[528] Such techniques include software that blurs specific parts of the captured image, e.g. the faces of the persons being observed or even their entire silhouettes. Another appropriate measure may be the proper placement of cameras so that there is no violation of dignity or other personal rights, as well as the principle of freedom and independence of trade unions. Furthermore, it should be remembered that monitoring in premises excluded from its scope must be treated as an exception, which in practice may translate into its temporary nature.[529]

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.[530]

Nevertheless, as indicated above, when creating a list of premises that cannot be covered by video monitoring, the Polish legislator divided it into two separate provisions. The reason for this division is to exclude areas made available to the company trade union organisation from the possibility of exceptional monitoring indicated in Article 22^2 §2 of the PLC concerning sanitary rooms, locker rooms, canteens and smoking rooms.[531] This solution should be considered eminently justified and, by all means appropriate, since allowing any kind of monitoring in such premises used by trade unions would automatically violate the principle of freedom and independence of trade unions.

Unlike Polish regulations, neither the Slovakian, Czech, nor Hungarian labour codes explicitly specify which areas of a workplace should be excluded from monitoring or where monitoring should be restricted, which creates a problematic situation from the perspective of both parties of the employment relationship.

Due to the lack of a legal definition of the territorial scope of camera monitoring in the workplace within the Slovak model of monitoring, the need emerged to fill this gap through doctrinal considerations.

---

[528] Art. 22^2 §2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[529] Urząd Ochrony Danych Osobowych, 2018b, pp. 26-27.
[530] Art. 22^2 §2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[531] Miłosz and Świątek-Rudoman, 2019, p. 35.

Siskovičová points out that the areas most frequently monitored by employers include production halls, warehouses, entrance halls, bank and office counters, i.e. areas strictly related to the performance of work.[532] However, when considering the areas that require greater respect for privacy and full or partial exclusion from monitoring, the author follows the position expressed by the EDPS, in which the authority indicated that areas such as individual offices, including offices shared by two or more people and even large open spaces; leisure areas, like canteens, cafes, bars, kitchens, lunchrooms, lounge areas, waiting rooms, etc; toilets, shower rooms and changing rooms. Nevertheless, the EDPS provides for the possibility of derogating from these rules – in such a situation, the employer must carry out an impact assessment of the derogation.[533]

Furthermore, the doctrine indicates that a possible solution would be to introduce provisions into the Slovak Labour Code that would define the exact limits of its territorial applicability (similarly to the regulations under the Polish Labour Code), although it is also noted that this would be extremely challenging in practice. Instead, it is proposed to establish a framework that would give the parties of the employment relationship at least a general idea of when camera monitoring is permissible. An example of such a regulation might be the exemplary enumeration of areas excluded from monitoring, such as: toilets, changing rooms, dining rooms, smoking rooms, etc. A similar solution can also be applied to premises that would be subject to monitoring, e.g. rooms where employees store their personal belongings, server rooms, conference rooms, warehouses, production halls, etc.[534] As Žuľová and Švec point out, the distinguishing feature of premises where camera monitoring is permissible is that they house goods that should be protected against destruction, damage or theft. The authors indicate that such premises may include warehouses, data centres, access routes to protected premises, as well as common rooms and corridors, if there is a justified need for their monitoring.[535]

The issue of the territorial scope of CCTV monitoring is particularly important in relation to road transport employees. This mainly concerns situations where there are cameras in the driver's cab for monitoring purposes. Professional drivers very often spend their mandatory rest periods in the rear of the vehicle cab, treating it as a private space, which is reflected, among other things, in the placement of many personal items there.[536] The question that arises in this context is whether the cab of a vehicle, which is undoubtedly the driver’s place of work, can

---

[532] Siskovičová, 2015, p. 57.
[533] European Data Protection Supervisor, 2010, p. 29.
[534] Puci, 2016, p. 95.
[535] Žuľová, and Švec, 2018, p. 108.
[536] Greguš, 2017, p. 240.

also be considered his or her private space, and if so, whether video surveillance of such a place is permissible? The answer to this question is complex, as it depends on many factors and circumstances. Firstly, it should be noted that the cab can be considered the driver's private space, even in his absence, if it contains items that reflect his political views, religion or sexual orientation.[537] Secondly, the admissibility of camera monitoring depends on whether the monitoring is to take place during or outside working hours. Monitoring outside working hours would certainly constitute an excessive invasion of the employee's privacy and be contrary to their dignity, but what about monitoring during working hours? Given the specific nature of a driver's work and their workplace, which is the vehicle cab, it must be concluded that CCTV monitoring would not meet the requirement of proportionality in this case. It seems that a less intrusive and more appropriate measure of monitoring for professional drivers (especially long-distance drivers) would be vehicle monitoring using GPS.

Considering the similarity between Section 316 (2) of the Czech Labour Code and Section 13 (4) of the Slovak Labour Code, it is evident that the Czech model of camera monitoring shares the same shortcoming as the Slovak model – the lack of an explicitly defined territorial scope of monitoring. Furthermore, as in the case of Slovakia, in the Czech Republic, the task of clarifying this scope has been undertaken by legal doctrine and case law.

In fact, there are no particular differences between the aforementioned positions expressed by Slovak labour law scholars and the opinions articulated within the Czech labour law doctrine. Authors such as Šmejkal, Sehnálek, and Potyková agree that there are areas within the workplace where employees should be able to maintain a particular degree of privacy. These areas include rooms used for hygiene purposes (e.g. toilets and showers) and places where employees may find themselves in intimate situations or have private conversations with other employees (e.g. changing rooms, smoking rooms and canteens).[538] This position was confirmed and even expanded upon by the Czech Administrative Court. In its ruling of 23 August 2023, the court indicated not only that monitoring should not take place in areas designated for hygiene or rest, but also that the monitoring should be directed at the employer's property and not at the employee's person.[539] The demand to exclude the person of the employee from the scope of monitoring partly coincides with the position expressed by the Hungarian DPA.[540]

---

[537] Greguš, 2017, p. 240.
[538] Šmejkal, 2019, p. 72, 80; Sehnálek, 2023, p. 260; Potyková, 2018/2019, p. 58.
[539] Judgement of the Czech Supreme Administrative Court of 23 August 2013, 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."
[540] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013, p. 5; A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 23-24.

However, it should be noted that complete exclusion and recognition of employee monitoring as inadmissible would be exceptionally challenging, if not impossible, to implement, given the employer's obligation to organise the work process and ensure appropriate conditions in accordance with occupational health and safety requirements. Therefore, the position expressed by the Hungarian DPA should be considered more realistic, as it does not completely reject the possibility of monitoring an employee, but states that monitoring whose sole purpose is to monitor an employee is unacceptable.

In the Hungarian Labour Law Code, as well as in the Czech and Slovak labour law codes, we will not find a detailed territorial scope of camera monitoring that would indicate which areas may be subject to surveillance and which are excluded from it. Nevertheless, this has not been overlooked by either the Hungarian DPA or labour law scholarship.

Reflections on the territorial scope of CCTV monitoring within the Hungarian model of workplace monitoring lead us to a highly prominent concept within this model, which has already been mentioned above, namely "human dignity." According to the position expressed by the Hungarian DPA, the use of monitoring in areas such as changing rooms, showers, toilets, medical rooms, waiting rooms, as well as in rooms designated for employees to spend their work break (e.g. canteens), constitutes a violation of human dignity and is unacceptable.[541] Nevertheless, an exception to this rule may occur when such rooms contain goods that require protection. Such goods may include, e.g., a beverage or food vending machine. However, in such a situation, the employer's interest in monitoring such a device and installing cameras in the specific premise must be duly justified, e.g. if the employer's equipment has been damaged before, which resulted in a financial burden for the employer. In such a situation, a camera placed in a room characterised by an increased degree of privacy must only be used to monitor a specific device, and its field of view must only be directed at that device.[542]

However, it should be noted that the entire workplace, including "sensitive" areas, may be monitored if no one is legally permitted to be in the workplace (e.g. on public holidays or after working hours). Ultimately, monitoring conducted by the employer is limited to the locations it owns or uses. Monitoring of any public places is excluded.[543] The strict exclusion of public places from the scope of monitoring is a reasonable solution, although unfortunately, it may be problematic in reality. There may be situations when an employer would need to monitor the

[541] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013), p. 5
[542] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013, p. 5, A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 24.
[543] Ásványi, 2022, p. 273; A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 24.

areas around the workplace, which will be a public area. In comparison, the Polish legislator has recognised that such a need may indeed arise and has indicated in the provisions that not only the workplace itself may be monitored, but also the area around the establishment.[544]

1.4.4.2. Data Retention Period

Another issue related to video monitoring that should be considered when conducting comparative legal analysis between workplace monitoring models in Visegrad Group countries is the data retention period. On the grounds of this issue, there are many differences apparent between the four models. It should be noted that the most distinctive mode of all, primarily due to its specificity, is the Polish one.

The Polish legislator, in order to comply with the principle of data storage limitation, derived from the GDPR, which stipulates that personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed,[545] decided to introduce Article 22^2 §3-5 into Polish Labour Code. These provisions regulate precisely the data retention period and the question of what should happen to such data after that period has expired. As a general rule, the data storage period shall not exceed 3 months from the date of the recording. [546] There is no obstacle to the period specified by the employer being significantly shorter than three months, but it is essential that it be specified in some way, as this is implied, among other things, by the employer's obligation to provide information on the application of monitoring.[547] However, there is an exception to the data retention rule - 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.[548] The legislator did not specify exactly the type of proceedings in question, indicating only that they should be conducted under the law. Therefore, a broad range of proceedings should be accepted, such as criminal, administrative, disciplinary,

---

544 Art. 22^2 §1of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
545 Art. 5(1)(e) of the GDPR.
546 Art. 22^2 §3 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
547 Miłosz and Świątek-Rudoman, 2019, p. 35.
548 Art. 22^2 §4 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).

misdemeanour and civil proceedings.[549] Apart from legal proceedings, it is also possible to imagine other situations where data storage for longer than three months may be applicable, e.g. in the event of a warranty or guarantee claim. Certainly, if personal data is processed during monitoring in such a situation, the employer may not extend the data retention period beyond three months without a proper legal basis. However, if no personal data is processed as part of the monitoring, e.g. because the monitoring introduced for production control purposes only covers the production line, excluding recording the appearance of employees, or because employees are anonymised, then it is possible to extend the data retention period.[550] After the end of the retention period, the recordings containing personal data must be destroyed, unless separate regulations provide otherwise.[551]

As regards Slovakia and the Czech Republic, the labour codes of these two countries do not contain any similar regulations to the Polish one concerning the period of data storage and the obligation to destroy data after such a period has expired. Therefore, once again, we must address doctrinal considerations, which serve as interpretative guidelines in this matter.

Within the framework of the Slovak monitoring model, Žuľová et al. draw attention primarily to the data controller's information obligation stemming from Article 13 of the GDPR. It can be inferred from this provision that the employer is obliged to inform its employees about the period of storage of personal data for each processing purpose separately, or at least to provide the criteria on the basis of which such a period may be determined.[552] Therefore, it should be concluded that in this case, the Slovak legislator has taken a more liberal approach than the Polish one, as it does not specify a maximum data retention period in advance, but leaves this matter entirely to the discretion of the employer. This conclusion is endorsed by the position expressed by the Slovak DPA, which indicated that in order for data processing to be considered compliant with the principles set out in Article 5 of the GDPR, one of the obligations of the operator is to demonstrate that the processed personal data are stored for a period that depends on the purpose of their processing.[553] In turn, Beňová and Ladiverová, in their work, pay particular attention to the principle of data storage limitation resulting from Article 5(1)(e) of the GDPR. The authors point out that, firstly, the employer is obliged to specify the period of data storage, and secondly, the purpose of monitoring employees usually

[549] Miłosz and Świątek-Rudoman, 2019, p. 36.
[550] Miłosz and Świątek-Rudoman, 2019, p. 36.
[551] Art. 22^2 §5 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[552] Žuľová, et al., 2018, p. 55; Art. 13 of the GDPR.
[553] Office for Personal Data Protection of the Slovak Republic, Frequently Asked Questions, https://dataprotection.gov.sk/en/legislation/guidelines-faq/frequently-asked-questions-faq/# (Accessed: 3 May 2026).

ceases immediately after the control has been carried out; thus, the monitoring period should not exceed three months.[554] It seems that specifying a maximum data retention period is a desirable solution, but it should be noted that under Slovak law, in contrast to the Polish model, this period is not legally binding and can only be considered as a guideline. Moreover, the Slovak doctrine[555] refers to the EDPB guideline, in which the authority proposes a black box solution, under which data is automatically deleted after a certain storage period and only made accessible in the event of a specific incident.[556]

Under the Czech model of monitoring, it is indicated that the purpose of data processing is crucial for determining the period of data retention.[557] When it comes to camera recording, a period of several days or even weeks is considered appropriate. The specific flexibility of the period results, among other things, from the aforementioned purpose and who operates the camera monitoring system.[558] On the other hand, Czech labour law doctrine also included a standpoint that defines the retention period of video monitoring recordings in a more restrictive manner. For instance, Skubal writes that such a period should not exceed 7 days. However, it may be extended if this is due to the employer's duly justified needs. Further, the author points out that in situations when a data operator has solid arguments for a longer period of retention, in most cases, the Office for Personal Data Protection (UOOU) leans towards its acceptance.

At first glance, it may appear that a time limit of 7 days is more in line with the principle of data retention than, e.g., the 3-month period specified in Polish regulations. Nevertheless, this time limit is not explicitly set in law, and its application is dependent on the approval of the public authority responsible for personal data protection. Such a situation should be considered undesirable, as it creates uncertainty with regard to the parties to the employment relationship.[559]

Another shortcoming of the Czech regulation, which is also present in the Slovak provisions, is the lack of specification as to what should be done with the data after the retention period has passed. However, in accordance with the principles set out in the GDPR, the literature indicates that after the storage period, if the recordings are no longer needed for the purpose for which they were made, they should be deleted.[560]

---

[554] Beňová and Ladiverová, 2020, p. 82.
[555] Beňová and Ladiverová, 2020, p. 82.
[556] The European Data Protection Board, 2020, p. 11.
[557] Žůrek, 2017, p. 211.
[558] Potyková, 2018/2019, p. 58.
[559] Mirosławski, 2025, p. 207.
[560] Žůrek, 2017, p. 212.

Hungarian regulation, just like Czech and Slovak regulations, is silent on the subject of the storage period of personal data obtained through monitoring. However, this issue looked completely different under the previous legal status. In 2013, the Hungarian DPA, in its recommendation on the basic requirements for electronic monitoring systems used in the workplace, indicated that, unless there is another legal basis, the provisions §31 (2)-(4) of Act CXXXIII of 2005 on the rules for the protection of persons and property and the activity of private detectives[561] should apply to the storage period of recordings made within the electronic monitoring system.[562] According to these provisions, recordings obtained from monitoring could, in principle, be stored for three working days, and after that period they should be deleted. If, however, it was necessary to store the recordings for longer than three working days, the employer had to justify this need in accordance with the principle of purposefulness and the test of balancing the interests of the parties to the employment relationship. Furthermore, if any of the exceptional circumstances specified in §31 (3)-(4) of the Act CXXXIII of 2005 occur, recordings may be stored for a period of 30 days or even 60 days in some cases.[563] This view was confirmed in 2016 by the information on the basic requirements for data processing in the workplace issued by the Hungarian DPA.[564]

Under the current legal framework, the above provisions are no longer in force; therefore, regulations concerning the retention period should be sought primarily at the level of the Hungarian act on information self-determination right and information freedom,[565][566] the GDPR[567] and in the employer's information obligation[568]. This situation resembles that in Slovakia and the Czech Republic, although, unlike those countries, under the Hungarian monitoring model, even the doctrine is silent on the issue of a precisely defined maximum

---

[561] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól.
[562] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013, p. 6.
[563] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013, p. 6; Lukács, 2017, p. 96.
[564] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 24
[565] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (hereinafter: Info Act).
[566] Section 4 of this Act regualtes the principle of "purpose limitation," which resembles a combination of the principles of "purpose limitation", "data minimisation" and "storage limitation" derived from the GDPR. Paragraph 2 of this section indicates that only personal data that is necessary for the purpose of data processing and that is appropriate for achieving that purpose may be processed. Moreover, it states, which is crucial to the issue under discussion, that personal data may only be processed to the extent and for the period necessary to achieve the purpose. For more detailed considerations about the principles stated in Info Act - See: Bankó and Szőke, 2016, pp. 45–50.
[567] This primarily concerns the obligations arising from the principle of storage limitation (Art. 5(1)(e) of the GDPR) and the information obligation imposed on the controller (Art. 13 of the GDPR).
[568] Information regarding the introduction of monitoring addressed to employees must include, among other things, information whether the recordings made by cameras and recorded and stored, and if yes, for what purpose - See: Az Adatvédelmi Biztos, 1998, pp. 52-53.

period for data storing. It should therefore be recognised that the Hungarian model gives employers the greatest level of discretion in determining the period for which monitoring recordings will be stored. Of course, this period is not unlimited - in accordance with the principle of data storage limitation, recordings should be deleted immediately when their processing is no longer necessary for the purpose for which they were processed.

Concluding the comparative legal considerations regarding the retention period for data collected through camera monitoring, two further issues should be addressed. Firstly, what kind of data can be recorded during CCTV monitoring? Is it only images or also sound? Secondly, what if the cameras used in the surveillance system only record images in real time without recording them? In such a situation, is there no data processing involved, and will the personal data protection regulation not apply to such a scenario?

In terms of the scope of data that can be recorded by CCTV monitoring systems, there is a significant difference between the Polish model and the other three workplace monitoring models.

By stating in Art. 22^2 §1 of the Polish Labour Code, which states that visual monitoring constitutes technical measures enabling video recordings, the Polish legislator has explicitly determined that this type of monitoring cannot involve the recording of audio data.[569] In contrast, Slovak, Czech and Hungarian provisions regulating CCTV monitoring do not indicate that it is limited only to measures enabling the recording of images, excluding sound. These regulations have a much more open structure and are *de facto* silent on what types of data may be collected and processed as part of video monitoring. It can therefore be concluded that, in addition to video, which is obvious in the case of camera monitoring, these systems can also record sound. This finding is confirmed by the positions presented by legal doctrine and national DPAs.[570] Nevertheless, monitoring that simultaneously records both image and sound cannot be considered a standard solution that can be used in every situation, as it constitutes a much greater invasion of privacy than video recordings alone.[571] An employer intending to introduce a monitoring system that records both types of data should first carefully assess whether audio recordings are truly necessary for the indicated purpose of processing, as

[569] Miłosz and Świątek-Rudoman, 2019, p. 35.

570 All these postions lead to one conclusion: CCTV monitoring can be used not only to record images but also to record audio – See: Šimečková, 2021, p. 99; Úřad pro ochranu osobních údajů (2024), p. 34; Siskovičová, 2015, p. 60; Švec, Toman, Olšovská and Žuľová, et.al., 2023, § 13 - V. Zavedenie kontrolného mechanizmu u zamestnávateľa; Nemzeti Adatvédelmi és Információszabadság Hatóság, Decision in case NAIH-2732-2/2023, p. 22.

[571] Nemzeti Adatvédelmi és Információszabadság Hatóság, Decision in case NAIH-2732-2/2023, p. 22.

otherwise such monitoring may be considered a violation of Article 6 (1) of the GDPR.[572] In practice, as the Czech DPA points out, in most cases only video recordings will be proportionately sufficient for the employer to achieve the intended purpose of monitoring.[573]

Regarding the second issue - video monitoring in real time, without recording, it should be indicated that within Slovak and Czech labour law doctrines, a frequently occurring view is that a precise distinction should be made between camera monitoring systems that record images and those that perform monitoring, but without recording (so-called online camera systems).[574] This distinction is based on an interpretation of the notion of "processing" expressed in Article 4 (2) of the GDPR. Some of the authors point out that in the case of the use of non-recording cameras, there is no "processing" of employees' data; therefore, the employer will not have to comply with the requirements of the GDPR when introducing and using such monitoring, but only with those established by the Czech or Slovak Labour Code. According to this position, data processing only takes place in a situation where the surveillance cameras are recording monitored employees and in that case, not only the labour law regulations, but also the GDPR will apply.

Nevertheless, when analysing the notion of "processing" indicated in the GDPR, it appears that the aforementioned position is not properly justified. Article 4 (2) of the GDPR reads that "processing" means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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".[575] When interpreting this provision, it should be noted that the list of operations that constitute processing in accordance with the provisions of the GDPR is exemplary and forms an open catalogue.[576] In particular, this is indicated by the phrase used in the interpreted provision "processing means any operation or set of operations (…) such as".[577] In addition, the stance expressed by the European Data Protection Board[578] is also symptomatic. The EDPB in its Guidelines 3/2019 on processing of personal data through video devices, adopted on 29 January 2020, expressed the opinion that "In other situations, it

[572] Nemzeti Adatvédelmi és Információszabadság Hatóság, Decision in case NAIH-2732-2/2023, p. 22.
[573] Úřad pro ochranu osobních údajů, 2024, p. 34.
[574] See: Škvarková, 2017, p. 205; Siskovičová, 2015, p. 56; Šimečková, 2021, p. 99; Sehnálek, 2023, p. 260.
[575] Article 4 (2) of the GDPR.
[576] Lubasz, Chomiczewski, Czerniawski, Drobek, Góral, Kuba, Makowski, Witkowska-Nowakowska, 2018, Art. 4.
[577] Fajgielski, P., 2025, Art. 4.
[578] Hereinafter: EDPB

might not be necessary to record the video material at all, but more appropriate to use real-time monitoring instead. (…) Sometimes real-time monitoring may also be more intrusive than storing and automatically deleting material after a limited timeframe (e.g., if someone is constantly viewing the monitor, it might be more intrusive than if there is no monitor at all and material is directly stored in a black box)”.[579] A situation in which this type of monitoring may be more appropriate is the workplace, where employee performance is monitored in real time either by staff assigned to it or by algorithms programmed for it. Moreover, the EDPB also indicated that in the context of such processing, the principle of data minimisation should apply, thus stating that video monitoring without recording should be considered data processing in terms of the GDPR.[580]

Therefore, it must be stated that regardless of what type of camera system we are dealing with, whether it is a system where cameras only monitor or cameras that also record in addition to monitoring, both the provisions indicated in Article 13 (4) of the Slovak Labour Code and Section 316 (2) of the Czech Labour Code, and the provisions of the GDPR will apply in the case of video surveillance.[581]

1.4.4.3. Determination of Objectives, Scope and Manner of Monitoring

Another element, which in fact concludes the procedure of introducing camera surveillance in the workplace, is determining its objectives, scope and manner of use, as well as the information obligation that must be fulfilled by the employer.

Regarding defining objectives, scope and manner of the use of video monitoring, Art. 22^2 §6 of the Polish Labour Code deserves special attention. This provision specifies that all of these issues 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.[582] This solution complies with the principle of transparency of data processing and Opinion 2/2017 of the no longer active 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.[583] The

[579] The European Data Protection Board, Guidelines, 2020, p. 29.
[580] The European Data Protection Board, Guidelines, 2020, p. 29.
[581] Štěpánková points out that virtually all devices that capture or transmit images of natural persons, such as cameras, camera systems, photo traps and similar devices, should be covered by the rules stated in the GDPR, regardless of whether their operation involves recording – see: Štěpánková, 2025, p. 331.
[582] Art. 22^2 §6 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[583] Article 29 Data Protection Working Party, 2017, p. 23.

introduction and amendment of both the collective labour agreement and the work regulations require agreement with the trade union organisation active in the establishment.[584] 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.[585]

Compared to other monitoring models, this regulation appears to be unique and means that Polish employees, among other employees of Visegrad Group states, have the greatest influence on the shape of the monitoring system to be used in a given workplace. Similar, nevertheless, not so impactful regulations can be found in Slovak and Hungarian law, but not in the Czech Republic.

The second sentence of Section 13 (4) of the Slovak Labour Code provides for discussions between employers and employee representatives on the scope of monitoring, the manner in which it is carried out and its duration.[586] The consultation process is regulated by Section 237 of the Slovak Labour Code.[587] However, such consultations do not constitute a formal procedure and do not impose any additional rights or obligations on the parties.[588] Moreover, if employees have not elected their representatives within a given workplace, the employer may act autonomously.[589] The provision establishes a minimum range of matters that should be discussed, including the scope of the control, the manner in which it is to be carried out and the duration of the control. It is important to point out that the discussion does not imply the need for consent to introduce monitoring from the side of employee representatives; therefore, its absence is not binding on employers. Additionally, following the Polish model, the literature recommends that all necessary information on the monitoring mechanism, in particular on its nature and method, be included in the employer's internal regulations (work regulations), collective agreement, or individual employment contract.[590] Such a solution would effectively bring the employees' side closer to actual participation in the creation of rules and procedures related to monitoring in their workplace.[591] In the case of Hungarian regulation, only Section 264 (2) (d) states that at least fifteen days before the employer makes his/her decision on the

[584] Art. 241^2, 241^9, and 104^2 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[585] Miłosz and Świątek-Rudoman, 2019, p. 36.
[586] So-called: consultation obligation.
[587] Section 237 of the Slovak Labour Code.
[588] Greguš, 2018, p. 30-31.
[589] Section 12 (2) of the Slovak Labour Code.
[590] Švec and Valentová, 2021, p. 50.
[591] On the consultation obligation - See more: Švec and Valentová, 2021, pp. 50-53.

application of a technical device for monitoring the employee, he/she shall ask the opinion of the works council on the draft of such a measure.[592]

1.4.4.4. Information Obligation

In terms of information obligation, the Polish model continues to follow the path of detailed and extensive regulation.[593] It places 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 notification should be the one adopted by the employer concerned.[594] In relation to new employees, contrary to employees already in an employment relationship, the information obligation is of an individual character.[595] 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 the objectives, scope and manner of the use of monitoring in writing.[596]

In contrast, the Slovak, Czech and Hungarian models regulate this issue in a much briefer manner. Under Slovak regulation, the employer's information obligation regarding monitoring means that the employer must inform employees of the same scope of technical details as covered by the consultation obligation discussed above.[597] The Labour Code does not explicitly indicate in which form the information obligation should be completed. Using a grammatical interpretation, it should be stated that the information on the scope, manner and duration of the monitoring can be provided orally in an informal way or generally, as in Poland, in accordance with the practice adopted by a given employer.[598] The same applies to the consultation duty. The lack of specification of the concrete form of fulfilment of these obligations should be considered a negative aspect of the regulation,[599] as it significantly violates the requirement of transparency, which is crucial in the context of an interference in an employee's privacy. Taking this into account, and above all, for evidentiary reasons, it is recommended to inform employees about monitoring measures in a written form, and in case of fulfilling the consultation obligation, to draw up a discussion protocol together with employee representatives.[600]

---

[592] Section 264 (2) (d) of Act I of 2012 on the Labor Code.
[593] Art. 22^2 §7, §8 and §9 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[594] Art. 22^2 §7 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[595] Dąbrowska, 2019, p. 17.
[596] Art. 22^2 §8 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[597] The second sentence of the Section 13 (4) of the Slovak Labour Code.
[598] Švec and Valentová, 2021, p. 53.
[599] Greguš, 2018, p. 30-31.
[600] Greguš, 2017, p. 234.

Information obligation in the realm of the Czech model is limited to a single provision. Namely, Section 316 Paragraph 3 of the Czech Labour Code stipulates that in the case of the 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.[601] Therefore, this obligation can be fulfilled in any appropriate form that enables the individual to directly transfer information to each employee.[602] 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.[603] The specific discretion of the form of information on monitoring is also apparent in the Polish and Slovak models. The Polish Labour Code explicitly indicates that "an employer shall notify employees of the introduction of monitoring, in the manner adopted by the given employer."[604] However, when it comes to Slovakia, this matter, as in the case of the Czech Republic, is rather based on the doctrinal deliberations and interpretations of regulations that are concise in their nature. 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.[605]

The fourth of the models discussed, namely the Hungarian model, stands out from the other regulations, as the Hungarian legislator is the only one to have established a specific form in which the employer's information obligation should be fulfilled, namely, it is a written form.[606] Unfortunately, however, Hungarian regulation concerning information obligation essentially ends there, which makes it similar in its shortcomings to Slovak and Czech regulations. According to the guidelines of the Hungarian DPA, written information regarding monitoring in the workplace, which is to be provided to the employee, must at least include the legal basis for data processing; the location of each camera, the purpose of its installation and the area being monitored; the place and time of storage of the recordings; an indication of the security measures used in connection with data storage; rules regarding access to recordings; as well as the rights of employees in relation to the monitoring system, how they can exercise their rights

---

[601] Section 316 (3) of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".
[602] Sehnálek, 2023, p. 259.
[603] Morávek, 2017, p. 10.
[604] Art. 22^2 §7 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[605] Morávek, 2020, pp. 26-27.
[606] The second sentence of the Section 11/A (A) of Act I of 2012 on the Labor Code (Hungarian Labour Code).

and what legal remedies are available to employees in the event of a violation of their rights.[607] The scope of information covered by the notification is exceptionally broad and stands out from other V4 countries, which focus primarily on matters strictly related to the monitoring system, rather than, for example, employee rights. Moreover, within the Hungarian model, particular attention is paid to the appropriate language of written communication, which should be simple, free of jargon and understandable to every employee to whom the information is addressed. This is particularly important from the perspective of the principle of transparency expressed in the GDPR.[608] Furthermore, the employer bears the burden of proving that employees have actually received information about camera recordings made in the workplace, e.g. by means of written confirmation of a given document or by completing and signing a questionnaire. New employees should be informed of the above matters before starting work, in a document separate from the employment contract. Such a document should also be signed by the employee.[609] Interestingly, Švec and Valentová, on the basis of Section 13(4) of the Slovak Labour Code, come to completely opposite conclusions. The authors point out that in practice it does not matter whether they have actually familiarised themselves with the information, but it is sufficient that they have had the opportunity to familiarise themselves with it in a place accessible to them, e.g. via the intranet, the internet or a notice board at the workplace.[610] However, it is difficult to agree with this position. In accordance with recital 58 of the GDPR preamble, as well as Articles 12 and 13 of the GDPR, it should be noted that the aim of the European legislator was not only to data subjects whose personal data are processed to familiarise themselves with a message providing detailed information about such processing, but above all to achieve a situation in which the understanding of this information and the mechanisms of data processing was as comprehensive as possible.[611] However, considering the scope of information to be provided, the complexity of the GDPR and the specialised language used in the regulation, it must be said that we are facing a paradox, as the European legislator requires data controllers (in relation to the subject of this paper, this mainly concerns employers) to achieve a goal that it was not able to fully achieve itself when drafting the regulation.[612] Furthermore, understanding the information on data processing is not facilitated by the fact that most employees do not have legal knowledge, which, in practice, is necessary

[607] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013, p. 7; A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 25; Ásványi, 2022, p. 273.
[608] Article 5 (1) (a) of the GDPR.
[609] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013, p. 7.
[610] Švec and Valentová, 2021, p. 53.
[611] Łuczak, 2018, Art. 12.
[612] Łuczak, 2018, Art. 12.

to understand the majority of matters relating to data processing, including monitoring in the workplace. Therefore, based on the current state of the discussion on the requirement of transparency in the workplace, especially in the context of monitoring and new technologies, whose mode of operation further complicates the overall understanding of how personal data is processed, it should be pointed out that employers are not only obliged to provide employees with the opportunity to familiarise themselves with information on monitoring, but above all to create a situation in which they can be certain that the employee has reviewed and understood such a communication, which is at least theoretically the case under the Hungarian model of workplace monitoring.

Information obligation consists of one more element, which is the need to designate the monitored area visibly and legibly. Among the four discussed workplace monitoring models, only the Polish one explicitly expresses this need, indicating that monitored areas should be marked by appropriate signs or sound announcements, but no later than one day before starting the monitoring.[613] However, in practice, the need for adequate signage of monitored areas and monitoring equipment is also evident in the other three models.[614]

In its guidelines on the use of video surveillance, the President of the Polish Personal Data Protection Office has formulated universal conclusions that can certainly also be applied to other Visegrad Group countries. Namely, he stated that it is essential for persons who are present in the monitored areas to be aware that monitoring activities are taking place in their location. Therefore, 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.[615] Nevertheless, the aforementioned measures cannot be considered sufficient in light of Articles 12 and 13 of the GDPR, which are binding in all four Visegrad Group countries. Based on these provisions, it should be noted that in a workplace where all or part of the premises are subject to monitoring, full information on monitoring systems should be provided, including the requirements of Article 13 of the GDPR. In order to fulfil this obligation, a layered information system may be used, i.e. first providing employees with basic information and subsequently supplementing it in further layers of information.

[613] Art. 22^2 §9 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[614] Švec and Valentová 2021, p. 56; Úřad pro ochranu osobních údajů, 2024, p. 53; A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013, p. 7.
[615] Urząd Ochrony Danych Osobowych, 2018b, p. 20.

Layered information may take the form of a document or even a book, which will be available at the reception desk or at the controller's representative.[616]

2. Property of the Employer

The second most common purpose of using monitoring in the workplace, after the desire to check and control the tasks performed by employees, is to protect the employer's property. Obviously, the forms of monitoring discussed earlier - communication monitoring and camera monitoring - can be used to achieve this goal. However, this part of the thesis will focus primarily on two forms, the use of which is most often justified by employers specifically for the purpose of protecting their property. Namely, these are monitoring using the Global Positioning System[617] and personal inspection in the workplace.

2.1. GPS Monitoring

GPS in the Visegrad Group countries is considered a modern measure of monitoring.[618] As Lukács points out, due to technological developments, monitoring is no longer limited to the workplace in its physical sense, but can also "follow the employees home," allowing their activities outside the workplace to be observed. One of the many measures that certainly fit this definition is monitoring via a GPS system.[619]

The most common use of GPS tracking can be found in the instance of transport employees, sales representatives, couriers and professional drivers, as it is installed in vehicles, which are their working tools. Nevertheless, the GPS system is not limited to the above-mentioned groups of employees, as it is also used in the case of company vehicles and even other items entrusted to an employee for the purpose of performing their employment duties, and in some cases even for their private affairs, if this has been authorised by the employer.

GPS monitoring is permissible under all four analysed workplace monitoring models, although it is not explicitly mentioned in any of them.

616 Urząd Ochrony Danych Osobowych, 2018b, p. 14.
617 Hereinafter: GPS.
618 Greguš, 2017, p. 231; Maciejewska and Figurski, 2014, p. 2.
619 Lukács, 2021, p. 122; Bibby, 2016, p. 1-2.

Under the Polish regulation, Article 22^3 §4 opened up the catalogue of monitoring measures, allowing for measures other than those explicitly mentioned in the provisions.[620] According to the Article 22^3 §4, the provisions of articles 22^3 §1-3 of the Polish Labour Code (thus, also articles 22^2 §6-10 of the Polish Labour Code) shall apply accordingly to other form of monitoring if their use is necessary to fulfil the objectives specified in the Article 22^3 §1 – i.e. when it is necessary to ensure an organisation of work enabling the full use of the working time and proper use of work tools made available to the employee. The extended catalogue of monitoring methods certainly includes tracking via GPS.[621] Furthermore, out of the four Visegrad models of workplace monitoring, only the Polish one explicitly specifies the purposes for which GPS monitoring may be used.

The basis for GPS monitoring in the case of the three remaining models will be the provisions analysed in an earlier section of this thesis, in particular, the provisions discussed in the context of beyond communication forms of monitoring, i.e. Section 13 (4) of the Slovak Labour Code, Section 316 (2) of the Czech Labour Code and Section 11/A (1) of the Hungarian Labour Code. This is primarily due to the relatively open nature of these provisions, which do not set out a closed list of specific permissible monitoring measures. None of the four models requires employee's consent for the introduction of GPS monitoring, but it should be remembered that, as in the Polish model, such a measure must be justified by appropriate objectives, which will also constitute the framework for its application.[622]

In the case of Slovakia and the Czech Republic, GPS monitoring may be justified by the discussed earlier "serious reasons arising from the employer's nature of activity" as stated in Section 13 (4) of the Slovak Labour Code and Section 316 (2) of the Czech Labour Code. Many of the reasons expressed by employers are connected to the economic side of the business, namely, cost saving, optimising taxation and protecting property from damage and theft.[623] Also, very often in the transport sector, discussion focuses on the need to ensure driver safety and monitor data such as vehicle movement, fuel consumption, etc., as a basis for GPS tracking.[624]

---

620 Art. 22^3 §4 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code.(Polish Labour Code).
621 Barański, 2018, p. 48.
622 Bureau of the Inspector General for Personal Data Protection from Poland, Office for Personal Data Protection from the Czech Republic, Croatian Personal Data Protection Agency, Commission for Personal Data Protection from the Republic of Bulgaria, 2012, p. 22; Greguš, 2017, p. 238.
623 Greguš, 2017, p. 238; Šmejkal, 2019, p. 73.
624 Šmejkal, 2019, p. 81; Potyková, 2018/2019, p. 64; Greguš, 2018, pp. 26-35.

In turn, when it comes to Hungary, the employee may only be checked for his/her behaviour related to the employment relationship.[625] In practice, it is recommended that monitoring be used for so-called logistical purposes, that is, e.g. to determine the position of a vehicle, to organise in a more efficient manner workflow, or when it is justified by the value of the vehicle or cargo (when large amounts of cash, other valuable goods or dangerous items are being transported). Furthermore, GPS may be justified as a measure of monitoring in situations where it is necessary to protect the life or physical integrity of an employee, e.g. when moving through a conflict zone.[626] The Hungarian DPA draws attention to an immensely important issue that must be resolved before GPS monitoring is introduced. Namely, a balancing of interest test must be carried out, in which the main question is for what purpose the employer intends to use the GPS system and why its use constitutes a proportionate restriction of the employees' right to privacy and the protection of their personal data.[627] Such a test must be carried out not only within the Hungarian monitoring model, but also in each of the models under analysis.

GPS monitoring, at least in theory, should focus on monitoring means of production, which is the property of the employer rather than the person who uses it. Considering the duty of the employer to organise the work process and the risks it entails, the employer's desire to oversee the location of its property must certainly be considered legitimate. On the other hand, in this context, it is often argued that an employer monitoring the location of its property used by an employee does not violate the employee's privacy, as no personal data is processed.[628] This statement is far from reality, as it should be pointed out that, for example, monitoring the route of a car or other vehicle or object used by an employee in practice implies monitoring the whereabouts and other information, sometimes of a private nature, of its driver/user, i.e. the employee.[629] The personal nature of the data collected through GPS monitoring and the possibility of obtaining more data than is actually necessary for the employer in connection with the use of such a monitoring measure were emphasised by the Hungarian and Polish data protection authorities.[630] This issue has not escaped the attention of labour law doctrine either. Stefański directly points out that regular GPS monitoring can reveal the behaviour patterns of individual employees, their preferred routes, rest stops and even dietary preferences. In this

[625] Section 11/A (A) (1) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[626] Ásványi 2022, p. 274; Szádeczky, 2012, p. 38; A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 33.
[627] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 33.
[628] Metelka, 2024; Šmejkal, 2019, p. 73.
[629] Kuźnicka, 2018, p. 75.
[630] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 33; Urząd Ochrony Danych Osobowych 2018a, p. 37.

regard, the author indicated that it is necessary to define as narrowly as possible the scope of data that may be collected and processed as part of this form of monitoring - “the key issue is that employers should acquire the data that corresponds with the purposes of data processing (principle of data minimisation). Hence, the employer is required to clearly specify the purpose of data acquisition.”[631] As examples of such purposes for GPS monitoring, Stefański points out: protection of the employer’s property; preventive measures against events harmful to the workplace; protection of information constituting corporate secrets; and monitoring the proper performance of work, including checking compliance with working hours.[632]

Apart from the theoretical dimension, the issue of GPS monitoring, the scope and nature of data collected during its use, and their subsequent exploitation, has primarily practical significance.

Bratislava Regional Court, when hearing the appeal in the case concerning the invalidity of the immediate termination of the employment relationship for breach of work discipline, pointed out that the data that was obtained by the employer through the GPS monitoring system installed in the vehicle that was used by the employee constituted only data concerning the movement of the vehicle and not data concerning the employee's compliance with working hours.[633] This judgment has significant consequences, as in practice it means that, in disciplinary dismissal cases, an employer’s evidence based on data obtained through the use of GPS monitoring in the vehicle used by the employee might be found inadmissible.[634]

Another landmark case concerning the usage of GPS monitoring in the context of employment is the case of the Czech Post.[635] In this case, Czech Post introduced a large-scale system for monitoring its employees using GPS. In this case, Czech Post introduced a large-scale GPS surveillance system for its employees. All postmen in 7777 postal districts were covered by this system for one year (postmen had to carry GPS locators with them). With the technology, the employer could collect and process the following data: the length of the route covered by the postman; the time spent on the route; the districts in which the postman travelled; the ratio of places visited to those not visited; the delivery points with the highest number of visits, etc. While justifying the introduction of such a system, the employer pointed out that it is intended to speed up and improve the provided postal services; optimise delivery areas, i.e.

[631] Stefański, 2021, p. 16.
[632] Stefański, 2021, p. 16.
[633] The judgment of the Regional Court in Bratislava from 16 January 2013, n. 4CoPr/1/2012 and n. 4CoPr/2/2012.
[634] Mesarčík and Poruban, 2023, p. 465.
[635] Judgment of the Municipal Court in Prague, 6A 42/2013 - 48.

better distribute the work of postmen; monitor the movement of postal vehicles and ensure the safety of employees.

Firstly, the case was referred to the Office for Personal Data Protection, which in its inspection report of 4 October 2012 (ref. INSP1-3568/12-12/BYT), indicated that personal data had been processed within the GPS system used, as the route analysed within the system could be attributed to a specific employee by means of the schedules existing in the relevant post offices, which specified who operated which route and when. The authority assessed this monitoring measure applied by the Czech Post as unlawful. This assessment was justified by stating that GPS monitoring did not comply with the principle of proportionality – systematic monitoring for the purpose of optimisation cannot take precedence over privacy, even in the workplace. Furthermore, the authority pointed out that the monitoring was contrary to Section 316 (2) of the Czech Labour Code, as the employer had not presented any serious cause arising from the specific nature of its activities that would allow for the infringement of the employee's privacy in the workplace.

Subsequently, the case was brought before the Municipal Court in Prague, which, after conducting a test of adequacy, necessity and proportionality, upheld the position expressed by the Office for Personal Data Protection. According to the judgment, the monitoring measure in the form of GPS was not adequate, as it could not prevent the possible non-delivery of the parcel or the violation of the secrecy of correspondence. The necessity to apply this measure did not arise, as in order to achieve the desired objectives (optimisation of delivery districts, reliable service performance, etc.), it was sufficient to track only whether or not the postman had approached the delivery point. Moreover, the measure used did not pass the proportionality test, as it excessively interfered with the privacy of employees. Every movement of the delivery personnel was monitored, and they were under constant observation. On the other hand, the court pointed out that if the subject of the processing were only data concerning the place and time of visiting the delivery point, such a system would not constitute an interference with the privacy of employees within the meaning of Section 316(2) of the Czech Labour Code.

Analysing the above-mentioned cases, it can be concluded that the *sine qua non* condition for the lawful use of GPS as a means of monitoring in the workplace is to properly define its purpose and precisely limit the scope of the data whose processing is necessary to achieve it. It is also crucial where and how the GPS transmitter is installed, as this significantly affects the degree of privacy infringement.[636] Certainly, the amount of employee data of a personal nature

[636] Siskovičová, 2015, p. 81.

acquired in the case where employees are required to carry transmitters with them or where their work smartphones are tracked will be greater than in the case of tracking a vehicle used by the employee during working hours. Moreover, the danger of processing an overly broad catalogue of data and using it for a purpose that deviates from the original and legitimate intent was rightly pointed out by the now-defunct Article 29 Data Protection Working Party. In one of its opinions, the Working Party stated that "Vehicle tracking devices are not staff tracking devices. Their function is to track or monitor the location of the vehicles in which they are installed. Employers should not regard them as devices to track or monitor the behaviour or the whereabouts of drivers or other staff, for example, by sending alerts in relation to the speed of the vehicle."[637]

Nevertheless, the situation may change when the reason for installing this type of monitoring is to increase safety and reduce accidents at work. Tracking individual employees via GPS may be applicable in specific situations where such employees perform exceptionally dangerous work. The flagship example of such employees is miners, whose location tracking is an essential condition for safety and in relation to whom there is an ongoing discussion about what means of location tracking should be used so they are as resistant to damage and loss as possible.[638] Another example would be rescue workers participating in a rescue operation.[639] Nevertheless, even in such exceptional situations, it is important to remember that GPS monitoring focusing on individual employees must be used in accordance with the framework set out in national labour codes[640] and the GDPR.

2.1.1. GPS Monitoring Outside Working Hours

When discussing GPS as a means of monitoring in the workplace, one more issue needs to be resolved, namely, whether this form of monitoring can be used outside working hours. The prevailing opinion expressed, among others, by the Article 29 Data Protection Working Party[641] and the labour law doctrine of the Visegrad Group countries,[642] is that GPS monitoring should,

[637] Article 29 Data Protection Working Party, 2011, p. 14.
[638] See: Barański, M., Mirosławski, T., 2023, p. 13.
[639] Šmejkal, 2019, p. 81.
[640] Although Siskovičová primarily discusses compliance with the Slovak Labour Code, her position is universal and can be also applied to other workplace monitoring models – See: Siskovičová, 2015, p. 80.
[641] "Given the sensitivity of location data, it is unlikely that there is a legal basis for monitoring the locations of employees' vehicles outside agreed working hours." - See more: Article 29 Data Protection Working Party, 2017, p. 20.
[642] Dörre-Kolasa, D. 2023, p. 72; Siskovičová, 2015, p. 83; Šmejkal, 2019, p. 81; A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 34; Balogh, Hagedorn, Kiss, Polyák, Rátai, Szőke, 2012, p. 120, cited in Bankó and Szőke, 2016, p. 68.

in principle, only take place during working hours. However, what if the employer agrees to allow, e.g. a company car or electronic equipment to be used for the employee's private purposes as well? In such situations, as a rule (except for specific exceptions, which will be discussed in a moment), it is still considered that GPS monitoring may only take place during working hours.[643] This principle is to be implemented through a solution that allows employees to switch off the GPS tracking system when using the vehicle for private purposes, e.g. when travelling to a doctor's appointment. Dividing the use of the vehicle into "work mode" and "private mode" allows employees themselves to protect specific data and locations as private.[644] However, it should be recognised that this solution is particularly vulnerable to certain mistakes or even deliberate misuse by employees.[645] Employees may simply forget to switch on the GPS after a period of private use, especially since, in accordance with the "privacy by default" principle resulting from the GDPR, such a system should be switched to "private mode" to prevent tracking.[646] Moreover, they may also intentionally refrain from activating it, preventing the employer from achieving the purpose of monitoring.

However, there are certain exceptions where GPS monitoring of a vehicle or other object outside working hours will be proportionate and justified. Such exceptions include, among others, preventing theft of a vehicle or other object. In such situations, GPS tracking will take a different form than tracking throughout the entire period of use of the vehicle or object. Such a system should only be activated when the vehicle or object leaves the designated area. In addition, the location would be disclosed on a "break-the-glass" basis, which means that the employer could activate the visibility of the location of a given object only when it leaves a specifically defined territory.[647] This solution may indeed contribute to respecting the employee's privacy, but unfortunately, it may be contrary to the employer's interests – activating monitoring only after the stolen object leaves the specific territory may prove too late, which will ultimately prevent the employer from recovering it.

2.1.2. GPS Monitoring Principles

Considering the above and the fact that individual national workplace monitoring models do not establish any specific grounds in the context of GPS that differ from the forms of workplace

[643] Kuźnicka, 2018, p. 75.
[644] Article 29 Data Protection Working Party, 2017, p. 20.
[645] Dörre-Kolasa, 2023, p. 71.
[646] Stefański, 2021, p. 16.
[647] Article 29 Data Protection Working Party 2017, p. 20.

monitoring discussed above, attention should be paid to the principles stemming from the GDPR, which largely constitute an important source of reference for national models.

2.1.2.1. Data Protection Impact Assessment

Firstly, it should be noted that the employer (as data controllers or processors) should initially conduct a so-called data protection impact assessment before implementing GPS monitoring. Such an assessment should be carried out when data processing may potentially lead to a high risk against the rights and freedoms of natural persons (e.g. employees). The assessment allows for the evaluation, in particular, of the origin, the nature and the severity of that risk.[648] In accordance with Article 35 of the GDPR, a data protection impact assessment shall be performed when, *inter alia*, systematic and extensive evaluation of personal aspects relating to natural persons is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.[649] There is no doubt that the use of GPS as a form of monitoring in the context of employment fulfils the specified conditions, and therefore, such a test should be applied. The assessment should take into account various factors relating to GPS monitoring: what its purpose is, when it will be carried out, during what kind of tasks it will be used, where it will be located, etc. Some national DPAs explicitly indicate in which situations the use of GPS cannot be considered proportionate, thereby significantly limiting its applicability. An example of such a DPA is the Hungarian one, which clearly states that the sole protection of vehicle property, if it does not carry valuable goods or if its value is not significant, cannot constitute a valid justification for the usage of GPS tracking. The same conclusion applies to situations where the employee's place of work is a "home office"; in such cases, GPS monitoring will also be disproportionate.[650]

2.1.2.2. Data Protection by Design and by Default

[648] Recital 84 of the GDPR.
[649] Article 35 (3) (a) of the GDPR.
[650] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 34; Bankó and Szőke, 2016, p. 69.

Secondly, the GDPR imposes an obligation on employers to ensure that workplace monitoring measures are implemented in accordance with the principles of "data protection by design and by default".[651] Data protection by design means that the impact of a given monitoring measure on employees' privacy should be taken into account from the outset, in fact, even before the measure is implemented. As Fajgielski points out, data protection by design means "proactive, not reactive approach; preventive, not remedial."[652] In practice, this means that employers should not wait until there is an excessive breach of privacy and then apply corrective measures, but should strive to prevent such breaches from occurring in the first place.[653] When establishing the obligation to develop monitoring measures in accordance with the requirement of data protection by design, the European legislator indicates that the controller (in that case employer) when determining the means of processing and during the processing itself, should implement appropriate technical and organisational measures, such as pseudonymisation, designed to effectively implement data protection principles, such as data minimisation, and to provide the processing with the necessary safeguards to meet the requirements of the GDPR and protect the rights of data subjects.[654] The principle of "data protection by design" is closely related to the requirement for a "data protection impact assessment" described in the previous paragraph.

In turn, the principle of "data protection by default" is a manifestation of the principle of adequacy and minimisation.[655] Article 25 (2) of the GDPR imposes an obligation on employers to implement appropriate technical and organisational measures to ensure that, by default, only personal data that is necessary for the achievement of each specific purpose of processing is processed.[656] An example of such a measures is the GPS system discussed earlier, based on the employee's modes of travel - "at work" and "private" - which by default should be switched to the latter. The data protection by default applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.[657]

2.1.2.3. Information Obligation

[651] Recital 78 of the GDPR.
[652] Fajgielski, 2025, Art. 25.
[653] Fajgielski, 2025, Art. 25.
[654] Article 25 (1) of the GDPR.
[655] Fajgielski, 2025, Art. 25.
[656] Article 25 (2) of the GDPR.
[657] Fajgielski, 2025, Art. 25.

Thirdly, in accordance with the provisions of the GDPR, each employer must comply with the **information obligation**, i.e. fulfil the principle of transparency. In the context of GPS monitoring, this principle has been defined by the Article 29 Data Protection Working Party. The Working Party states that an employer must clearly notify employees that a tracking device has been installed in any company vehicle they operate and that their movements are being monitored while the vehicle is in use (and, where the technology permits, that driving behaviour may also be recorded). The information should be displayed prominently in each vehicle, in a location that is visible to the driver.[658] This position is consistent with, among other, the guidelines issued by the Polish and Hungarian DPAs, although the authorities draw attention to the need for a broader scope of information provided to employees, especially with regards to the purpose of monitoring, and detailed information about the data being processed – where it will be recorded, how long it will be stored, and who will have access to it.[659]

2.1.3. Consent as the Basis for GPS Monitoring

In terms of workplace monitoring in the form of GPS tracking, there is one more issue that is of significant importance for both this and other forms of workplace monitoring, and needs to be discussed. The issue at stake is the employees' consent as the basis for processing their data as part of GPS monitoring. In some countries of the Visegrad Group, it is indicated that pursuant to Article 6 (1) (a) of the GDPR[660], such consent may constitute a basis for GPS monitoring outside working hours when private use of the vehicle or other item belonging to the employer is permitted.[661] In accordance with the GDPR, such consent must be given freely and without any coercion.[662] However, in Recital 43, the Regulation states that in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller.[663] The employment relationship is precisely this kind of legal relationship whose inherent characteristic is the inequality of the parties (of the employer who is the controller and of the employee who is the data subject). Therefore, it should be concluded that "the regulations

[658] Article 29 Data Protection Working Party 2017, p. 20.
[659] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 33; Urząd Ochrony Danych Osobowych 2018a, p. 37.
[660] This article indicates that processing of the personal data might be lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes - Article 6 (1) (a) of the GDPR.
[661] Potyková, 2018/2019, p. 62; Urząd Ochrony Danych Osobowych 2018a, p. 38.
[662] Article 4 (11) of the GDPR.
[663] Recital 43 of the GDPR.

providing for the admissibility of consent to the processing of personal data do not apply to the employee`s data (including geolocation data). The specificity of the employer-employee relationship, and in particular the subordination of the employee and the inequality of the parties to the employment relationship (also informative), does not allow for full consent of the employee (…).”[664]

2.2. Personal Inspection in the Workplace

Another form of surveillance closely related to the protection of the employer’s property is the so-called personal inspection, which can take various forms, e.g. searching employees’ bags or clothes, as well as inspection using devices that detect various materials and substances. This form of control is highly controversial, primarily due to its physical nature and direct interference with the employee’s privacy.

Among the workplace monitoring models present in the Visegrad Group countries, we can distinguish models that do not directly mention the possibility of personal inspection (Poland and Hungary), as well as those that refer to this form of surveillance explicitly in the provisions of labour codes (the Czech Republic and Slovakia).

2.2.1. Personal Inspection in the Workplace Under the Polish and Hungarian Workplace Monitoring Models

In Poland, the lack of any regulation covering this form of surveillance prior to 2018 has resulted in two different positions regarding its admissibility. The first position, due to the lack of rules on this issue stated in the Labour Code, excluded the admissibility of personal checks of employees by the employer.[665] On the other hand, the second view, referring to the Supreme Court judgement of 13 April 1972[666] and the employer’s managerial powers, the employee’s subordination (Art. 22 of the PLC) and their obligation to care for the good of the workplace (Art. 100 §2 (4) of the PLC), stated that such a form of control, if carried out in an appropriate manner, should be considered acceptable.[667] This dispute has now lost some of its significance due to the 2018 amendment of the Labour Code, introducing Article 22^3 §4. Nevertheless, the

664 Barański and Giermak, 2017, p. 208.
665 Otto, 2023, p. 410.
666 Judgment of the Polish Supreme Court of 13 April 1972, I PR 153/72.
667 Smolski, 2015, pp. 75 – 94; Ziółkowska, 2013, pp. 131-142.

views and arguments of the supporters of the second position remain valuable, especially in the context of theoretical considerations concerning personal inspection, its origins, and, above all, the manner in which an employer can exercise such control.

Wujczyk, analysing the issue of personal inspection under the previous legal regime, pointed out that, as a rule, such inspection is admissible. However, this does not mean that it can take any arbitrary form. Firstly, the author points out that there must be justified grounds for the inspection activities. This means that the inspection must be aimed at protecting property and business secrets. However, it should be remembered that only an employee who could potentially come into possession of specific property or protected information may be subject to inspection. Secondly, the dignity of the employee plays an important role in the control process, as it constitutes the ultimate limit to the scope of control. The mere request by the employer to undergo an inspection does not constitute a violation of the employee's dignity, but if the inspection results in the humiliation of the employee, it should be discontinued.[668]

As indicated above, the key source for interpreting personal inspection as a form of workplace monitoring is the Supreme Court judgment of 13 April 1972. In the judgment, the Court indicated that "The widespread practice of searching employees in order to prevent the removal of company property, as provided for in work regulations or established customs, is lawful and does not violate the personal rights of employees when employees have been warned about the possibility of such checks being carried out to protect company property and when these checks are carried out in consultation with staff representatives in a manner that does not conflict with their socio-economic purpose or with the principles of social coexistence."[669]

A particularly important premise, referred to as a *sine qua non* condition of workplace monitoring in general, resulting from the above judgment, is the employer's obligation to inform employees about the inspection.[670] Informing an employee about the possibility of surveillance helps to preserve their dignity and demonstrates that the employee is recognised as a subject rather than an object of the employment relationship.[671] Furthermore, the significance of this premise is evidenced by the fact that in 2018, Articles 22^2 §6 and §7 were added to the Labour Code, which constitute its legal expression. The new regulation largely corresponds to the postulates raised by the doctrine.[672]

---

[668] Wujczyk, 2012, 2. Prawo pracownika do prywatności a kontrola osobista.
[669] Judgment of the Polish Supreme Court of 13 April 1972, I PR 153/72.
[670] Smolski, 2015, p. 84.
[671] Wujczyk, 2012, 2. Prawo pracownika do prywatności a kontrola osobista.
[672] Smolski, 2015, pp. 91-92; Wujczyk, 2012, 2. Prawo pracownika do prywatności a kontrola osobista; Ziółkowska, 2013, p. 133.

The court also points out that inspection should not contradict its socio-economic purpose and the principles of social coexistence. In practice, this means that inspection should only be carried out for the purpose, which is specified by law – in the case of Poland, this is ensuring 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[673] – and not, for example, for the purpose of additional punishment or intimidation of the employee. Moreover, the form of inspection must be proportionate to its specific purpose. If items of large size have been taken from the workplace, it will be difficult to justify searching employees' bags and pockets.[674]

The final premise indicated by the Supreme Court is the need to consult with employees' representatives. This premise has been partially reflected in Article 22^2 §6 of the Polish Labour Code, which states that "the objectives, the scope, and the manner of use of monitoring shall be established in a collective labour agreement or in the work regulations, or in an announcement if the employer is not covered by a collective labour agreement or is not obliged to adopt work regulations."[675] From the employees' point of view, the most preferred form of internal source of labour law, which specifies the objectives, scope and manner of conducting inspections, is a collective labour agreement, as the employees' side has the most rights and the greatest influence on its content during its negotiation. The current regulation maintains a certain balance between the need for consultation with employees' representatives and the employer's freedom to act, resulting from their managerial powers. Making the possibility of conducting an inspection entirely dependent on agreement with employees or on their consent could lead to the ineffectiveness of this form of monitoring. A similar position, albeit based on the previous legal situation, was expressed by Wujczyk, who pointed out that: "the lack of agreement with staff representatives regarding the conduct of personal searches does not automatically lead to a violation of dignity or an unlawful violation of an employee's privacy. A personal search conducted with respect for the dignity of employees cannot be considered illegal if they have been informed of the possibility of such a search being carried out."[676]

Despite the fact that personal inspection of employees has been regulated through Article 22^3 §4, it is still not entirely clear how exactly it should be carried out. Therefore, the fundamental value underlying the rules for conducting personal inspection should be respect for the dignity and privacy of the employee. This approach enables the inspection to be

[673] Art. 22^3 §1 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[674] Wujczyk, 2012, 2. Prawo pracownika do prywatności a kontrola osobista.
[675] Art. 22^2 §6 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).
[676] Wujczyk, 2012, 2. Prawo pracownika do prywatności a kontrola osobista.

conducted in a manner that is adaptable and provides extensive protection for the employee.[677] Therefore, it should be considered that searching an employee's clothing or luggage (bags, baskets, backpacks) should, in principle, be permissible, although in such a situation, the items in the bag or pockets should be removed by the employee himself or herself. In situations where an employee refuses to submit to an inspection, and there is a high probability that the employer's property has been stolen, the employer may call the police to carry out the inspection.[678] Another form of personal inspection, which seems to be less intrusive than searching an employee's personal belongings, is the use of specialised equipment by the employer, such as metal detectors or X-ray gates.[679] Such devices are commonly used in workplaces such as coin mints or warehouses.[680] Nevertheless, considering the dignity of the employee, it is unacceptable for the employer to conduct inspections in a manner that interferes with the physical integrity of the employee, i.e. searching parts of their body (e.g. mouth or nose) or ordering them to undress to their underwear or nakedness.[681] As contrary to the dignity of an employee, should be also considered the inspection of the employee by the internal security service, which might be employed by the employer for the purpose of protecting the workplace and property. According to the Act on the Protection of Persons and Property,[682] security guards are not authorised to conduct personal inspections of employees, even if such an authorisation or even an obligation is specified in their employment contracts.[683]

In view of the above, it is clear that the exact manner of conducting a personal inspection of an employee (classified as “other forms of monitoring”) has not been precisely defined by the legislator, thus leaving some discretion to the parties to the employment relationship, and above all to the employer. According to the views expressed in labour law doctrine, when conducting a personal inspection of an employee, attention should be paid primarily to his or her dignity. Nevertheless, given the broad scope for interpretation of the concept of “employee dignity” in the context of personal inspections, it may lead to many irregularities. On the other hand, as Smolski points out, referring to the currently forgotten educational function of labour law, honesty, reliability and trust should form the basis of labour relations, and any obligations or prohibitions should be secondary in nature.[684] Naturally, Smolski's position deserves support,

[677] Wujczyk, 2012, 2. Prawo pracownika do prywatności a kontrola osobista.
[678] Ziółkowska, 2013, 134.
[679] Wujczyk, 2012, 2. Prawo pracownika do prywatności a kontrola osobista.
[680] Ziółkowska, 2013, 134.
[681] Wujczyk, 2012, 2. Prawo pracownika do prywatności a kontrola osobista.
[682] Act on the Protection of Persons and Property of 22 August 1997, Dz.U.2025.532.
[683] Wąż, 2008, p. 6.
[684] Smolski, 2015, pp. 92 – 93.

but it should be remembered that currently, labour relations in Poland are based primarily on individual employment contracts, avoiding deviations from the rules set out in the Labour Code. Dialogue between social partners is conducted to a very limited extent, and the level of unionisation and coverage of employees by collective agreements is low.[685] Promoting good practices and mutual trust between the parties to an employment relationship in such conditions is extremely difficult, and very often, strict code regulations are more effective and desirable, especially for the employees.

Within the Hungarian monitoring model, doctrinal considerations on personal control are rather limited, but the issue has been the subject of proceedings before Hungarian courts and the DPA, which enables its analysis and comparison with other V4 countries' models. In the case of the Hungarian Labour Code, as in the Polish one, there is no specific provision comprehensively regulating the issue of personal inspection. However, as in Poland, the original source of this form of surveillance is indicated as the specific rights, obligations and interests of the parties to the employment relationship. One such source is, among others, the obligation of cooperation between the parties,[686] the protection of the legitimate interests of the employer,[687] or the employer's obligations in the field of occupational health and safety[688]. Furthermore, given the employer's managerial powers, it should be recognised that personal monitoring of employees, provided that their dignity and privacy are duly respected, is permissible in the sphere of employment.[689]

According to the above, it can be concluded that the provisions of the Hungarian Labour Code concerning the protection of personal rights and data management, specifically Sections 9 to 11/A, shall apply to the personal inspection of employees.

Firstly, it should be noted that the employee's personal rights may be restricted if the restriction is absolutely necessary for a reason directly related to the purpose of the employment

[685] According to statistics presented by OECD, collective barganing coverage in Poland in 2023 was at the level of 11.6 % and trade union density in 2022 was at the level of 9.4 %. In both cases, the trend is downward. – See: OECD Data Explorer, Collective Bargaining Coverage, https://data-explorer.oecd.org/vis?lc=en&df[ds]=dsDisseminateFinalDMZ&df[id]=DSD_TUD_CBC%40DF_CBC&df[ag]=OECD.ELS.SAE&dq=..&pd=2000%2C&to[TIME_PERIOD]=false&vw=tb (Accessed: 3 May 2026); OECD Data Explorer, Trade Union Density, https://data-explorer.oecd.org/vis?tm=trade%20union&pg=0&snb=81&df[ds]=dsDisseminateFinalDMZ&df[id]=DSD_TUD_CBC%40DF_TUD&df[ag]=OECD.ELS.SAE&df[vs]=1.0&dq=..&ly[cl]=TIME_PERIOD&ly[rs]=REF_AREA&to[TIME_PERIOD]=false&lom=LASTNPERIODS&lo=10&vw=tb (Accessed: 3 May 2026); See also: Adamczyk, 2025, pp. 91-94.

[686] Section 6 (2) of Act I of 2012 on the Labor Code (Hungarian Labour Code).

[687] Section 8 of Act I of 2012 on the Labor Code (Hungarian Labour Code).

[688] Section 51 (4) of Act I of 2012 on the Labor Code (Hungarian Labour Code).

[689] Hadady-Lukács, 2024, p. 1460.

relationship and is proportional to the achievement of the goal.[690] This means that, before introducing personal inspections, the employer should first balance the interests involved - compare the objective to be achieved through the inspections with the degree of infringement of the employee's personal rights, in this case primarily privacy and dignity.[691] In the field of employment, the employer's legitimate interest will constitute the basis for inspection.[692] Moreover, it is also important for the employer to comply with the principle of data minimisation,[693] i.e. to process only the data that are necessary to achieve a legitimate purpose.[694]

Under the Hungarian model of workplace surveillance, great importance is attached to respecting the dignity of employees, which is also a characteristic feature of the Polish model. Admittedly, following the amendment of the Hungarian Labour Code in 2019, the provisions regulating monitoring have been reformulated and no longer contain a direct obligation to respect human dignity, but as I have already pointed out, this obligation stems from the general principles of labour law and is universally applicable. As indicated in the doctrine, human dignity may be violated if the inspection is carried out in an inappropriate manner or by disproportionate means, e.g. when an employee is ordered to undress completely during a search; when the inspection is carried out by a person of the opposite sex; when it takes place in a public place, in front of other employees; or when the employee who is to be inspected is randomly selected.[695] Often, forms of personal inspection, such as metal detection gates or baggage X-rays, allow employers to better achieve their goal of securing their property without violating the dignity of employees, as they do not interfere with their privacy as much as, for example, a physical search of their clothing.

Considering that the provisions of the Labour Code will apply to personal inspections, another condition, which, as in Poland, can be called a *sine qua non* condition, is prior notification of the employee.[696] The information is to be provided to the employee in writing,

---

690 Section 9 (2) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
691 Hadady-Lukács, 2024, p. 1461.
692 The Hungarian DPA pointed out that "during the course of employment, the employer may restrict the privacy of employees in certain, precisely defined cases in order to ensure the proper functioning of the employer's economic activities, while maintaining guarantee requirements." - A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013, p. 3. Conducting a proportionality test also satisfies the requirements for data processing compliance with the law specified in Article 6 of the GDPR, specifically point (f).
693 Article 5 (1) (c) of the GDPR.
694 Hadady-Lukács, 2024, pp. 1461-1462.
695 Hadady-Lukács, 2024, p. 1462.
696 Section 11/A (1) of Act I of 2012 on the Labor Code (Hungarian Labour Code).

and its content should include the conditions and expected duration of the restriction of personal rights, as well as the justification for the necessity and proportionality of the inspection.[697]

Another questionable issue with regard to personal inspections is the possibility of such inspections being carried out by security personnel employed by the employer. Hadady-Lukács points out that in such a situation, reference should be made to the provisions of the Act on the rules governing personal and property protection and private investigation activities[698].[699] According to Section 28 of the Act, in order to enforce his obligations arising from the contract, the security guard may request the presentation of the contents of the package, vehicle and shipment, if: 1. there are reasonable grounds to believe that the person concerned is in possession of items originating from a criminal offence or administrative offence, the safekeeping of which is the security guard's contractual obligation; 2. the person concerned fails to hand over the items despite being requested to do so; 3. the measure is necessary to prevent or interrupt the unlawful act.[700] On the other hand, the Hungarian DPA, in one of its decisions, presents an opposing position, in which it indicates that the employer monitoring must remain within the realm of labour law, and the rules of the Act on the rules governing personal and property protection and private investigation activities cannot be applied to such monitoring.[701] In its effects, the position expressed by NAIH is consistent with the prevailing view expressed in Polish labour law doctrine that personal inspection of an employee carried out by security guards employed for this purpose has no legal basis in the provisions of the Labour Code and may be contrary to the dignity of the employee.

The issue of personal inspection of employees was also addressed by the Hungarian Supreme Court in two judgments and was considered by the Hungarian DPA in one of its decisions. The cases in question, which will be briefly discussed below, are extremely important in the context of analysing personal inspections of employees, as they provide guidance on how such inspections should be carried out in practice. Moreover, their significance is all the greater given that the number of sources discussing the issue of personal inspection within the Hungarian labour law doctrine is extremely limited.

[697] Hadady-Lukács, 2024, p. 1462.
[698] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól.
[699] Hadady-Lukács, 2024, p. 1462.
[700] Section 28 (1) of 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól.
[701] Decision of NAIH, NAIH/2017/439/H, p. 13.

The first case, decided by the Supreme Court under reference number Mfv.I.10.427/2016/4,[702] concerned the immediate termination of employment of two senior employees (a security manager and a customer service director). According to the employer's justification, the first employee was dismissed because he asked the second employee (customer service director) to order another employee (chief cashier’s assistant) to strip down to her underwear during a clothing inspection. In turn, the second employee was dismissed because, at the request of the security manager (who was not his supervisor), he actually instructed the employee he supervised (the chief cashier's assistant) to strip down to her underwear during the inspection. The reason for the personal inspection of the employee was the alleged theft of 30,000 forints from the shop's cash register. When deciding on this case, the court ruled that the dismissal of the employees was lawful and drew attention to several important issues concerning the personal inspection of an employee.

Firstly, the Court placed significant emphasis on the person conducting the inspection. In this case, the Kúria found that the person conducting the inspection (a customer service director) was not authorised to do so. Furthermore, the court pointed out that a serious breach of employee obligations is when an employee, at the request of a person of the same rank in the company but holding a different position (such as a security manager in relation to a customer service director), takes action against his subordinate that goes beyond the scope of his duties and authority. Such action may lead to a violation of the subordinate's dignity, and immediate dismissal in such a case should be considered justified.

Secondly, the court addressed the issue of the employee's consent to the inspection and pointed out that in the case of the employer's surveillance activities, the employee's consent is irrelevant, as the employment relationship is hierarchical in nature and the employer has a dominant role in it.

Furthermore, the court also pointed out that the information obligation had not been fulfilled – employees had not been informed about the possibility of surveillance measures that would restrict their personal rights.

The final issue addressed by the court was the principle of proportionality, pointing out that the purpose of surveillance could have been achieved by less intrusive means than a personal inspection, leading to the employee being stripped to her underwear.

The second judgment that should be mentioned - Mfv.X.10.281/2019/4 – was issued in a case concerning a routing and systematic procedure of checking employees’ bags, backpacks

[702] Judgment of Kúria (Curia/Supreme Court), Mfv.I.10.427/2016/4.

and other personal luggage by the employer.[703] Referring to the earlier decision of the NAIH and the district court ruling in this case, the Supreme Court drew attention primarily to the inappropriate legal basis for the inspection invoked by the employer. The Court pointed out that Section 28 (1) of the Act on the rules governing personal and property protection and private investigation activities does not constitute a general authorisation to inspect employees' parcels. Moreover, as in the previously cited Kúria judgment and in accordance with the position expressed in this thesis, the court indicated that the employer cannot also rely on the employee's voluntary cooperation regarding the inspection, as consent can only be valid if the employee has the opportunity to make a genuine and free choice, which is not the case when it comes to an employment relationship.

Analysis and comparison of the above judgments of the Hungarian Supreme Court allows the identification of certain principles, or rather a framework, from which personal inspection of an employee should not deviate. Firstly, a personal inspection must be carried out by an authorised person; secondly, the employee's consent does not constitute a valid basis for the inspection, as the employee is in a subordinate position to the employer, which prevents him or her from giving his or her consent freely; thirdly, the manner in which the inspection is carried out must respect the principle of proportionality – if the objective indicated by the employer can be achieved by other means, a personal inspection is not permitted; and fourthly, informing the employee about the possibility, method and duration of the inspection is a necessary but not the only condition for the inspection to be considered legal – it is extremely important for the employer to properly state the legal basis of it.

When analysing the issue of personal inspection within the Hungarian workplace monitoring model, it is necessary to refer to the decision of the Hungarian DPA, ref. NAIH/2017/439/H,[704] in which NAIH takes a comprehensive approach to the rules according to which personal inspection of an employee may be carried out. In this case, personal inspection took the form of random checks of employees' luggage as they were leaving work. The data protection authority found that the processing of data in connection with the inspection of the employee's luggage by the employer was unlawful.

The authority justified its decision primarily on the grounds that the data processing was based on an incorrect legal basis – when conducting the inspection, the employer referred to the provisions of the Act on the rules governing personal and property protection and private investigation activities. The NAIH pointed out that the common practice of randomly selecting

[703] Judgment of Kúria (Curia/Supreme Court), Mfv.X.10.281/2019/4.
[704] Decision of NAIH, NAIH/2017/439/H.

employees to show the contents of their luggage or having it unpacked by a security guard in order to protect the employer's property without any specific justification is not in accordance with the provisions of this Act. The Act on the rules governing personal and property protection and private investigation activities allows security guards to request employees to show their luggage (security guards do not have the right to touch, open, unpack or order the opening of luggage) only if all three conditions set out in Section 28 of the Act are met. Therefore, there must be reasonable grounds to believe that the person concerned is in possession of items originating from a criminal offence or administrative offence, the safekeeping of which is the security guard's contractual obligation; the person concerned fails to hand over the items despite being requested to do so; and the measure is necessary to prevent or interrupt the unlawful act.[705][706] Furthermore, if an employer would like to rely on the Property Protection Act during an inspection, they would have to prove that violations by employees occurred regularly and that personal inspection is necessary to prevent them because, as the Hungarian Constitutional Court pointed out "only a real and direct, rather than a potential, threat can be interpreted as a constitutional criterion that meets the requirement of purposefulness of data processing"[707].[708]

In further considerations regarding the legal basis for personal inspections, the authority indicated that the employee's consent cannot constitute such a basis, as it would have to be voluntary, which is doubtful in the context of the relationship between the employee and the employer.[709] Therefore, with regard to employment, the legal basis for data processing, including personal inspection, may be constituted by the legitimate interest of the employer. If such an interest exists, the employer may, without the consent of the employees, restrict their privacy, but only in specific cases and only in accordance with the guarantees laid down by law.[710] According to the current legal status, such guarantees should be considered to be the principles set out in the GDPR (in particular Article 5) and Section 9 (2) of the Labour Code, according to which a personal inspection is permissible when it is absolutely necessary in connection with the purpose of the employment relationship and is proportionate to achieving that purpose,[711] as well as Section 11/A of the Labour Code, according to which a personal inspection may be carried out if it serves to verify the employee's behaviour in connection with

---

[705] Section 28 (1) of 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól.
[706] Decision of NAIH, NAIH/2017/439/H, pp. 10-11.
[707] Decision of the Hungarian Constitutional Court, 35/2002. (VII. 19.).
[708] Decision of NAIH, NAIH/2017/439/H, p. 13.
[709] Decision of NAIH, NAIH/2017/439/H, p. 14.
[710] Decision of NAIH, NAIH/2017/439/H, p. 14.
[711] Section 9 (2) of Act I of 2012 on the Labor Code (Hungarian Labour Code).

the employment relationship.[712] Furthermore, a necessary condition for recognising the employer's interest as a legitimate basis for a personal inspection of an employee is to carry out a balancing test of interests. The first step in such a test is to determine the nature and source of the legitimate interests of the data controller (employer) and to assess the impact of the planned measure on the data subject (employee). Weighing these two sides will lead to achieving a “provisional balance”; however, if, after the balancing, there are still doubts about the relation of the interest and rights of both parties, the next step is to evaluate additional safeguards for the data subject, which may tilt the balance in favour of legitimate data processing.[713] In other words, if the test concludes that the employer's legitimate interest outweighs the employee's right to privacy, a personal inspection may be carried out.[714]

The NAIH also drew attention to the principle of proportionality, pointing out that when monitoring the behaviour of employees in connection with their employment relationship, the employer must first apply a method that does not lead to data processing. Only when such a measure is not possible, the employer should implement a method that will lead to the processing of as little data as possible, only as much data as is necessary to achieve the indicated objective. Therefore, before implementing inspections, the employer must prove that other methods would not be effective in protecting the employer's property. In such a case, the justification for personal checks may be regularly recurring violations of the employer's property by employees, which cannot be eliminated by other means.[715]

Moreover, when conducting an inspection, the employer must follow an appropriate procedure to protect the employee from excessive invasion of privacy and, as a result, dignity. One of the measures to protect employees is to conduct inspections in a separate room to ensure adequate privacy. At the employee's request, another person, e.g. a trade union representative, should also be allowed to be present during the inspection. It is also good practice to draw up an inspection protocol and specify a detailed inspection procedure, e.g. in the work regulations, including what to do if an employee refuses to participate in the inspection.[716] As already indicated in Polish and Hungarian doctrine, the Hungarian data protection authority takes the view that an acceptable (it could even be said preferred) method of conducting less invasive checks is the use of metal detectors and X-ray baggage screening equipment, which enable the

[712] Section 11/A of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[713] Article 29 Data Protection Working Party, 2014.
[714] Decision of NAIH, NAIH/2017/439/H, p. 15.
[715] Decision of NAIH, NAIH/2017/439/H, pp. 15-16.
[716] Decision of NAIH, NAIH/2017/439/H, p. 16.

detection of employer property being removed from the workplace.[717] However, it should be remembered that due to the exceptionally private nature of an employee's luggage and clothing (if such clothing is private), even during such forms of personal inspection, the employer may obtain information about the employee that is deeply rooted in their private life, to which the employer should not have access under any circumstances.

The last issue highlighted by the authority was the employer's obligation to provide information in connection with data processing. In this case, although the employer informed employees about the possibility of an inspection, the information provided did not contain all the required elements, including the conditions for data processing. Under the Hungarian model of workplace monitoring, the importance of the information obligation is emphasised by the practice of the Constitutional Court, according to which Article 6(3) of the Hungarian Constitution[718] – the right to personal data protection – implies that everyone has the right to know who, where and for what purpose their personal data is being used.[719]

To summarise, the approach to personal inspection in the Polish and Hungarian models of employee monitoring, it should be noted that neither of the two labour codes explicitly regulates this form of monitoring, but rather sets out a certain framework, which has been filled in by doctrine, case law and the practice of personal data protection authorities. Both models recognise that personal inspection of employees is a form of surveillance that significantly interferes with their privacy; however, considering the employer's managerial powers and the employee's duty to care for the best interests of the employer’s establishment, as expressed in both regulations,[720] its use should be allowed, but only in respect of the relevant rules.

Firstly, the inspection must be carried out on the basis of a specific legal basis, which in both cases may be the employer's interest. However, it should be noted that in the Polish model, the employer's interest in relation to personal inspection has been limited to ensuring 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.[721] Whether the employer’s interest constitutes a legitimate basis for personal inspection must be assessed on the basis of a balancing test, which the employer is required to carry out before applying monitoring, and the exact procedure for which was referred to by the Hungarian DPA in its decision, ref. NAIH/2017/439/H.

[717] Decision of NAIH, NAIH/2017/439/H, p. 16.
[718] Article 6 (3) of the Fundamental Law of Hungary of 25 April 2011.
[719] Decision of NAIH, NAIH/2017/439/H, p. 17.
[720] The employee’s obligation to take care of the best interests of the employer’s establishment is directly expressed in Article 100 §2 (4) of the Polish Labour Code, and in the case of Hungarain regualtion, it can be inferred from Section 8 (1) of the Hungarian Labour Code.
[721] Art. 22^3 §1 of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code).

Furthermore, the employer's interests must be genuinely at risk, and therefore regular direct personal inspections, e.g. by randomly selecting employees to be subjected to such surveillance under the pretext of preventive measures, should be considered unacceptable. However, there is a less intrusive form of inspection that can be preventive in nature and is accepted in both countries: security gates and luggage X-ray machines. Both models reject employee consent as an acceptable basis for inspection.

Moreover, in both cases, it should be noted that a necessary condition for conducting an inspection is the fulfilment by the employer of the information obligation, the scope of which, both in relation to Poland and Hungary, has already been described in an earlier section of this paper.

The final remark concluding this brief summary is that in both the Polish and Hungarian models, great importance is attached to the dignity of the employee, which sets the ultimate limits of the admissibility of a given form of monitoring – this also indicates the strong axiological roots of labour law in both countries.

2.2.2. Personal Inspection in the Workplace Under the Czech and Slovak Workplace Monitoring Models

Under the Czech and Slovak labour codes, the legislator directly refers to personal inspections, allowing this form of employee monitoring. Furthermore, the regulations governing this issue in both countries are remarkably similar and, in part, even identical. These provisions are Section 248 of the Czech Labour Code and Section 177 of the Slovak Labour Code.

The mentioned sections reflect the protective function of labour law and the specific principle of employee protection expressed in Section 1a (a) of CLC and Article 1 of the SLC. Nevertheless, they stipulate the employer's right to monitor employees, which stems from the organisational function of labour law.[722]

The wording of the first paragraph of both sections is, in fact, identical and indicates that the employer shall create such working conditions for employees so that they can duly perform their working tasks without hazards to their lives, health and property. If deficiencies are found, the employer is obliged to take measures to eliminate them.[723] Therefore, the provisions establish the obligation of preventive measures on the employer. This obligation is further

[722] Filípek, 2020/2021, p. 108
[723] Section 248 (1) of the CzechLABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce"; Section 177 (1) of the Slovak Labour Code.

specified in other provisions of the Czech and Slovak labour codes, including Section 101 of the CLC regulating preventive obligations in the field of occupational health and safety,[724] Section 224 of the CLC setting out the employer's obligation to provide the employee with safe working conditions,[725] Section 226 of the CLC indicating the need for the employer to provide a place where clothes and other personal items brought to the workplace by the employee will be safe[726][727], and Article 8 of the SLC imposing an obligation on employer to take appropriate measures to protect the life and health of employees at work[728].

On the other hand, the second paragraphs of the analysed provisions express the employer's interest in protecting its property and the workplace from hazards associated with, for example, employees bringing weapons or other dangerous items to work.[729] The provisions state the grounds for the employer to carry out checks on things which employees bring to and take away from the premises. However, it should be noted that, in addition to allowing employers to check items brought into and taken out of the workplace by employees, Czech regulation, in contrast to the Slovak one, also explicitly authorises employers to conduct a body search of employees. Nevertheless, Slovak labour law doctrine indicates that inspection of items is a broad concept covering not only the inspection of luggage, but also employees' clothing (pockets), means of transport, as well as places where employees can store certain items, and even employees' offices.[730]

A problematic issue, which is also present in the Polish and Hungarian workplace monitoring models, is that the above provisions do not specify how in detail a personal inspection may be carried out. The Czech legislator merely indicated that a body search may only be carried out by a natural person of the same sex,[731] which, was questioned by Siskovičová, who pointed out that in practice such a solution is extremely complicated and burdensome for employers who hire both women and men, because if an inspection is necessary, they must ensure that it is carried out by at least one male representative and one female representative.[732] In turn, the

[724] Section 101 of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".
[725] Section 224 of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".
[726] Section 226 of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".
[727] Filípek, 2020/2021, p. 108.
[728] Article 8 of the Slovak Labour Code.
[729] This conclusion by Štefko refers only to Czech regulations, but given the similarity between Paragraph 2 of Section 248 of the CLC and Paragraph 2 of Section 177 of the SLC, it can certainly be assumed that the author's statement can be attributed to both - See: Štefko, 2023, p. 154.
[730] Siskovičová, 2015, p. 78.
[731] Section 248 (2) of the Czech LABOUR CODE (full translation) No. 262/2006 Coll.
[732] Siskovičová, 2015, p. 78.

Slovak legislator indicated that the detailed terms and conditions of inspections shall be specified by the employer in the work regulations.[733]

Subsequently, it has to be noted that the possibility of conducting personal inspections should not be treated solely as an employer's entitlement, but as their obligation. According to a ruling by the Czech Supreme Court, ref. 21 Cdo 2172/2002, also cited by Slovak doctrine,[734] the employer has a duty to systematically monitor employees and should do so in a manner that minimises the risk of potential damage.[735] However, this does not mean that there are no limits on how a personal inspection may be carried out.

Firstly, such monitoring should only be carried out to the necessary extent and with respect for the employee's privacy and dignity. Moreover, it is also important to keep in mind the principle of proportionality, which applies to this provision and within the framework of which the interests and rights of the employer and the employee must be balanced, *inter alia,* by assessing the adequacy of the control measures applied and their burden on the employees to whom they are applied.[736] An example of a disproportional inspection that would interfere with an employee's privacy to an excessive degree would be a search involving the inspection of desks and filing cabinets during the employee's absence. An employee may reasonably assume that his desk and document cabinets belong to his private sphere, as he may store private items in them.[737]

Moreover, as indicated within the Polish and Hungarian workplace models, a necessary condition for conducting an inspection is that the employee must be properly informed about it.[738]

However, unlike in the case of Poland and Hungary, in the Czech Republic and in Slovakia, the inspection might be carried out by third parties, such as security agencies. In such a situation, it is important that the agency entrusted with the task indicated in Paragraph 2 of Section 248 of the CLC and Paragraph 2 of Section 177 of the SLC should act on the basis of a contractual relationship and have the appropriate authorisation from the employer.[739]

[733] Section 177 (2) of the Slovak Labour Code.
[734] Siskovičová, 2015, p. 78.
[735] Judgment of the Czech Supreme Court of 7 May 2003, 21 Cdo 2172/2002.
[736] Filípek, 2020/2021, p. 109.
[737] This conclusion can be drawn from the ECtHR judgment in Peev v. Bulgaria from 26 October 2007 (Application no. 64209/01), in which the court indicated that "a search which extended to the employee's desk and filing cabinets must be regarded as an interference with his private life.". This judgment was cited by Štefko in a similar context - See: Štefko, 2012, p. 19.
[738] Siskovičová, 2015, p. 78.
[739] Kyselková, 2013; Siskovičová, 2015, p. 78.

A situation where an employer discovers during a control that an employee has engaged in conduct that violates the employer's interests, e.g., by stealing equipment belonging to the employer, may lead to a finding of serious breach of work discipline and immediate dismissal of the employee.[740]

Considering Section 3 (2) (a) of the Czech Civil Code and Section 11 of the Slovak Civil Code, which regulate the right of individuals to protection of life and health, it should be noted that an employee may refuse a given form of inspection due to health reasons if it could endanger their health (e.g., not every employee can undergo an inspection using a metal detector or X-ray). However, such an employee must undergo a personal inspection carried out in another form. It should be remembered that such an inspection must be consistent with human dignity.[741]

3. Occupational Health and Safety

In addition to ensuring that employees perform their duties properly, checking whether their behaviour breaches the terms of their employment contract and safeguarding the company's property, another area of vital importance to employers is compliance with occupational health and safety regulations in the workplace and the closely related to it issue of employees' readiness to work, understood as the physical and mental capacity enabling an employees to perform their duties.[742]

In the labour law systems of all Visegrad Group countries, employees' right to health and safe working conditions, and the general obligation of the employer to ensure such conditions have been enshrined, both at the constitutional level[743] and within the labour codes[744].

One of the greatest risks to health and safety in the workplace, which also has a negative impact on employees' readiness for work, is the consumption of alcohol and other intoxicating substances by employees and being under their influence during working hours. As the Polish

740 Štefko, 2023, p. 154; Judgement of the Czech Supreme Court of 21 January 2014, 21 Cdo 1496/2013; Judgement of the Czech Supreme Court of 17 October 2012, 21 Cdo 2596/2011.
741 Siskovičová, 2015, p. 79.
742 Kuba, 2014, Rozdział 4 Formy kontroli gotowości pracownika do wypełniania obowiązków pracowniczych.
743 Article 66 (1) of the Constitution of Poland of 2 April 1997, Dz.U.1997.78.483; Article 28 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.); Article 36 of the Constitution of the Slovak Republic of 1 September 1992, 460/1992 Zb.; Article XVII (3) of the Fundamental Law of Hungary of 25 April 2011.
744 See: Articles 15, 94 (4) and 207 (2) of Act of 26 June 1974 Dz.U.2023.1465 Labour Code (Polish Labour Code); Sections 101, 102 and 103 of "Zákoník prace" No. 262/2006 Coll., as amended (full translation) (Czech Labour Code); Sections 146, 147, 148 of the Slovak Labour Code (Zákon č. 311/2001 Z. z.); Section 51 of Act I of 2012 on the Labor Code (Hungarian Labour Code).

Supreme Court rightly pointed out in its judgment of 7 March 2006, the mere physical presence of an employee in the workplace does not fulfil the obligation to perform work if the employee is not ready to do so. An employee must be at the employer's disposal, that is, ready to work, which in turn implies the employee's subjective intention to perform work and the objective ability of doing so. There is no doubt that an employee's intoxication automatically precludes their readiness to work.[745] Moreover, being under the influence of psychoactive substances can have a negative impact not only on the health and safety of employees and employers but also on third parties. It can also lead to absenteeism and is significantly linked to workplace stress.[746]

This issue of being sober at work becomes even more significant when considering statistics which show that between 5% and 20% of the working population in Europe has problems related to alcohol or drug use.[747] Furthermore, looking at the Visegrad Group countries, there is a noticeable tendency for per capita consumption of pure alcohol in the region to be higher than the average per capita consumption of pure alcohol in the entire EU.[748] A particularly disturbing phenomenon is morning drinking before work. In 2024, one of Poland's leading daily newspapers, "*Rzeczpospolita*," citing a report prepared by the market research centre "*Centrum Monitorowania Rynku*" on alcohol sales and consumption in Poland in the first half of 2024, indicated that between 5:00 a.m. and 12:00 p.m., Poles buy around 2.6 million beers, including 402 thousand strong beers. In the morning hours, the so-called "*małpki*" – 100 ml bottles of vodka or other strong alcohol – are also a frequent choice, with sales of around 410 thousand bottles.[749]

It should be stated that employers should have a means by which they can monitor compliance with the occupational health and safety rules, particularly with the obligation of employees to be sober during work. Under all workplace monitoring models in the V4 countries, employee sobriety checks are permissible, although their regulation takes different forms. Some legislators, such as those in Poland and, to some extent, in the Czech Republic, have decided to address this issue directly in their labour codes. On the other hand, the Slovak legislator has regulated the issue of employee sobriety checks directly in the Health and Safety

745 Judgment of the Polish Supreme Court of 7 March 2006, I UK 127/05.
746 Chikritzhs and Livingston, 2021, pp. 1-15; Borrelli, Santoro, Gualano, Perrotta, Daniele, Amantea and Moscato, 2022, pp. 1-2; Sygit-Kowalkowska and Ziółkowski, 2019, pp. 109 - 130.
747 European Union Drugs Agency, 2022.
748 The average consuption of pure alcohol per capita accross the EU is 10.1 liters. In the Visegrad Group countirs, the figures are as follows: Czech Republic – 12.7 liters, Poland – 11 liters, Hungary – 10.8 liters and Slovakia – 10.3 liters – See: WHO indicators on pure alcohol consumption, litres per capita, age 15+, https://gateway.euro.who.int/en/indicators/hfa_426-3050-pure-alcohol-consumption-litres-per-capita-age-15plus/#id=19443 (Accessed 3 May 2026).
749 Rzeczpospolita, 2024.

Act, while in the Hungarian model, this form of supervision only indirectly stems from Section 51 (4) of the Labour Code and the provisions of the Occupational Safety Act[750] (among others, Section 4, Section 54 (7) (a)-(b) and Section 60 (1)).

In light of the above, the next section, which also concludes the chapter on the objectives and forms of employee monitoring in the Visegrad Group countries, will focus on sobriety monitoring. Although the nature of this type of monitoring is to a certain extent different from the other forms of monitoring already analysed in this chapter, without any doubt, it can be included in the concept of "employee monitoring," especially when understood broadly, as in the case of this thesis.

Furthermore, this study pays particular attention to sobriety monitoring because, firstly, as the statistics cited above show, sobriety in the workplace remains a pressing issue in the Visegrad Group countries, secondly, amongst the methods of controlling compliance with health and safety rules in the workplace, it most closely fits within the framework of "monitoring" and constitutes, in a sense, a severe intrusion into the "private sphere of the employee," ultimately leading to a restriction of behaviour dependent mainly on the employee's free will (of course, we cannot speak of free will in the case of addiction to psychoactive substances).

3.1. Sobriety Monitoring

3.1.1. Sobriety Monitoring Under the Polish Workplace Monitoring Model

Starting with the Polish model, it should first be noted that the obligation to remain sober at work has been defined and classified as one of the fundamental obligations of an employee by the jurisprudence of the Supreme Court[751] and legal doctrine,[752] but has not been explicitly stated in the Labour Code. Moreover, according to the legal status in force until 20 February 2023, the issue of sobriety testing in the workplace was not regulated in the Labour Code, but in the Act on Upbringing in Sobriety and Counteracting Alcoholism[753] and in Regulation of the Minister of Health and the Minister of Internal Affairs and Administration of 28 December

---

[750] 1993. évi XCIII. törvény a munkavédelemről (Act XCIII on Occupational Safety).
[751] Judgment of the Polish Supreme Court of 23 July 1987, I PRN 36/87, OSNC 1989/2, Item 32; Judgment of the Polish Supreme Court of 7 March 2006, I UK 127/05, LEX nr 299138; Judgment of the Polish Supreme Court of 4 December 2018, I PK 194/17, OSNP 2019/6, item 73.
[752] Czichy, 2009, pp. 29-35; Majchrzak, 2015, pp. 151-167; Jaskulska, 2023, pp. 39-46.
[753] Act on Upbringing in Sobriety and Counteracting Alcoholism of 26 October 1982, Dz.U.2023.165.

2018 on testing for alcohol content in the body[754]. Article 17 of the Act on Upbringing in Sobriety and Counteracting Alcoholism set out the rules on how the obligation to prevent an employee under the influence of alcohol from working can be enforced, as it stated that:

1. The head of the workplace or a person authorised by him shall be obliged to prevent an employee from working if there is a reasonable suspicion that he has come to work under the influence of alcohol or has consumed alcohol during working hours. The circumstances giving rise to the decision shall be communicated to the employee.
2. At the request of the head of the workplace, a person authorised by him, or at the request of an employee who is reasonably suspected of coming to work under the influence of alcohol or of consuming alcohol during working hours, a sobriety test shall be carried out by an authorised body appointed to protect public order. In turn, blood sampling may only be performed by a person with the appropriate professional qualifications.[755]

On the basis of the previous regulation, three main conclusions can be drawn. The first conclusion is that preventing an employee from working in the circumstances specified in Article 17 of the Act on Upbringing in Sobriety and Counteracting Alcoholism was an absolute obligation of the employer, not a right. In this regard, the legislator did not leave the employer any discretion, but required it to undertake specific actions.[756] Secondly, the decision to prevent an employee from working could only be based on reasonable suspicion. The suspicion did not have to be confirmed by a sobriety test, as it was enough that the behaviour of the concerned employee indicated that he or she was under the influence of alcohol, e.g. the employee was staggering, mumbling or smelled of alcohol.[757] This has been indirectly confirmed by the Supreme Court, which indicated that "in proceedings before authorities examining disputes concerning employees' claims arising from their employment relationship, any evidence may be adduced to prove that the employee was intoxicated on a specific date, justifying his exclusion from work or removal from work and entitling the employer to apply other sanctions provided by law."[758] Thirdly, it follows from the wording of the provision that an employee's

[754] Regulation of the Minister of Health and the Minister of Internal Affairs and Administration of 28 December 2018 on testing for alcohol content in the body, Dz.U.2018.2472.
[755] Article 17 of Act on Upbringing in Sobriety and Counteracting Alcoholism of 26 October 1982.
[756] Kuba, 2014, 4.2.1. Kontrola trzeźwości pracownika w polskim systemie prawnym, in: Prawne formy kontroli pracownika w miejscu pracy.
[757] Kuba, 2025, Art. 22(1c)) Przesłanki wprowadzenia i sposób przeprowadzenia kontroli trzeźwości pracowników.
[758] Resolution of the Polish Supreme Court of 14 December 1978, V PZP 7/78, OSNC 1979/2, Item 21.

sobriety could only be tested by an authorised body appointed to protect public order, e.g. by the police.[759]

Based on the above conclusions, the limitations of the previous regulation are clearly visible. Firstly, the fact that, under the wording of Article 17 of the Act on Upbringing in Sobriety and Counteracting Alcoholism, employers were not allowed to carry out preventive checks should be assessed critically. An employer could only decide to prevent an employee from working if there was reasonable suspicion that the employee was under the influence of alcohol. Secondly, the regulation prevented employers from conducting sobriety tests, stating that this should be done only by an authority appointed to protect public order. The impossibility of conducting such tests by employers has been confirmed by the Polish DPA, which stated in one of its opinions that Article 17 of the Act on Upbringing in Sobriety and Counteracting Alcoholism excludes random or preventive breathalyser tests of employees.[760] This solution should definitely be considered unfavourable, especially in light of the obligations of the employee and the employer. As previously indicated, the employee has an obligation to remain sober at work. In order for this obligation to be enforced in reality, compliance with it must be monitored. Considering that inappropriate behaviour by an employee caused by their intoxication may have negative consequences, primarily for the workplace and other employees, the employer, as the person responsible for the workplace and workforce, should first and foremost have appropriate control powers to protect it and other employees who may be exposed to the negative effects of such behaviour. On the other hand, it should be noted that employers have a duty to protect the life and health of their employees by ensuring safe and hygienic working conditions, as set out in Article 207 §2 of the Labour Code[761].

In connection with this obligation, employers should have the legal means to take action against behaviours and events that would affect safe and hygienic working conditions, which in turn could negatively impact the life and health of employees. These means certainly include the right to test employees for sobriety using a breathalyser.

Similar critical voices, drawing attention primarily to the ineffectiveness of the previous regulation, had been heard for many years and contributed significantly to the change in the regulations.[762]

---

[759] Kuba, 2025, Art. 22(1c)) Przesłanki wprowadzenia i sposób przeprowadzenia kontroli trzeźwości pracowników.
[760] Urząd Ochrony Danych Osobowych, Opinia 138/1076.
[761] Art. 207 §2 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[762] Kuba, 2025, Art. 22(1c)) Przesłanki wprowadzenia i sposób przeprowadzenia kontroli trzeźwości pracowników.

On 21 February 2023, the Act of 1 December 2022 amending the Labour Code and certain other acts[763], including the Act on Upbringing in Sobriety and Counteracting Alcoholism, came into force. This amendment changed the model of employee sobriety testing by introducing Articles 22^{1c} – 22^{1h} to the Labour Code and rephrasing Article 17 of the Act on Upbringing in Sobriety and Counteracting Alcoholism to apply to sobriety testing and other substances with effects similar to alcohol at companies that are not employers[764].

In the context of this thesis, Article 22^{1c} is of the greatest analytical significance. Unlike the previous legal status, it clearly grants the employer the right to introduce sobriety tests on employees if this is necessary to ensure the protection of the life and health of employees or other persons or the protection of property.[765] Each of the mentioned premises may, either individually or collectively, constitute ground for testing.[766]

A characteristic and commendable element of the new regulation is that it also covers the protection of persons other than employees, which does not apply, for example, in the case of video surveillance. This element becomes even more relevant when contrasted with Article 304 of the Polish Labour Code, which states that an employer is obliged to ensure the healthy and safe conditions of work not only for employees but also for individuals who perform work on other basis than employment relationship, at the employer’s establishment or at another location designated by the employer, as well as for self-employer persons who conduct economic activity on their own account at the employer’s establishment or at another location designated by the employer.[767] Moreover, the employer should use measures to protect the life and health of persons who do not participate in the work process but have access to a location where work is performed.[768] The employer’s obligation is absolute and unconditional and must be fulfilled even in the event of an employee’s negligence of their duties.[769] When considering Article 22^{1c} of the Polish Labour Code, in the context of Article 304 of the Polish Labour Code, it should be noted that introducing the possibility for employers to conduct sobriety tests and extending such tests to non-employees is, to a certain extent, a realisation of Article 66 (1) of the Polish

---

[763] Act of 1 December 2022 on the amendment of the Labour Code and certain other acts, Dz.U.2023.240.
[764] Art. 17 of the Act on Upbringing in Sobriety and Counteracting Alcoholism of 26 October 1982, Dz.U.2023.2151.
[765] Art. 22^{1c} §1 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[766] In the official Polish version of the provision, the conjunction between the listed premises is “lub” (eng. or), which accoridng to Polish legal logic, establishes a joint (indivisible) alternative.
[767] Art. 304 §1 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[768] Prusinowski, 2025, Art. 304; Art. 304 §4 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[769] Jaskulska, 2023, p. 41; Judgment of the Court of Appeal in Lublin of 8 April 2020, III Apa 4/20, LEX nr 2978529 - Although the ruling concerns Article 207 of the Labour Code, given the nature of both provisions, it can certainly be extended to Article 304 of the Labour Code.

Constitution[770], which stipulates that everyone has the right to safe and hygienic working conditions.[771]

The sobriety tests should be conducted through methods that do not require laboratory testing using a device with a valid document confirming its calibration. In practice, it means that in order to conduct a sobriety test, the employer may only use a breathalyser to measure the alcohol content in exhaled air. By permitting only this form of sobriety testing by employers, the legislator was guided by the belief that this method would ensure the least possible interference with the personal rights of employees,[772] which is of particular importance as the regulation stipulates that sobriety checks must not violate the dignity or other personal rights of the employee.[773] Details on how to conduct such testing are regulated in the Regulation of the Minister of Health of 16 February 2023 on testing for the presence of alcohol or substances similar to alcohol in the organism of an employee.[774]

Specific issues related to sobriety monitoring, such as the group of employees covered by the monitoring, the manner in which it is carried out, the type of device used for monitoring, time and frequency of testing, should be specified in a collective labour agreement or work regulations, or in a notice if the employer is not covered by a collective labour agreement and is not required to establish work regulations (in a situation where the employer hires fewer than 50 employees[775]).[776] This solution has also been used in the case of technical monitoring forms regulated in the Labour Code, thus bringing all forms of monitoring closer to each other. Moreover, on the basis of this provision, Kuba draws attention to the controversial issue of the requirement to designate a group of employees who may be subject to sobriety checks. Such a designation may indeed raise doubts, particularly in view of the principle of equal treatment of employees expressed in Article 11^2 of the Labour Code[777]. However, it should be remembered that the principle of equal treatment does not mean that all employees working for a given employer should be treated equally, but rather that it should be considered in relation to specific

---

770 "Everyone has the right to safe and hygienic working conditions. The manner in which this right is exercised and the obligations of the employer are specified by law." – Art. 66 of the Constitution of the Republic of Poland of 2 April 1997, Dz.U.1997.78.483.

771 Wyka, T 2025, Art. 207, in: Baran, K. W. (ed.), *Kodeks pracy. Komentarz. Tom II. Art. 94–304(5)*, Warsaw. https://sip.lex.pl/#/commentary/587817102/803259/baran-krzysztof-w-red-kodeks-pracy-komentarz-tom-ii-art-94-304-5-wyd-vii?cm=URELATIONS (accessed 17 September 2025).

772 Justification for the government's draft act amending the Labour Code and certain other acts, print number 2335, p. 10.

773 Article 22^{1c} §2 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).

774 §3-§6 of the Regulation of the Minister of Health of 16 February 2023 on testing for the presence of alcohol or substances similar to alcohol in the organism of an employee, Dz.U.2023 poz.317.

775 Article 104 $§1^1$ of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).

776 Article 22^{1c} § 10 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).

777 Article 11^2 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).

groups of employees who have been assigned the same duties.[778] Therefore, it can be stated that given the differences between various professions and the specific nature of particular jobs, some variation in the level, method or frequency of sobriety checks is perfectly acceptable, as these differences usually translate into different levels of risk that may be generated during the performance of specific work tasks.[779] To illustrate this correlation, we can refer to two example groups of employees working for the same employer – miners and accountants in a mine. It is difficult to deny that the work of a miner involves much greater risks and can result in more serious accidents than the work of accountants working "above ground". It is the employer's responsibility to minimise such risks, and therefore, more frequent sobriety checks for miners than for accountants should be considered fully justified and even desirable.

When regulating the employer's obligation to provide information in the context of sobriety monitoring, Polish legislators did not limit itself to indicating that this issue should be covered by a collective labour agreement, work regulations or a notice, but also specified that employees should be informed about the introduction of such sobriety checks in a manner adopted by the employer no later than two weeks before the checks begin.[780] Furthermore, when hiring an employee belonging to a group affected by sobriety checks, the employer is obliged to inform him or her, in paper or electronic form, before allowing him or her to work, about the details of the checks specified in the collective labour agreement, work regulations or notice.[781]

The employer is entitled to process information related to sobriety checks, such as the date and time of the test and its result, solely for the purpose for which it was collected. The retention period for such data stored in the employee's personal files is one year,[782] unless the data constitutes or may constitute evidence in proceedings to which the employer is a party or the employer has become aware of the filing of a lawsuit or the initiation of proceedings, as in such cases, the data retention period is extended until the proceedings are legally concluded.[783] The retention period shall also be extended in the event of an employee receiving a warning, reprimand or fine. The data should be removed from the employee's file once the penalty has been deemed null and void.[784]

[778] Pisarczyk points out that the essence of the principle of equal treatment of employees is the uniform shaping of the reights of employees in the same (comparable) situation, and the relevnat criteria are the nautre of the duties and the manner in which they are performer - Pisarczyk, 2025, Art. 11(2).
[779] Kuba, 2025, Art. 22(1c)) Przesłanki wprowadzenia i sposób przeprowadzenia kontroli trzeźwości pracowników.
[780] Article 22^{1c} § 11 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[781] Article 22^{1c} § 12 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[782] Article 22^{1c} §6 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[783] Article 22^{1c} §8 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[784] Article 22^{1c} §7 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).

It should also be mentioned that in the case of testing employees for the presence of substances in their organisms that have a similar effect to alcohol, the regulations forming the above-discussed model should be applied accordingly.[785]

The amendment introduced to the Labour Code also defines the role of the authorised body appointed to protect public order, which was already mentioned in the previous wording of Article 17 of the Act on Upbringing in Sobriety and Counteracting Alcoholism, within the process of sobriety control. According to the current legal status, the authorised body, e.g. police, at the request of the employer or an employee who has not been allowed to work, shall carry out the employee's sobriety test. Such a test should be conducted through methods not requiring laboratory testing. In practice, the employer's breathalyser is most often used to perform such a test.[786] Nevertheless, in certain circumstances specified in §5 of Article 22^{1d} of the Labour Code, including when it is not possible to conduct a test using a method that does not require laboratory testing and when an employee who is not allowed to work refuses to undergo testing using this method, the authorised body should order a blood test. The blood test must be carried out by a person with the appropriate professional qualifications.[787] Specific indication of who has the right to perform blood tests is contained in the Act of 15 September 2022 on Laboratory Medicine.[788][789]

As a final remark on the Polish regulation on employee sobriety monitoring, it should be noted that it was also necessary from the perspective of the GDPR, as this control involves the processing of health data[790], which, according to Article 9 of the GDPR, falls within the category of special data subject to more stringent processing requirements. In the case of special category data, unlike ordinary employee data, the necessity to fulfil the legal obligations imposed on the employer is not a sufficient ground.[791] Special category data may be processed by the employer when it is necessary for the fulfilment of obligations and the exercise of specific rights, but only if it is permitted by EU or national law or by a collective agreement concluded under the law of a Member State providing for appropriate safeguards for the fundamental rights and interests of the data subject.[792] Under Polish labour law, Articles 22^{1c} –

---

[785] Article 22^{1e} §7 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[786] Jaskulska, 2023, p. 41.
[787] Article 22^{1d} §7 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[788] Act of 15 September 2022 on Laboratory Medicine, Dz.U.2023.2125.
[789] Żołyński, 2023, Art. 22^{1d}.
[790] According to Article 4 (15) of the GDPR – "data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
[791] Article 6 (1)(c) of the GDPR.
[792] Article 9 (2)(b) of the GDPR.

22[1h] of the Labour Code have become the national regulations required by the GDPR, allowing employers to process data related to employee sobriety testing, i.e. employee health data. Kuba rightly points out that until 21 February 2023, such norms were lacking.[793]

3.1.2. Sobriety Monitoring Under the Czech Workplace Monitoring Model

When discussing the Czech model of employee sobriety monitoring, it should be noted that it is less detailed than the Polish one. Section 106 (4) of the Czech Labour Code established a general obligation of the employee to "take all possible care of his own safety and health, and also of the safety and health of other persons on whom his or her conduct or negligence at work might have an immediate effect".[794] The specification of this obligation can be found further in the provision. According to Section 106 (4) (e) of CLC, the employee should not consume alcohol and other addictive substances at the workplace and outside it during working hours. Entering the workplace under the influence also constitutes a breach of work discipline.

An employee is obliged to undergo a test to check for the presence of specific intoxicating substances in their body if instructed to do so by their superior. The role of a superior should be assigned by the employer in writing and prior to issuing testing instructions.[795] A common method of conducting tests directly in the workplace is the breathalyser. It provides quick information about the employee's sobriety, but the results from such a device are not admissible as evidence in court.[796] Therefore, it may be necessary to send the employee to an appropriate medical facility to perform a blood or other sufficient biological material test. Furthermore, the Act 65/2017 on the Protection of Health from the Harmful Effects of Addictive Substances explicitly states that an employee who is reasonably suspected of having consumed alcohol or other substances and who, as a result of his or her actions or behaviour, may cause harm to him or herself, another person, or someone's property, is required to undergo a preliminary examination and a specialist medical examination.[797] In a situation where an employee refuses

---

793 Kuba, 2025, Art. 22(1c)) Przesłanki wprowadzenia i sposób przeprowadzenia kontroli trzeźwości pracowników.

794 Section 106 (4) of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".

795 Štěpánková, 2025, p. 331; Section 106(4)(i) of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".

796 Štefko, 2023, p. 148.

797 Section 20(1)(a)(b)(c) of Zákon č. 65/2017 Sb. - Zákon o ochraně zdraví před škodlivými účinky návykových látek.

to undergo a professional medical examination, the regulation provides for a legal presumption that such an employee is under the influence of alcohol or another substance.[798]

Štefko indicates that a failure to comply with regulations prohibiting the consumption of alcohol and other substances in the workplace certainly constitutes a serious breach of work discipline and may lead to disciplinary dismissal.[799] This statement reflects a position that could be described as "zero tolerance for alcohol in the workplace." Nevertheless, this position is not confirmed by the case law of the Czech Supreme Court, which, in its judgment, ref. no. 21 Cdo 4733/2015 expressed a much more balanced opinion on the recognition of alcohol consumption by an employee as a serious breach of his duties and grounds for immediate dismissal. In this case, a breathalyser test before the start of the shift showed that the employee had 0.32 per mille of alcohol in his breath. A subsequent test, which took place half an hour later, showed 0.23 per mille, and a third test conducted shortly afterwards showed 0.11 per mille of alcohol. On this basis, the employee was dismissed from work on disciplinary grounds. After a detailed analysis of the facts and the rulings of the courts of previous instances, the Supreme Court indicated that the assessment of whether the employee's behaviour constitutes a serious breach of duties cannot be made on the basis of a single factor. The criteria to be taken into account in such an assessment are as follows: the position held by the employee; their attitude to the performance of their duties to date; the time and circumstances in which the violation of the law occurred; the degree of the employee's fault; the manner and intensity of the violation of the employee's specific duties; the consequences of the violation of the law for the employer; whether the employee's actions caused damage to the employer, etc. Therefore, the Court ruled that the mere fact that an employee consumed alcohol cannot automatically constitute a breach of the employee's duties to such an extent that the employment relationship could be terminated immediately.[800]

Remaining on the subject of an employee's breach of duty in connection with alcohol consumption at work, it should be noted that the Czech doctrine also indicates that the refusal to undergo sobriety tests constitutes a breach of professional duties, which is certainly to be agreed with, especially when considered from the perspective of the interests of the employer and other colleagues.[801] However, it should be remembered that an employee may refuse to

[798] Section 20 (2) of Zákon č. 65/2017 Sb. - Zákon o ochraně zdraví před škodlivými účinky návykových látek.
[799] Štefko, 2023, p. 148.
[800] Judgment of the Czech Supreme Court of 19 December 2016, 21 Cdo 4733/2015; Balousová, 2017.
[801] Štěpánková, 2025, p. 331; Pichrt and Stádník 2019, pp. 590 – 599.

take the test for a justified reason (e.g. health reasons confirmed by a medical certificate). In such a situation, no breach of the employee's duties can be considered.

The prohibition of alcohol consumption at work and during working hours does not apply to all employees. Employees working in unfavourable microclimatic conditions should be allowed to consume beer with a reduced alcohol content.[802] In this case, reference can be made to employees performing traditional heavy industry work, such as mining or metallurgy.[803] Also, employees whose work is usually associated with or involves consumption of alcohol (e.g. wine tasters, bartenders, brewers, production controllers, etc.) are exempt from the prohibition in question.[804] In the context of this regulation, the above-mentioned ruling of the Czech Supreme Court, ref. no. 21 Cdo 4733/2015, gains significance.

3.1.3. Sobriety Monitoring Under the Slovak Workplace Monitoring Model

As regards sobriety checks under the Slovak model, all regulations have been moved from the Labour Code to the Act on Occupational Health and Safety.[805] Section 9 of the OHS Act establishes the employer's obligation to carry out regular inspections and to require compliance with all regulations and rules governing health and safety in the workplace. In particular, the employer should check whether the employees are under the influence of alcohol, narcotics or psychotropic substances during their working hours and whether they adhere to the issued prohibition to smoke on the employer’s premises.[806] If an employer discovers any irregularities during an inspection, he or she is obliged to rectify them.[807]

The details of how such a sobriety check should be carried out have been developed primarily by doctrine. As in Poland and the Czech Republic, it is indicated that the first step is to check for the presence of alcohol in the employee's breath using a breathalyser. Such checks are usually carried out at the employer's premises and may be performed by the employer himself or an authorised manager.[808]

In accordance with Section 12 (2) (l) of the OHS Act, the employee is obliged to undergo such a sobriety examination organised by the employer or by the competent state authority in

[802] Section 106 (4) (e) of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended “Zákoník práce“.
[803] Štěpánková, K 2024, p. 331; Pichrt and Stádník 2019, pp. 590 – 599.
[804] Section 106 (4) (e) of the Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended “Zákoník práce“.
[805] Act of 2 February 2006 on Occupational Health and Safety, 124/2006 Z. z. (hereinafter: OHS Act).
[806] Section 9 (1) (b) of the OHS Act.
[807] Section 9 (2) of the OHS Act.
[808] Greguš, 2017, p. 244.

order to assess whether he or she is under the influence of alcohol, drugs or psychotropics. Similar to Article 22[1c] (10) of the Polish Labour Code, under the Slovak model of sobriety checks, the employer in the work regulations or other internal regulations shall specify the group of employees and other persons who are authorised to instruct and an employee to undergo an examination.[809] An employee is exempt from undergoing an examination only if they have a relevant medical certificate stating that testing with a breathalyser could harm them, e.g. due to severe asthma.[810]

It is recommended that at least one independent witness be present during the examination. Such a witness may be a representative of employees responsible for occupational health and safety. The check should be concluded with a report or an after-check protocol. This is extremely important, as such a document is often the only evidence in court.[811]

In practice, in order to ensure legal certainty, the breathalyser test is repeated at ten-minute intervals and can be performed up to three times. If an employee disagrees with the result of the breathalyser test, they should voluntarily go to a medical facility, where a biological sample will be taken to test for the presence of alcohol in their body.[812]

Furthermore, the Slovak regulation on employee sobriety testing has one more feature that is also characteristic of the Czech model. Namely, the OHS Act states that the prohibition to consume alcoholic beverages at and outside the employer's workplaces and on their premises during working hours shall not apply to those employees for whom the exceptional consumption of alcoholic beverages is a part of their work tasks or is usually connected to the performance of such tasks.[813]

3.1.4. Sobriety Monitoring Under the Hungarian Workplace Monitoring Model

Under the Hungarian workplace monitoring model, as in Slovakia, regulations concerning the testing of employees for sobriety are included in the Occupational Safety Act. An important role in establishing the framework for sobriety monitoring is also played by the non-compulsory resolution of the Hungarian Supreme Court No. 122.[814]

---

[809] Section 12 (2) (l) of the OHS Act.
[810] Greguš, 2017, p. 244.
[811] Greguš, 2017, p. 245.
[812] Greguš, J. 2017, p. 245.
[813] Section 12 (3) of the OHS Act.
[814] The Hungarian Supreme Court resolution, MK no. 122.

Firstly, it should be noted that the Hungarian Labour Code, like other labour codes of the Visegrad Group countries, imposes an obligation on the employer to ensure safety and non-hazardous working conditions.[815] Detailed rules concerning this obligation are set out in the Act XCIII on Occupational Safety.[816] It is important to point out that, as stipulated in Polish regulations (Article 22^{1c} (1) of the Polish Labour Code), in accordance with Act XCIII, this obligation applies not only to employees, but also to other persons present at the workplace and using services.[817] In order to ensure occupational safety and health protection, the employer is obliged, among other things, to provide the employee with the necessary instructions and information before starting work; regularly check whether the working conditions comply with the requirements and whether employees are familiar with and adhere to the regulations that apply to them; and conduct training to enable employees to acquire theoretical and practical knowledge about safety at work and to familiarise themselves with the necessary rules, instructions and information.[818]

The employer's obligation to create appropriate working conditions is matched by corresponding entitlements related to the proper organisation of work, management, instruction, issuing orders to employees, disciplining employees and monitoring.[819] These entitlements also include the possibility of checking the employee’s sobriety.[820]

The possibility of employers conducting sobriety checks was also confirmed by the Supreme Court in its resolution No. 122. Furthermore, the court indicated that an employee is obliged to cooperate with the employer and undergo the check.[821] The employee's obligation to cooperate also stems from Section 6(2) of the Labour Code, according to which “when exercising rights and fulfilling obligations, the parties to an employment relationship should act in accordance with the principle of good faith and honesty, cooperate with each other and refrain from behaviour that infringes the rights and legitimate interests of the other party. The requirement of good faith and honesty is also violated by a person whose exercise of rights is contrary to their previous behaviour, which gave the other party grounds for reliance.”[822] However, there may be situations where an employee is exempt from the obligation to cooperate with the employer and undergo testing. Such a situation arises when the employer

[815] Section 51 (4) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[816] 1993. évi XCIII. törvény a munkavédelemről (Act XCIII on Occupational Safety).
[817] Section 4 of Act XCIII on Occupational Safety.
[818] Section 54 (7) (a)-(b) and Section 55 (1) of Act XCIII on Occupational Safety.
[819] Gyulavári, 2019, *Munkajog*, pp. 241-242.
[820] Lukács, 2023, p. 2093; Dobosi, 2025.
[821] The Hungarian Supreme Court resolution, MK no. 122, 3.
[822] Section 6 (2) of Act I of 2012 on the Labor Code (Hungarian Labour Code).

abuses his or her control powers.[823] Such abuse occurs when the purpose of the test is inconsistent with the intent of the law, i.e. when the test is not only used to check the employee's sobriety for health and safety reasons, but is the result of personal revenge, is carried out several times a day without justification, etc.[824]

Moving on to the method of conducting sobriety checks on employees, it should be noted that this form of monitoring falls under Section 11/A (1) of the Labour Code and therefore must comply with the guarantees set out in this provision, primarily the obligation to inform employees in writing in advance.[825] Moreover, the work regulations should specify the procedure for conducting sobriety checks, and above all, when, how often and under what circumstances they may be carried out. Unannounced, ad hoc, and unjustified checks may violate the personal rights of employees.[826]

According to Supreme Court Resolution No. 122, if one of the parties questions the results of a breathalyser test, it is possible to request a doctor to perform a blood test for alcohol. In addition, the Supreme Court also defines the principle of so-called free evaluation of evidence, applied in court proceedings, which allows the state of intoxication to be determined by means other than a breathalyser test, by comparing the evidence gathered.[827] After the check, a report should be drawn up for evidentiary purposes.[828]

The employer should also determine who is authorised to conduct sobriety checks in the workplace. It should be remembered that, in accordance with the aforementioned position of the Hungarian DPA, no. 2017/439/H, in the context of personal inspections, security personnel hired by the employer cannot carry out such checks, as they are not related to the protection of property.[829] The person authorised to carry out the checks should be in an employment relationship with the employer.[830]

Gyulavári claims that the above procedure will also apply to drug testing.[831] Nevertheless, it should be noted that alcohol and drugs are substances with different characteristics, which means that they cannot be equated with each other. Just as a breathalyser test can determine

---

[823] According to Section 7 (1) of Act I of 2012 on the Labor Code, abuse of the right is prohibited. For the purpose of the Hungarian Labour Code "abuse of the right" means any action that is aimed at or results in the infringement of the legitimate interests of others, the restriction of their opportunities to assert their interests, their harassment, or the suppression of their freedom of expression.
[824] The Hungarian Supreme Court resolution, MK no. 122, 3.
[825] Lukács, 2023, p. 2096.
[826] Tatár, 2021, p. 76.
[827] The Hungarian Supreme Court resolution, MK no. 122, 4.
[828] Lukács, 2023, p. 2097; Tatár, 2021, p. 77.
[829] A Nemzeti Adatvédelmi és Információszabadság Hatóság, Decision NAIH/2017/439/H, p. 11.
[830] Lukács, 2023, p. 2096.
[831] Gyulavári, 2023, pp. 295.

whether an employee is under the influence of alcohol at a given moment, drug tests provide information about the fact that a particular drug has been taken, but do not necessarily mean that the employee is currently under its influence, which results in their inability to work. Therefore, Lukács points out that the widespread use of drug testing in the workplace is not in line with the protection of employee rights.[832] Although this position may be justified by the lack of regulation of drug testing under the Hungarian monitoring model and by the nature of drug testing, it cannot be accepted in its entirety. According to the above considerations, it is the employer's obligation to ensure safe working conditions for employees and other persons present at the workplace, which is to be achieved through the employer's control powers. Therefore, it must be recognised that an employee may be subjected to drug testing if the employer has reasonable suspicion (based on the employee's behaviour) that he or she is under the influence of narcotic substances and his or her condition prevents him or her from performing work. Given that this issue is of great importance, as it has a significant impact on workplace safety, it is necessary to advocate for the development of a legal framework for drug testing of employees within the Hungarian model of workplace monitoring.

[832] Lukács, 2023, p. 2098.

Chapter III. Surveillance and the Right to Privacy

1. Introductory Remarks

The right of employees to privacy is a concept closely linked to the institution of employee monitoring. Over the years, the importance of this right has grown and undergone constant transformation under the influence of changing socio-economic factors. In recent years, the debate on the concept of employee privacy and its protection has gained new momentum. This is primarily due to the development of new technologies and forms of work, one of the key elements of which is detailed monitoring of employees.

Deleuze, in his essay "Postscript on the Societies of Control,"[833] describes a situation in which the traditional workplace - the factory, which can be compared to the "body" - created unity among the individuals functioning within it, which brought certain benefits to both sides of the employment relationship. Employers could oversee every element of the "mass," while trade unions could mobilise the "mass" to resist. The situation is different in a modern corporation, which is not a "body" but rather symbolises a "soul" that permeates each employee, under the pretext of healthy competition and necessary rivalry, leading to increased work efficiency. The French philosopher compares the position of a person in a corporation to that of an animal in a reserve – electronic surveillance allows the location of both to be determined in an open environment. In a control society, privacy is under constant pressure, as personal data is the most valuable commodity, and all surveillance and control mechanisms are geared towards obtaining it.

Certainly, Deleuze's position may be considered harsh, and by some even caricatural, but given the development of employee monitoring forms covering increasingly larger areas of privacy, as described in detail in the first chapter of this thesis, it is difficult not to consider it as justified.

The current state of workplace monitoring and constant interference in employees' private lives is compared by some authors to a return to quasi-feudal relations between employees and employers.[834] In today's world of work, the boundaries between working time and private time are becoming increasingly blurred.[835] The ability to connect to the internet via computers and mobile devices makes it possible to work virtually anytime, anywhere in the world. At first

[833] Deleuze, 1992, pp. 3 – 7.
[834] Collins, 2025, p. 469.
[835] Genin, 2016, pp. 280-281.

glance, this seems like a positive development, guaranteeing employees more flexibility, but in reality, it significantly reduces our time 'outside the workplace,' which has a direct impact on our privacy.[836] If we can work anywhere and at any time, we can also be monitored anywhere and at any time.

Taking the above into account, in order to establish a framework for employees' privacy that should not be violated by monitoring in the workplace, it is first necessary to consider exactly what this notion of privacy encompasses. When analysing the doctrine, it is possible to distinguish many concepts of privacy that cover or directly relate to employees' right to privacy. Among these concepts, two theories certainly deserve to be highlighted, as they have left a significant mark and continue to influence the discourse on employees' right to privacy.

The first theory derives from the Anglo-Saxon legal culture and is the concept developed by Samuel Warren and Louis Brandeis in their classic article 'The Right to Privacy' from 1890.[837] In this article, the authors draw attention to the threat posed by technological progress, which enables the collection, processing and transmission of increasingly detailed information from every area of an individual's life.[838] The prime example of this phenomenon cited in the article was the activity of the tabloid press. According to Warren and Brandeis, the right to privacy can be translated as "the right to be left alone." The right to be left alone states a negative freedom – freedom from unwanted intrusion and surveillance, and it also seeks to create clear boundaries between private and public spheres.[839] A related theory that develops the "right to be left alone" is Alan Westin's concept of "privacy as control,"[840] which means that every individual is entitled to control information about themselves, and such information may not be disclosed against their will.[841]

The second theory that has dominated the European continent is the concept that the right to privacy is a positive freedom and serves primarily to protect the autonomy of the individual. According to this theory, individuals have the right to organise their lives according to their

[836] Accoridng to Eurofund data from 2021, 16 percentage points more employees working from home worked long hours (41 to 60 hours) – 35%, than employees working only at their employer's premises – 19%. See: Predotova and Llave, 2021.
[837] Warren and Brandeis, 1890, pp. 193-220.
[838] Czubik, 2013, pp. 67-68.
[839] Collins, 2025, p. 479; Albin, 2025, p. 533.
[840] Westin, 1967(2018).
[841] Albin, 2025, p. 534.

own will, as long as this does not infringe on the privacy and freedom of others.[842] This understanding of the right to privacy stems from Article 8 of the ECHR.[843]

In addition to the two privacy concepts mentioned above, there are also privacy concepts that strictly relate to employee privacy. These include ensuring the protection of employees' personal data through collective action and privacy perceived as professional identity, and should rather be seen as a kind of complement to the two main concepts.[844]

Based on the first concept, the main guarantor of privacy in the workplace is strong unionisation and collective action. This approach seems to have been taken into account by the European legislator in Article 88 of the GDPR, which recognises the role of collective agreements in regulating the processing of personal data in the context of employment.[845] Although this concept is commendable, as it promotes the direct influence of employees on the respect for their privacy in the workplace, in practice, it does not play a significant role in the Visegrad Group countries, mainly due to low unionisation and collective bargaining coverage (against this background, only the Czech Republic stands out).[846]

The second concept is based on professional identity, which results from participation in a specific professional group. Within this theory, great importance is attached to the existence of codes of ethical conduct developed by various professional groups, which refer to principles related to privacy (however, codes are not a prerequisite). This approach is not based on legal provisions and rights, but rather leads to a discourse encompassing specific values, ethics and the morality that permeates a particular profession.[847]

Focusing on the two main approaches to privacy mentioned above and applying them to the sphere of employment, it may seem that they differ to such an extent that they are mutually exclusive. However, this is a superficial view, because in reality, both approaches are reflected in national workplace monitoring models[848] and in the practice of national and international

---

842 Collins, 2025, p. 479.

843 As Otto points out, for over two decades, the central axis of privacy protection in employment on the old continent appears to be the international dimension based on the ECHR and the case law of the ECtHR - See: Otto, 2019, p. 50.

844 Albin, 2025, p. 542.

845 Abraha, 2022, p. 286.

846 Trade union denisty: Poland – 9.4% (2022), Czech Republic – 9.4% (2023), Slovakia – 11.8% (2022), Hungary – 7.4% (2020); Collective barganing coverage: Poland – 11.6% (2023), Czech Republic – 43.2% (2024), Slovakia – 27.6% (2024), Hungary – 20.4% (2022). Based on OECD data indicated in the reports on main indicators and characteristics of collective barganing in Poland, Czech Republic, Slovakia and Hungary of 1 October 2025 – See: OECD/AIAS ICTWSS Database, Trade Union Denisty Data [Online].

847 On this approach, see more in: Albin, 2025, pp. 521-551.

848 In the context of workplace monitoring, an analogy to the private sphere of an individual, distinguished within the concept of "privacy as the right to be left alone," are premises within workplace exempted by specific regulations from the possibility of monitoring, so as to ensure the highest possible degree of privacy for employees therein. This concept also takes on practical significance in situations where the boundaries between work and

adjudicative bodies, which is most clearly visible in the judgments of the constitutional courts and tribunals of the Visegrad Group countries and in the case law of the European Court of Human Rights[849]. In view of the above, the following part of this chapter will be devoted to constitutional and human rights aspects of employees' right to privacy in the context of workplace monitoring. It will also analyse employees' right to privacy as a personal right within the legal systems of the Visegrad Group countries. Given the fact that the concept of privacy within the European system of human rights protection is widely reflected in national systems, failure to discuss the notion of employees' right to privacy from these perspectives would result in an incomplete analysis of national models of workplace monitoring. Ultimately, it is the specific interpretation of employees' right to privacy that indirectly determines the framework of admissibility and proportionality of specific forms of monitoring at the workplace.

2. Constitutional Perspective

2.1. Characteristics of Constitutional Provisions Establishing the Right to Privacy in the Visegrad Group Countries

When analysing individual provisions relating to privacy contained in the constitutions and fundamental laws of the Visegrad Group countries, the first conclusion that arises is that the understanding and approach to privacy in these countries is remarkably similar. Firstly, in each of these countries, the right to privacy is guaranteed at the constitutional level. Secondly, the provisions regulating this right and its various aspects are found in sections devoted to personal freedoms and rights.[850] Thirdly, each of the basic laws has retained a similar structure of regulations, within which the following can be distinguished: the right to privacy *per se* (a general provision establishing the protection of private and family life, as well as, among other things, good name, honour, dignity, etc.), the protection of the secrecy of communication, the inviolability of the home and the protection of personal data.

---

private life become significantly blurred, such as in the case of continuous monitoring of an employee's activity on a computer that is used for both work and private purposes - see: Collins, 2025, p. 481.

[849] The second approach, rooted in the European human rights system, stems from the wording of Article 8 of the ECHR and is subject to continuous development by the ECtHR in accordance with the doctrine of treating the convention as a living instrument. This approach permeates primarily the case law of the Visegrad Group countries, where the jurisprudence of the ECtHR is treated as a kind of benchmark for European standards of respect for human rights.

[850] In Poland, exact title of that section is “Personal freedoms and rights”, in Slovakia and the Czech Republic “Fundamental Human Rights and Freedoms” and in Hungary “Freedom and responsibility”.

The constitutional aspect plays a significant role in the Polish model of workplace monitoring. This is primarily due to the fact that when creating this model, the legislator did not establish in the Labour Code an obligation for employers to respect employee privacy, and therefore, such an obligation must be derived from constitutional regulations, namely from Article 47 of the Polish Constitution.[851]

This article states that everyone shall have the right to legal protection of his/her private and family life, of his/her honour and good reputation, and to make decisions about his/her personal life.[852] This provision constitutes a general source for other constitutional provisions relating to other, more specific aspects of privacy – Articles 48–51 of the Polish Constitution – among which, with regard to employment, and in particular monitoring, the following provisions are of particular importance: Articles 49, Article 50 and Article 51, which regulate, respectively, the secrecy of communication,[853] the inviolability of the home (the so-called domestic mir)[854] and the right to personal data protection.

As Oręziak points out, Article 47 of the Polish Constitution serves as a positivistic legal exemplification of the concept of the right to privacy derived from natural law. Therefore, it should be recognised that every human being has the right to privacy by virtue of the very fact that he/she is a human, regardless of whether or not there is a provision guaranteeing this right.[855] This position might be further confirmed by the fact that the wording of this provision, taking also into account Article 31 (3) of the Polish Constitution relating to the possibility of restricting constitutional freedoms and rights, is largely consistent with the wording of Article 8 of the ECHR. Furthermore, the rights referred to in Article 47 of the Polish Constitution are

[851] Otto, 2023, p. 394.
[852] Article 47 of Constitution of the Republic of Poland of 2nd April 1997 no. 78 item 483.
[853] Article 49 of Constitution of the Republic of Poland of 2nd April 1997 no. 78 item 483, states that "the freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute."
[854] Article 50 of Constitution of the Republic of Poland of 2nd April 1997 no. 78 item 483, states that "the inviolability of the home shall be ensured. Any search of a home, premises or vehicles may be made only in cases and in a manner specified by statute."
Article 51 of Constitution of the Republic of Poland of 2nd April 1997 no. 78 item 483, states that: "1. No one may be obliged, except on the basis of statute, to disclose information concerning his person. 2. Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law. 3. Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute. 4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute. 5. Principles and procedures for collection of and access to information shall be specified by statute."
[855] Oręziak, 2023, p. 322, 324.

protected by so-called non-derogable rights, i.e. rights that cannot be restricted even during martial law or a state of emergency (Article 233 (1) of the Constitution)[856].[857]

With regard to the right to privacy regulated in the Polish Constitution (although these considerations may also apply to other countries of the Visegrad Group), it should also be noted that it has a horizontal and vertical dimension. The horizontal application of this right means that it is intended to protect against unjustified interference in a person's private life by another private entity. The vertical dimension, on the other hand, applies to relations between individuals and public authorities and is intended to protect against violations of privacy by those authorities.[858] At first glance, the right to privacy will apply horizontally in the sphere of employment. However, given the hierarchical nature of the relationship between the parties to an employment relationship, it should be noted that certain elements of the right to privacy in the vertical sense will also be evident here. In addition to its negative element, mentioned earlier, the vertical right to privacy also establishes a positive obligation for state authorities to create appropriate legal regulations that guarantee respect for the individual's right to privacy. In the context of workplace monitoring, it can be pointed out that the practice of its use is largely dependent on the employer, who is the stronger party in the employment relationship and, therefore, the employer, is responsible for ensuring that monitoring is used in a manner that respects the dignity of employees, their privacy and the standards set by law, what is to certain extent similar to the obligation incumbent on state authorities.[859]

Moving on to the Slovak and Czech constitutional models of privacy protection, it should be noted that they are virtually identical, with the same structure of provisions and the same wording.

Both begin with a provision that grants respect for the privacy and integrity of all individuals. This right may only be restricted in particular situations specified by law.[860]

---

[856] Article 233 (1) of Constitution of the Republic of Poland of 2nd April 1997 no. 78 item 483 – "The statute specifying the scope of limitation of the freedoms and rights of persons and citizens in times of martial law and states of emergency shall not limit the freedoms and rights specified in Article 30 (the dignity of the person), Article 34 and Article 36 (citizenship), Article 38 (protection of life), Article 39, Article 40 and Article 41, para.4 (humane treatment), Article 42 (ascription of criminal responsibility), Article 45 (access to a court), Article 47 (personal rights), Article 53 (conscience and religion), Article 63 (petitions), as well as Article 48 and Article 72 (family and children)."

[857] Judgment of the Polish Constitutional Tribunal of 30 October 2006, File ref. P 10/06, 4.3.

[858] Oręziak, 2023, pp. 320-321.

[859] Polish labour law doctrine includes extensive concepts of equating a workplace with an administrative facility – See: Sobczyk, 2021.

[860] In the Slovak Constitution of 1 September 1992 (160/1992 Zb), this is Article 16 (1), while in the Czech Charter of Fundamental Rights and Freedoms of 16 December 1992 (Const. act No. 2/1993 Coll. as amended by constitutional act No. 162/1998 Coll.), which is part of the constitutional order, it is Article 7 (1). Both provisions have the same wording.

According to the position of the Slovak Constitutional Court, the protection of privacy under Article 16 (1) of the Slovak Constitution is related to physical integrity and material values of a private nature.[861] A similar position is expressed by the Czech doctrine, according to which Article 7 (1) of the Charter applies only to the physical and mental integrity of a person.[862] This approach stems from the case law of the Czech Constitutional Court and is the prevailing one.[863] In view of the above, it should be concluded that these provisions do not constitute a general clause regarding privacy protection, as their scope is specific and limited in terms of subject matter.[864] Nevertheless, they can play an important role in protecting employee privacy in connection with the upcoming trends related to the cyborgisation of employees' bodies[865] and the increasing use of pharmacological cognitive enhancement substances to improve work performance.[866]

The provisions relating primarily to privacy in the context of employment relations are considered to be Article 19 of the Slovak Constitution and Article 10 of the Czech Charter of Fundamental Rights and Freedoms.[867] The first paragraph of both regulations focuses on the protection of the dignity, honour, reputation and good name of individuals. The Slovak Constitutional Court points out that although these terms are often used interchangeably, they actually have different meanings. Dignity protects the very essence of individual humanity from humiliation, thus protecting humanity from being merely an object of power. Reputation and good name can be defined as a perception of a person in the community or broader in society, and are social components of the right to privacy. These concepts play an important role in the context of privacy in the workplace, as they open up this concept to the possibility of employees establishing social relationships within and outside the workplace. In turn, honour is an internal concept lying on the edge of personal and social spheres.[868]

Subsequently, the second paragraph of the provisions in question prohibits unjustified interference in the private and family life of individuals. The wording of these provisions refers to Article 8 of the ECHR and is largely similar to Article 47 of the Polish Constitution.

On the basis of Article 19 (3) of the Constitution of the Slovak Republic and Article 10 (3) of the Charter of Fundamental Rights and Freedoms, the protection of personal data has been

[861] Judgment of the Slovak Constitutional Court of 13 May 1997, II. ÚS 19/97.
[862] Sehnálek, 2023, pp. 237-238.
[863] Judgment of the Czech Constitutional Court of 27 February 2019, IV. ÚS 774/18.
[864] Sehnálek, 2023, p. 237.
[865] See more: Surdykowska, 2023, pp. 1-15.
[866] Surdykowska, 2025, pp. 303-325.
[867] Škvarková, 2017, p. 204; Sehnálek, 2023, p. 237.
[868] Decision of the Slovak Constitutional Court of 26 March 2015, II. ÚS 191/2015, 54.

included - everyone shall have the right to be protected against unjustified collection, disclosure and other misuses of personal data – which is particularly important in the context of workplace monitoring. Unlike in Poland, under the Slovak and Czech constitutional systems, personal data protection has been incorporated into the provision covering also other aspects of privacy. This approach may draw greater attention to the relationship between multiple aspects of individual privacy and may be more understandable to citizens and other persons residing in Slovakia and the Czech Republic, including employees.

The principle of personal data protection is also enshrined in Article 22 of the Slovak Constitution and Article 10 of the Charter. However, it should be noted that these provisions constitute *lex specialis* in relation to the provisions mentioned in the previous paragraph, as they primarily concern respect for the privacy of communications.[869] According to this regulation, the secrecy of letters, other communications and written messages delivered by post, as well as personal data, shall be guaranteed. The scope of protection also covers communication by telephone, telegraph, and other similar means.[870] It should therefore be noted that the concept of communication within the Slovak and Czech constitutional systems should be understood broadly as covering both traditional and modern forms of communication.

When referring to Articles 16 (1), 19 and 22 of the Constitution of the Republic of Slovakia, the Slovak legal doctrine states that these provisions form a constitutional privacy standard which is under the umbrella of the so-called eternity clause.[871] It means that neither the parliament nor the population deciding by referendum can abolish this standard.[872]

Considering the twin nature of the privacy standard established in the Czech Charter of Fundamental Rights and Freedoms, and the fact that in Article 1 of the Charter, the Czech legislator,[873] similarly to the Slovak legislator in Article 12 (1) of the Constitution,[874] grants the highest level of protection to fundamental rights and freedoms of all people, it should be concluded that the eternity clause will also apply to it.

---

[869] Šmigová, 2023, p. 182.

[870] Article 22 of Slovak Constitution of 1 September 1992 (160/1992 Zb); Article 13 of Czech Charter of Fundamental Rights and Freedoms of 16 December 1992 (Const. act No. 2/1993 Coll. as amended by constitutional act No. 162/1998 Coll.).

[871] Husovec, 2017, p. 181.

[872] Article 12 (1) of the Slovak Constitution of 1 September 1992 (160/1992 Zb); Decision of the Slovak Constitutional Court of 28 October 2014, PL. ÚS 24/2014, 37.

[873] Article 1 of the Czech Charter of Fundamental Rights and Freedoms of 16 December 1992 states that: “All people are free and equal in their dignity and rights. Their fundamental rights and freedoms are inherent, inalienable, non-prescriptible, and irrepealable.”

[874] Article 12 (1) of the Slovak Constitution of 1 September 1992 states that: “All human beings are free and equal in dignity and in rights. Their fundamental rights and freedoms are sanctioned, inalienable, imprescriptible and irreversible.”

The eternity clause can be compared to the "non-derogability" clause that exists within the Polish constitutional system. Although these clauses grant the right to privacy a special, supreme standard of protection, they do not mean that this right is absolute and cannot be restricted under certain conditions, as will be explained in more detail later in this chapter.

Under Slovak and Czech constitutional law, as in Poland, respect for the privacy of the dwelling is also enshrined, stating that the dwelling is inviolable and that entry is subject to the consent of the person living there.[875]

When the right to privacy under the Fundamental Law, the Hungarian legislator adopted a different methodological approach than the Polish, Slovak and Czech legislators. Instead of breaking down individual aspects of privacy, such as the general right to privacy, the protection of personal data, the privacy of communication, and the inviolability of the dwelling into separate provisions, it was regulated comprehensively in four paragraphs of Article VI of the Fundamental Law.[876] From the perspective of employee privacy and personal data protection in the workplace, paragraphs 1 and 3 of this article are considered to be the most important.[877]

The first paragraph of Article 6 of the Fundamental Law states that "everyone shall have the right to have his or her private and family life, home, communications and good reputation respected.[878] Exercising the right to freedom of expression and assembly shall not impair the private and family life and home of others.[879]" In turn, paragraph 3 of the article in question provides the protection of an individual's personal data and the right to access and disseminate data of public interest.

A characteristic feature of the Hungarian constitutional system of privacy protection is the obligation under paragraph 4 of Article 6 of the Fundamental Law to establish a special authority for personal data protection – the authority is the National Authority for Data Protection and Freedom of Information (*Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)*).

According to the decision of the Constitutional Court, the right to privacy under Hungarian constitutional law has its origins in another, even broader fundamental right, namely the right

[875] Article 21 (1) of the Slovak Constitution of 1 September 1992 (160/1992 Zb); Article 12 (1) of the Czech Charter of Fundamental Rights and Freedoms of 16 December 1992 (Const. act No. 2/1993 Coll. as amended by constitutional act No. 162/1998 Coll.).
[876] Article VI of the Fundamental Law of Hungary 25 April 2011.
[877] Gyulavári, 2023, p. 289.
[878] The wording of this provision is essentially identical to Article 7 of the Charter of Fundamental Rights of the European Union and to Article 8 of the European Charter of Human Rights.
[879] The second sentence of this provision was introduced by amendment no. 7 in 2018 and aims to prevent conflicts of constitutional fundamental rights that may arise in relation to the right to privacy.

to respect for human dignity.[880] A similar position regarding the constitutional right to privacy is also held by the rest of the Visegrad Group countries.

2.2. The Concept of the Right to Privacy in the Constitutional Systems of the Visegrad Group Countries

On 5 March 2013, the Polish Constitutional Tribunal issued a ruling in which it explicitly defined the notion of the right to privacy under the Polish constitution. The Tribunal stated that Article 47 of the Polish Constitution regulates two distinct situations. Firstly, pursuant to the provision in question, an individual is entitled to legal protection of the spheres of life indicated in the first part of the Article. i.e., private and family life, honour and good reputation, which in practice means that there must be statutory regulations enabling the protection of the specified spheres of an individual's life.[881] Secondly, every individual has the freedom to decide about his or her personal life, as indicated at the end of Article 47 of the Polish Constitution. In other words, it can be said that interference with an individual's freedom to shape his or her personal life is prohibited. Furthermore, the Tribunal pointed out that this freedom is an expression of the general freedom of the human being under Article 31(1) of the Constitution[882] and of personal freedom *sensu stricto*, under Article 41(1) of the Constitution[883].[884]

In view of the above, it is evident that the Polish Constitutional Tribunal recognises both the positive and negative aspects of the right to privacy.

Under the Polish constitutional law, particularly in matters relating to employment, privacy in the sense of negative freedom is of significant importance. As Otto points out, referring to the case law of the Constitutional Tribunal, the right to privacy boils down to "the right to be left alone."[885] This understanding of the right to privacy stems from its strong roots in the constitutional requirement to protect human dignity (Article 30 of the Polish Constitution)[886], as one of the elements constituting human dignity is respect for a person's private sphere, so

[880] Decision of Hungarian Constitutional, 1115/B/1995. AB.
[881] An example of this type of regulation are the provisions of the Polish Labour Code relating to the protection of employees' personal data and monitoring in the workplace - Articles 22^1 - 22^3.
[882] Article 31 (1) of the Polish Constitution states that: "Freedom of the person shall receive legal protection."
[883] Article 41 (1) of the Polish Constitution states that: "Personal inviolability and security shall be ensured to everyone. Any deprivation or limitation of liberty may be imposed only in accordance with principles and under procedures specified by statute."
[884] Judgment of the Polish Constitutional Tribunal of 5 March 2013, U 2/11, part III, 4.2.
[885] Otto, 2023, p. 395.
[886] Article 30 of the Polish Constitution states that: "The inherent and inalienable dignity of the person shall constitute a source of freedoms and rights of persons and citizens. It shall be inviolable. The respect and protection thereof shall be the obligation of public authorities."

that he or she is not burdened with the necessity of "being with others" or "sharing with others" his or her experiences and sensations of an intimate nature.[887]

When analysing the concept of privacy as expressed in the case law of the Polish Constitutional Tribunal, it is also necessary to consider one of the main aspects of privacy that is of key importance for employee privacy, namely the protection of personal data.

In its judgment of 24 June 1997, the Constitutional Tribunal pointed out that the constitutional right to privacy also includes the protection of personal data, as it can be understood as the right to keep information about one's private life confidential.[888] This position was approved and reiterated in subsequent judgments of the Constitutional Tribunal, in which the Tribunal indicated that there is a strong link between Article 47 of the Constitution, which expresses the general right to privacy, and Article 51 of the Constitution, which provides for the protection of personal data,[889] and that privacy can be understood as the protection of information concerning a given person and a guarantee of a certain degree of independence, within which a person can decide on the scope and extent of sharing and communicating information about their life to others.[890]

The Constitutional Tribunal expressed further considerations on the relationship between the right to privacy and personal data protection in the justification for its judgment of 12 November 2002, indicating that "the right to personal data protection undoubtedly constitutes a special instrument for protecting those interests of individuals that are related to the protection of private life. This right is therefore a specialised instrument of protecting the same values that are protected by Article 47 of the Constitution."[891] In light of the above, it should be stated that the right to data protection corresponds to the concept of so-called information autonomy.[892] Moreover, in the same judgment, the Tribunal ruled that the contemporary understanding of privacy in relation to personal data leads to the protection of all personal information regardless of its content, i.e. regardless of whether it is embarrassing or neutral in terms of morality or social norms. The subject of protection under the evolving concept of privacy is the ability to freely conduct one's affairs, make decisions about one's life and the types of personal relationships established with other people. This sphere of privacy constitutes the autonomous activity of the individual and should be subject to as little interference from the outside world

[887] Judgment of the Polish Constitutional Tribunal of 5 March 2013, U 2/11, part III, 4.4.
[888] Judgment of the Polish Constitutional Tribunal of 24 June 1997, K 21/96.
[889] Judgment of the Polish Constitutional Tribunal of 24 June 1998, U 4/97.
[890] Judgment of the Polish Constitutional Tribunal of 19 May 1998, U 5/97.
[891] Judgment of the Polish Constitutional Tribunal of 12 November 2002, SK 40/01.
[892] More on information autonomy in the context of employment relations in: Grzybowski, 2020, pp. 47 – 67.

as possible.[893] This position, which extends the concept of privacy to include the aspect of establishing relationships with other people, reflects the development of the concept of privacy and is highly relevant in the context of protecting employee privacy. It coincides with what the ECtHR expressed in its judgments, e.g. in the cases of Niemietz v. Germany[894] and Bărbulescu v. Romania,[895] indicating that the right to privacy of employees also includes the possibility of establishing and developing relationships with other people, also within the workplace.

The Polish Constitutional Tribunal has also made numerous direct references to the issue of employee data protection. As Barański points out, these rulings focus on two issues related to employee data protection, namely restrictions on information autonomy and employee consent to the processing of their personal data.[896] Most of these rulings are based on the concept of privacy already referred to, developed by earlier Constitutional Tribunal rulings, but from the point of view of workplace monitoring, two characteristic judgments should be mentioned.

Firstly, in its judgment of 19 June 2018, the Constitutional Tribunal pointed out that "the sphere of individual privacy, protected under Article 47 of the Constitution, also covers information about a person's health, because the protection of medical data is fundamental to an individual's ability to exercise their right to respect for private and family life." According to the Tribunal, health data is of a special nature, as it directly concerns areas of privacy or even intimacy of a natural person and is associated with a greater sense of threat in the event of its unjustified processing. Special categories of personal data should be subject to a higher standard of protection and may be processed for health purposes only where necessary to achieve those objectives for the benefit of individuals and society as a whole.[897] This judgment is particularly significant in the context of workplace monitoring forms, such as psychological tests that enable the monitoring of employees' psychological and emotional state.[898]

Secondly, in the judgment of 26 April 2018, the Tribunal addressed the issue of an employee's consent to disclose their personal data to another entity. In the justification of the judgment, the Constitutional Tribunal stated that an element of privacy protection is the informational autonomy of every individual, which means the ability to decide on the scope of access to data concerning them, and that the consent of the person concerned to disclose

[893] Judgment of the Polish Constitutional Tribunal of 12 November 2002, SK 40/01.
[894] ECtHR judgment in Niemietz v. Germany from 16 December 1992 (Application no. 13710/88), 29.
[895] ECtHR judgment in Bărbulescu v. Romania from 5 September 2017 (Application no. 61496/08), 70.
[896] Barański, 2022a, p. 51.
[897] Judgment of the Constitutional Tribunal of 18 June 2018, SK 19/17.
[898] Barański and Mirosławski, 2026, pp. 1-20.

information to another entity is of fundamental importance in this case.[899] Nevertheless, it should be noted that, as in the case of certain personal data, the employee's consent to its disclosure may play an important role; however, in the case of employee monitoring, it will be irrelevant, as has already been explained and justified multiple times in the previous chapter of this thesis. The reason why an employee's consent cannot be considered as a basis for the processing of personal data as a result of monitoring is the doubt as to whether an employee can give “free and uncoerced consent” during the duration of an employment relationship, which is characterised by an imbalance between the parties.

Moving on to the concept of privacy within the Slovak and Czech constitutional systems, it should be noted that they largely overlap. In both systems, the right to privacy is defined by the concept of individual informational autonomy, which brings these systems closer to the meaning of the right to privacy expressed by the Polish Constitutional Court. In one of its most commonly cited judgments regarding the understanding of privacy, the Slovak Supreme Court stated that the right to privacy entails the right of a natural person to decide independently, at his or her own discretion, whether and to what extent facts about his or her private life should be disclosed to other persons or made public. A violation of this right will occur not only in the case of unauthorised acquisition of knowledge and information about the privacy of a natural person, but also in the case of unauthorised dissemination of such knowledge and information.[900] A similar, albeit more elaborate, position was expressed by the Slovak Constitutional Court in its judgment of 4 December 2007, stating that: “the general constitutional principle of freedom (Article 2(3) of the Slovak Constitution), which is one of the core values of a democratic state governed by the rule of law and which consists in the state's obligation to respect and protect the sphere of personal autonomy of the individual, is directly related to the rights defined in this way. In their interconnection, these rights and principles guarantee a certain "inner sphere" in which individuals can live according to their own ideas and exclude the "outside world," and a sphere in which individuals can freely develop, express their personality, and enter into and develop relationships with other people. The right to privacy and the protection of private life, in conjunction with the principle of freedom, thus guarantee the individual the possibility of autonomous self-determination in its most basic definition, based on the right to human dignity.”[901] The Czech Constitutional Court also draws attention to the possibility of autonomous self-determination of the individual. In its

[899] Judgment of the Polish Constitutional Tribunal of 26 April 2018, K 6/15.
[900] Judgment of the Slovak Supreme Court of 18 February 2010, 3 Cdo 137/2008.
[901] Judgment of the Slovak Constitutional Court of 4 December 2007, PL. ÚS. 12/01.

judgment of March 22, 2011, it indicates that ensuring space for such a possibility and self-realisation of the individual's personality is one of the fundamental functions of the right to respect for private life. It can therefore be said that the Czech Constitutional Court views the right to privacy as a right guaranteeing the individual's right to decide independently whether, to what extent, how, and under what circumstances facts and information relating to their privacy should be disclosed to other entities. In this judgment, the Constitutional Court also draws attention to an interesting issue from the point of view of current changes taking place in workplaces. It points out that the requirements for respect for privacy and its protection are closely linked to the development of technical and technological capabilities, which clearly increase the state's potential to infringe upon freedom.[902] Exactly the same conclusion can be drawn with regard to employee privacy, as technological development largely affects it, among other things, through the development of new forms of surveillance.

A characteristic feature, visible primarily in the case law of the Slovak Constitutional Court, but also appearing in the Czech constitutional system, is the significant influence of the ECtHR's jurisprudence on national concepts of privacy. In its judgment of November 6, 2014, the Slovak Constitutional Court, referring to the case law of the ECtHR, ruled that the right to privacy extends beyond protection from publicity and also includes, *inter alia*, aspects of an individual’s physical and social identity, including the right to personal autonomy, personal development and to establish and develop relationships with other human beings and the outside world[903].[904] The reason for the Slovak Constitutional Court's rigid adherence to the case law on the right to privacy developed by the ECtHR is not the court's own will or fear of violating international standards. As Šmigová points out, firstly, the European Convention on Human Rights, like the Slovak Constitution, guarantees the protection of the right to privacy, which already indicates a certain obligation to take Article 8 of the Convention into account in the judgments of the Constitutional Court. Secondly, there is an even more important formal reason. The European Convention on Human Rights, as an international treaty on human rights and fundamental freedoms, which has been ratified and promulgated in the manner laid down by a Slovak law, according to Article 154c of the Slovak Constitution,[905] shall be a part of Slovakia’s

---

[902] Judgment of the Czech Constitutional Court of 22 March 2011, Pl. ÚS 24/10.
[903] ECtHR judgment in Evans v. the United Kingdom from 10 April 2007 (Application no. 6339/05), 71.
[904] Judgment of Slovak Constitutional Court of 6 November 2014, II. ÚS 424/2012.
[905] Article 154c of the Slovak Constitution of 1 September 1992 states that: “International treaties on human rights and fundamental freedoms which the Slovak Republic has ratified and were promulgated in the manner laid down by a law before taking effect of this constitutional act, shall be a part of its legal order and shall have precedence over laws if they provide a greater scope of constitutional rights and freedoms.”

legal order and shall have precedence over laws, as it provides a greater scope of constitutional rights and freedoms.[906]

Following the case law of the ECtHR concerning Article 8 of the Convention, the Czech Constitutional Court reached a similar conclusion to that of the Slovak Constitutional Court. In its judgment of 20 May 2002, it stated that the right to privacy is not limited solely to the freedom of an individual to decide whether to disclose facts concerning his or her private life to others and to protection against unauthorised interference with that right, but also includes the protection of fundamental social relationships.[907] We can therefore see that the Constitutional Court recognised that the ability to maintain and establish social ties is an inherent element of privacy.[908] A similar position was also expressed by the Czech Constitutional Court in its judgment of 1 March 2000, in which the Court criticised the narrow understanding of privacy. It pointed out that: "the right to privacy can be defined as the right of a natural person to decide at their own discretion whether, and to what extent and in what manner, facts relating to their personal privacy should be made available to others (positive component of the right) and at the same time to defend (resist) against unauthorized interference in this sphere by other persons with equal legal status (negative component of the right). Excessive emphasis on the positive component of the right to privacy leads to an inadequate narrowing of protection to ensure that facts about a natural person's private life are not disclosed to the public without their consent or without a reason recognised by law, thereby preserving the integrity of the inner sphere, which is essential for the positive development of personality. A typical case of violation of the right to personal privacy occurs primarily when someone unlawfully obtains knowledge of facts about the private life of another person, but also when they disseminate such facts." Nevertheless, the Constitutional Court points out that this view is not sufficient, as the respect for private life must also include the right to establish and develop relationships with other human beings.[909] The Czech Office for Personal Data Protection also followed the broad interpretation of the right to privacy in its Opinion No. 6/2009, in which, in an attempt to define privacy, it indicated that "privacy can be briefly described as the personal, intimate sphere of a man in his integrity, which encompasses all manifestations of the personality of a particular and unique human being. The concept of privacy also includes the material and intellectual space of an individual, and the right to create and develop relationships

[906] Šmigová, 2023, p. 171.
[907] Judgment of the Czech Constitutional Court of 20 May 2002, IV. ÚS 315/01.
[908] Siskovičová, 2015, p. 24.
[909] Judgment of the Czech Constitutional Court of 1 March 2000, II. ÚS 517/99.

with other human beings."[910] In one of its rulings, the Constitutional Court of the Czech Republic referred directly to the concept of privacy in relation to employment. In this ruling, the court applied the so-called negative definition, distinguishing between the right to privacy in the sphere of employment and in other strictly private spheres. The Court pointed out that "the right to protection against unauthorised interference with privacy usually applies to cases of interference in the private and family sphere, where individuals freely and autonomously express their personality. However, in this sphere, they are not in a situation where they act and perform official functions in the employer's environment. Similarly, the secrecy of correspondence, the secrecy of other documents and records, and the secrecy of messages transmitted by telephone, telegraph, or other similar means cannot be applied to activities that are, by their nature, work-related."[911] The restriction of an employee's privacy at work stems from the very fact of performing dependent work, i.e., work that is performed personally in a relationship of authority between the employer and the employee, on behalf of the employer and in accordance with the employer's instructions.[912] Clearly, an employee cannot be completely deprived of privacy on the grounds of performing a specific job. Very often, the private and professional spheres overlap, as many work-related activities can be performed in a private home. This is emphasised by the ruling of the Czech Constitutional Court of 8 June 2010, which, in line with the case law of the ECtHR, noted that "it is not possible to make a sharp spatial distinction between privacy in places used for living and privacy in places and environments used for work or business activities or for satisfying one's own needs or interests, even if these activities take place in areas that are accessible to the public or are not enclosed, e.g., business activities, may be subject to certain restrictions that may constitute a certain interference with the right to private life."[913] The failure of the judiciary to adopt a broad understanding of privacy, i.e., excluding it from application in the sphere of employment, could lead to many employees, who perform their work in such a way that their private sphere is intertwined with their professional sphere, being deprived of protection against excessive infringement of their privacy by employers.[914] An example of such a group of employees is those who perform their work remotely.

As regards the concept of privacy in the Hungarian constitutional system, its development has been similar to that in Poland, Slovakia and the Czech Republic. Initially, the Hungarian

[910] Šimečková, 2021, p. 98.
[911] Resolution of the Czech Constitutional Court of 31 March 2009, I. ÚS. 452/09.
[912] Judgment of the Czech Supreme Court of 16 August 2012, 21 CDO 1771/2011.
[913] Judgment of the Czech Constitutional Court of 8 June 2010, Pl. ÚS 3/09.
[914] Siskovičová, 2015, p. 26.

Constitutional Court (under the provisions of the 1949 Constitution of the Republic of Hungary) expressed the view that protection of personal data as the right to privacy should be understood as the right to informational self-determination,[915] which is also consistent with the concept of informational autonomy present primarily in the jurisprudence of the Polish Constitutional Tribunal. In its judgment No. 15/1991 (IV.13), the Court stated that "the right to protection of personal data guaranteed means that everyone has control over the disclosure and use of their personal data. Therefore, personal data may generally only be collected and used with the consent of the data subject (…)."[916] In this judgment, the Court drew attention to an exceptionally important issue that had previously been absent from the judgments of constitutional courts and tribunals of other Visegrad Group countries, namely the requirement of transparency in the processing of personal data. According to the Hungarian Constitutional Court, the whole process of data processing must be transparent and verifiable, which means that everyone has the right to know who is using their personal data, where, when and for what purpose.[917][918]

In a more recent ruling on the right to privacy, the Constitutional Court drew attention to the continuing validity of the concept expressed in the Court's earlier practice, according to which an essential conceptual element of the private sphere is that others cannot enter or view it against the will of the person concerned. Nevertheless, the Constitutional Court did not stop at this statement and, expanding the concept of privacy, pointed out that there is a particularly close link between the right to privacy expressed in Article VI of the Fundamental Law and Article II of the Fundamental Law, which covers the right to human dignity. However, according to the Court, the right to privacy cannot be limited to the internal or intimate sphere excluded from external intervention and protected by Article II, but extends to privacy in a broader sense (maintaining relationships) and to the spatial sphere in which private and family life takes place (home).[919] Moreover, the Constitutional Court stated that when referring to the notion of personal data, we always need to remember that it concerns information about a person's private and family life.[920]

---

[915] Bankó and Szőke 2016, p. 44-45.
[916] Judgment of the Hungarian Constitutional Court, 15/1991. (IV. 13.) AB.
[917] Judgment of the Hungarian Constitutional Court, 15/1991. (IV. 13.) AB.
[918] This position on the requirement for transparency is referred to, for example, in the NAIH decision concerning the violation of employees' privacy in connection with the personal inspection of their luggage – see: Decision of NAIH, NAIH/2017/439/H, p. 17.
[919] Judgment of the Hungarian Constitutional Court, 11/2014. (IV. 4.) AB.
[920] Judgment of the Hungarian Constitutional Court, 11/2014. (IV. 4.) AB.

When analysing the aforementioned judgments of the Hungarian Constitutional Court, it is clear that, despite directly referring to the practice of the ECtHR, it followed a broad concept of privacy, which also includes the possibility of maintaining and establishing social relationships with other people. Although the above judgments did not deal directly with employee privacy, but rather with the privacy of the individual as a human being *per se*, given the practice of the Hungarian DPA, it must be concluded that this concept also applies to the sphere of employment.[921]

2.3. The Limitations of the Right to Privacy

The above analysis of the concept of the right to privacy, as expressed by most courts and constitutional tribunals of the Visegrad Group countries, leads us to the conclusion that this concept in each of the V4 countries has very similar designations and, in practice, is interpreted broadly, bearing the hallmarks of the case law developed by the ECtHR. Nevertheless, although in each of the constitutional systems under consideration, the right to privacy has been recognised as a fundamental human right protected by the "eternal" or "non-derogatory" clause, this does not mean that this right is absolute,[922] as expressed in the case law of both the Polish Constitutional Tribunal[923] and the constitutional courts of Slovakia,[924] the Czech Republic,[925] and Hungary[926].

In its judgment of 26 April 2018, the Polish Constitutional Tribunal indicated that the admissibility of restricting the exercise of informational autonomy is assessed on the basis of three criteria resulting from Article 31(3) of the Constitution,[927] namely utility, necessity, and proportionality *sensu stricto*.[928]

---

[921] See: Decision of NAIH, NAIH/2017/439/H.
[922] Barański 2022, p. 49; Hamuľák and Minčič, 2017, p. 69; Sehnálek 2023, p. 241; Decision of NAIH, NAIH/2017/439/H, p. 14.
[923] Judgments of the Polish Constitutional Tribunal of 14 October 2015, Kp. 1/15; 25 May 2016, Kp 5/15; 11 October 2016, SK 28/15; 26 April 2018, K 6/15.
[924] Judgments of the Slovak Constitutional Court of 29 November 1995, I. ÚS 33/95; 4 February 2009, I. ÚS 117.07.
[925] Resolution of the Czech Constitutional Court of 31 March 2009, I.ÚS 452/09; Judgment of the Czech Constitutional Court of 8 June 2010, Pl.ÚS 3/09; See also: Judgment of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011.
[926] Judgments of the Hungarian Constitutional Court: 15/1991. (IV.13.); 32/2013. (XI. 22.).
[927] Article 31 (3) of the Polish Constitution of 2 April 1997, reads that "Any limitation upon the exercise of constitutional freedoms and rights may be imposed only by statute, and only when necessary in a democratic state for the protection of its security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights."
[928] Judgment of the Polish Constitutional Tribunal of 26 April 2018, K 6/15.

Utility means that the legislator may only introduce restrictions on constitutional rights and freedoms that are justified from the point of view of a rational need for interference in a given legal and factual situation and directly serve the achievement of a constitutionally justified objective.

In order to fulfil the condition of necessity, the legislator may only introduce restrictions that are necessary in a democratic state governed by the rule of law to protect at least one of the values listed in Article 31(3) of the Constitution, if the protection of that value cannot be achieved *in concreto* without restricting rights and freedoms.

In turn, proportionality *sensu stricto* in a situation of interference with an individual's informational autonomy means: a) the existence of legally determined procedural and technical guarantees for the secure processing of personal data; b) limiting the list of data processors to the minimum dictated by the type of data and the purpose of its processing; c) specifying the time frame for data processing; d) the introduction of an effective anonymization mechanism; e) the introduction of provisions enabling stable financing and maintenance of databases in order to ensure their uninterrupted functioning in an era of dynamic development of modern technologies and various types of risks associated with it.[929]

The system for assessing the admissibility of restrictions on constitutional rights and freedoms developed by the Polish Constitutional Tribunal can be compared to the proportionality test used in European Union law, which serves to prove that the measure applied is appropriate to achieve a specific objective related to the public interest, does not go beyond what is necessary to achieve that objective, and that this objective cannot be achieved by applying a less restrictive measure.[930] A proportionality test understood in this way should also apply to regulations issued by a public authority restricting the right to privacy of an individual.[931]

As Oręziak points out, the constitutional regulation of the right to privacy, as well as the requirements of Article 31 (3) of the Constitution concerning the possibility of restricting this right, and consequently also the practice of the Constitutional Tribunal, constitute a timeless solution, resistant to all kinds of technological changes currently taking place. Although Oręziak refers in his conclusion to the broadly understood concept of digital reality and the changes taking place in connection with its development,[932] this position can certainly also

[929] Judgment of the Polish Constitutional Tribunal of 20 January 2015, K 39/12.
[930] Gekiere, Baeten, and Palm, 2010, p. 507.
[931] Oręziak, 2023, p. 322.
[932] Oręziak, 2023, p. 325.

include technological changes in the sphere of work, which in many respects may encroach on the area of the aforementioned digital reality.

The Slovak Constitutional Court does not deviate far from the practice developed by the Polish Constitutional Tribunal and, in its judgment of 29 November 1995, states that state authorities are entitled to interfere with the right to personal data protection, provided that such interference can be considered justified only under Article 19(3) of the Constitution[933].[934] The doctrine indicates that an example of a violation of the right to privacy as a result of the collection of personal data under the Slovak Constitution is the monitoring of employees by their employer. Due to the fact that such monitoring violates one of the fundamental human rights, its conditions must be laid down in a legal act with the rank of a statute.[935] This position is based on Article 13(2) of the Slovak Constitution,[936] and the same conclusion can be drawn with regard to restrictions on the right to privacy in the Czech Republic[937].

However, in the context of restrictions on the right to privacy, the most significant ruling of the Slovak Constitutional Court, which also had a huge impact on legal doctrine, is the ruling of 4 February 2009, in which, based on the jurisprudence of the ECtHR,[938] the court indicated that in the case of interference with an individual's right to privacy, its legality, legitimacy and proportionality must be examined.[939] This ruling raises justified associations with the above-mentioned ruling of the Polish Constitutional Tribunal of 26 April 2018, as, despite a few differences, their essence is consistent.

According to the Constitutional Court, the legality of interference with the right to privacy means that the state may only interfere with the right to privacy on the basis of the law. Therefore, within the framework of the legality of the interference, it is examined whether it took place in accordance with the applicable legal regulations, taking into account whether the legal regulation was publicly disclosed and thus accessible, and whether its consequences were

[933] Article 19 (3) of the Slovak Constitution of 1 September 1992 states that: “Everyone shall have the right to be protected against unjustified collection, disclosure and other misuse of his or her personal data.”
[934] Judgment of the Slovak Constitutional Court of 29 November 1995, I. ÚS 33/95.
[935] Škvarková, 2017, p. 204.
[936] Article 13 (2) of the Slovak Constitution of 1 September 1992 states that: “Limitations of fundamental rights and freedoms shall be regulated only by a law and under the conditions set in this Constitution.”
[937] In the Czech Charter of Fundamental Rights and Freedoms, Article 4(3) is identical to Article 13(2) of the Slovak Constitution.
[938] As Šmigová pointed out “Since most articles of the Constitution protecting several aspects of the right to privacy miss these legitimate aims, it is understandable that the right to privacy protected by the Constitution is being interpreted as applying conditions specified by the Convention.” - See: Šmigová, 2023, p. 171.
[939] Judgment of the Slovak Constitutional Court of 4 February 2009, I. ÚS 117/07.

foreseeable. The quality of the legal regulation that forms the basis for the interference with the right to privacy is therefore also examined.[940]

On the other hand, the legitimacy of interference with the right to privacy stems from Article 8(2) of the ECHR and means that the right to privacy may only be interfered with when it is in the interest of the state for reasons of national security, public safety, the prevention of disorder and crime, in the interests of society for the protection of health and morals, for the protection of the economic well-being of the country, and in the interests of individuals for the protection of their rights and freedoms.[941]

In turn, the proportionality of interference means that interference may only be undertaken when it is necessary (the objective pursued cannot be achieved by less intrusive means) and only in accordance with the requirements of a democratic society characterised by pluralism, tolerance, and a free spirit.[942]

The general principles of legality, legitimacy and proportionality expressed by the Slovak Constitutional Court[943] have been brought down from the vertical dimension to the horizontal one by the legal doctrine and reinterpreted in terms of employee privacy in the context of workplace surveillance. From this perspective, monitoring is lawful only if its use is provided for by law, and its scope and manner of conduct must remain within the limits set by that law. The principle of legitimacy is fulfilled only if the employer has complied with the obligation to inform the employee in advance about the possibility of monitoring, its scope, form and method of implementation. Finally, proportionality means that monitoring is carried out to the extent necessary to fulfil a specific purpose, e.g. protection of the employer's property, and does not violate the human dignity of the employee.[944] In other words, it can be said that a specific form of monitoring will be assessed using the criterion of whether the given purpose could have been achieved by other, less severe means.[945]

As regards restrictions on the right to privacy under the Czech system, we can refer to the conclusions of the Slovak Constitutional Court, since, as already indicated above, the constitutional regulations on the right to privacy in both countries are virtually identical.

However, in one of its rulings, the Czech Constitutional Court addressed the issue of conflict between fundamental human rights or freedoms, which is an important issue in relation

---

[940] Judgment of the Slovak Constitutional Court of 4 February 2009, I. ÚS 117/07.
[941] Judgment of the Slovak Constitutional Court of 4 February 2009, I. ÚS 117/07.
[942] Judgment of the Slovak Constitutional Court of 4 February 2009, I. ÚS 117/07.
[943] Hamuľák and Minčič consider these principles to be components (steps) of the constitutional proportionality test. – See: Hamuľák and Minčič, 2017, p. 69.
[944] Šmigová, 2023, pp. 187-188.
[945] Barancová, 2016, p. 48.

to the right to privacy.[946] In this judgment, the court indicated that in a situation of conflict between two fundamental rights or freedoms, it is necessary to determine the conditions under which one fundamental right or freedom takes precedence and under which conditions another may take precedence. Therefore, there is a fundamental principle that each fundamental right or freedom may be restricted only on account of another fundamental right or freedom. In other words, it can be said that a comparison of rights or freedoms should be made.

Three criteria must be taken into account as part of this comparison. The first is applicability, i.e., whether the restriction of a specific fundamental right allows the achievement of the desired objective (protection of another fundamental right). This criterion can be compared to the criterion of utility existing within Polish constitutional law and the principle of legitimacy expressed by the Slovak constitutional court. The second criterion is the criterion of necessity, which involves comparing a legislative measure restricting a fundamental right or freedom with another measure that can achieve the same objective, but in a way that does not infringe on a fundamental right or freedom. The third criterion is the comparison of the conflicting rights or freedoms, during which empirical, systemic, contextual, and value-oriented arguments should be considered. As an empirical argument, the actual seriousness of the phenomenon related to the protection of certain fundamental rights can be understood. A systemic argument means considering the significance and classification of a given fundamental right or freedom within the system of fundamental rights and freedoms. As a contextual argument, the further negative effects of restricting one fundamental right in order to favour another right can also be understood. Lastly, the value-oriented argument means taking into account the positive aspects of conflicting fundamental rights in relation to the accepted hierarchy of values.[947]

At first glance, the approach of the Czech Constitutional Court is slightly different from that of the Polish and Slovak Constitutional Courts and Tribunals, but in practice, the principles it has laid down largely coincide with the well-established "constitutional proportionality test."

Under the Hungarian fundamental law, the possibility of restricting fundamental rights enjoyed by individuals is established on the basis of Article I (3), which stipulates that, firstly, fundamental rights and obligations should be regulated by an act of law with the force of statute; secondly, these rights may be restricted only to allow the effective use of another fundamental right or to protect a constitutional value; thirdly they might be restricted to the extent necessary

[946] Judgment of the Czech Constitutional Court of 12 October 1994, PL. ÚS 4/94.
[947] Judgment of the Czech Constitutional Court of 12 October 1994, PL. ÚS 4/94.

and proportionate to the objective pursued and with full respect for the essential content of these fundamental rights.

The above provision should be supplemented with the practice concerning the possibility of restricting fundamental rights developed by the Hungarian Constitutional Court. The Hungarian Constitutional Court has formulated the so-called necessity-proportionality test,[948] which means that public authorities may only resort to measures restricting a fundamental right if the protection or enforcement of another fundamental right or value cannot be achieved by other means. However, such a restriction must meet the requirements of proportionality, which means that the weight of the intended objective and the weight of the infringement of the fundamental right must remain in proportion. When regulating the possibility of restricting a fundamental right, the legislator is obliged to apply the least severe measures appropriate to achieve a specific objective. It would be unconstitutional to arbitrarily restrict fundamental rights without a legitimate reason or if it would exceed the intended objective.[949]

Based on the above indications, we can see that the Hungarian model of derogation from fundamental rights also fits within the framework of the broadly understood "constitutional proportionality test." Nevertheless, when deciding on the possibility of restricting the right to personal data protection, the Hungarian Constitutional Court focuses in particular on assessing compliance with the principle of limited purpose and determining whether there is a legitimate public interest in the collection, processing, and dissemination of personal data.[950] However, it should be noted that the mere convergence of a specific purpose with the public interest is not a sufficient basis for restricting a fundamental right. The reason for the restriction must also be expressed in the provisions of the Fundamental Law.[951]

3. Employee's Right to Privacy From the Human Rights Perspective

3.1. The Inclusion of the Professional Sphere in the Concept of Private Life by the ECtHR

As already indicated in the thesis, the key provisions protecting employee privacy in the Visegrad Group countries from a human rights perspective at the international and supranational level are Article 8 of the ECHR and Article 7 of the CFREU, which have similar

[948] Judgments of the Hungarian Constitutional Court: 30/1992. (V. 26.) AB; 30/2015. (X. 15.) AB; 3046/2016. (III. 22.) AB.
[949] Judgment of the Hungarian Constitutional Court, 30/1992. (V. 26.) AB.
[950] Koltay, 2023, p. 105.
[951] Judgment of the Hungarian Constitutional Court, 46/1995. (VI. 30.) AB.

wording. In accordance with Article 32 of the ECHR, which states that the ECtHR is responsible for the interpretation and application of the Convention,[952] and the preamble[953] and Article 52 (3) of the CFREU guaranteeing consistency between the meaning of human rights under the Charter and the Convention,[954] it should be noted that in order to understand the meaning and conditions guaranteeing respect for the right to privacy of employees, as well as the very concept of privacy in the context of human rights, the reference should be made to the case law developed by the ECtHR. Furthermore, the significance of the concept of the right to private life arising from the ECtHR case law is growing alongside the development of the horizontal interpretation of the Convention.[955]

In view of the above, the emphasis of the rest of this chapter will be placed primarily on the analysis of cases concerning workplace monitoring decided by the court in Strasbourg, as the characteristics of the employee's right to privacy presented in them are most relevant to the subject matter of this work.

When analysing the case law of the ECtHR, there is no doubt that the sphere related to an individual's work has been included in the scope of the right to private life.[956] One of the most important judgments in this context is the judgment of 16 December 1992 in *Niemietz v. Germany*, which has already been mentioned several times in this thesis. In this case, the ECtHR ruled that the concept of "private life" cannot be limited only to the notion of an "inner circle"

---

[952] Article 32 of the ECHR reads: "The jurisdiction of the Court shall extend to all matters concerning the interpretation and application of the Convention and the Protocols thereto which are referred to it as provided in Articles 33, 34, 46 and 47."

[953] The fifth paragraph of the preambule to the CFREU states that: "This Charter reaffirms, with due regard for the powers and tasks of the Community and the Union and the principle of subsidiarity, the rights as they result, in particular, from the constitutional traditions and international obligations common to the Member States, the Treaty on European Union, the Community Treaties, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Social Charters adopted by the Community and by the Council of Europe and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights."

[954] Article 52 (3) of the CFREU reads: "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."

[955] Accoridng to the partly dissenting opinion of the Judge Pinto De Albuquerque to the judgment of the fourth section of the ECtHR in case of Bărbulescu v. Romania "the Convention rights and freedoms have a horizontal effect, insofar as they are not only directly binding on public entities in the Contracting Parties to the Convention, but also indirectly binding on private persons or entities, the Contracting State being responsible for preventing and remedying Convention violations by private persons or entities. This is an obligation of result, not merely an obligation of means." See: ECtHR judgment in Bărbulescu v. Romania from 12 January 2016 (Application no. 61496/08), para. 23.

[956] See e.g. ECtHR: of 25 September 2001, P. G. and J. H. v the United Kingdom, Application No.44787/98; of 17 July 2003, Perry v the United Kingdom, Application No.63737/00; of 7 February 2012, Von Hannover v Germany (no. 2), Application No.40660/08; of 12 June 2014, Fernández Martínez v Spain, Application No.56030/07; of 5 September 2017, Bărbulescu v Romania, Application No.61496/08; of 28 November 2017, Antović and Mirković v Montenegro, Application No.70838/13; of 25 September 2018, Denisov v Ukraine, Application No.76639/11; of 17 October 2019, Lopez Ribalda and Others v Spain, Applications Nos.1874/13 and 8567/13; Decision of the ECtHR of 5 October 2010, Köpke v Germany, Application No.420/07.

within which individuals can live their personal life according to their own choices, and to completely exclude the outside from this circle. Therefore, the respect for private life should, to a certain degree, include the right to establish and develop relationships with other human beings. Moreover, the court granted the employee the right to build a social identity[957] in the workplace, pointing out that there is no fundamental reason why the concepts of "private life" should exclude professional or economic activity, since it is during one's professional life that most people have significant, if not the greatest, opportunities to establish relationships with the outside world. It is not always possible to clearly distinguish which activities of a given person are part of their professional or business life and which are not. In particular, in the case of people performing liberated professions, their work in this context may be such an important part of their lives that it is impossible to determine in what capacity they are acting at a given moment.[958]

As Ford points out, the *Niemietz v. Germany* case gives rise to the first of two conceptions of the right to privacy in employment existing on the basis of ECtHR case law.[959] The author presents this conception as one that acknowledges a collective dimension to privacy - a right to develop social relations with other coworkers that are free from external impacts. Implementing this approach may require establishing areas in the workplace that are free from the influence and "gaze" of employers, so that employees can develop free relations there.[960] Referring back to the previously analysed models of workplace monitoring in the Visegrad Group countries, it should be noted that they meet this requirement, and thus it can be said that they take into account the present concept of privacy as a possibility for establishing social relations at work.

The second landmark case concerning the right to privacy in employment is *Halford v. United Kingdom*. This case should be compared to *Niemietz v. Germany*, as the approach to privacy presented by the ECtHR in it is, at least at first glance, slightly different from the one already discussed.

The case was based on an application by Ms Halford, the Assistant Chief Constable of Merseyside Police, concerning her superiors' interception of her work telephone. The complainant was allowed to use the telephone for private purposes and was assured that she could use it to make calls regarding the rejection of her application for promotion within the police force. The Strasbourg Court, finding that there had been a violation of Article 8 of the

---

[957] Barański and Mirosławski, 2023, p. 2.
[958] ECtHR judgment in Niemietz v. Germany from 16 December 1992 (Application No. 13710/88), par. 29.
[959] Ford, 2002, pp. 139-143.
[960] Ford, 2000, p. 30.

Convention, rejected the UK government's position that, due to its managerial powers, the employer had the right to monitor telephone calls made using a telephone that it had provided to Ms Halford. ECtHR stated that there was no evidence that the applicant had been informed of the possibility of her telephone conversations being monitored by her employer, and that she was therefore in a state of “reasonable expectation of privacy.”[961] The case of Halford v. UK is a manifestation of the second of the aforementioned concepts of privacy, namely the concept of “reasonable expectation of privacy.” This concept has been applied in monitoring models in the Visegrad Group countries as an employer's obligation to provide prior information on the possibility of using monitoring.

According to Ford, an analysis of both concepts in relation to the employer's management powers reveals their differences. Firstly, the concept of privacy covering social relations in the workplace is more resistant to potential violations, as established “privacy zones” in the workplace are, in principle, immune to discretionary decisions of the employer. Conversely, the concept based on “reasonable expectations of privacy” can be easily negated by the employer informing employees about the possibility of monitoring.[962]

Nevertheless, considering that in Halford v. UK, the court referred to Niemietz v. Germany, stating that "in the Court’s view, it is clear from its case law that telephone calls made from business premises as well as from the home may be covered by the notions of “private life” and “correspondence” within the meaning of Article 8 of the Convention,"[963] it should be concluded that viewing these concepts as to some extent contradictory does not accurately reflect their character. The concept that includes the professional sphere and building of social bonds defines the conceptual scope of the notion of private life, while the concept of “reasonable expectation of privacy” refers rather to the sphere of conditions of protection guaranteed by Article 8 of the Convention. Therefore, it is justified to state, following Otto, that in reality, both concepts complement each other and express the standards of privacy protection in employment,[964] with particular emphasis on the issue of monitoring.

Leaving aside, although not entirely, above considerations on the concept of privacy in employment, and moving on to analyse the standards of privacy protection set by the ECtHR on the basis of recent rulings on employee monitoring, which have been widely discussed in the case law and doctrine of the Visegrad Group countries, it is still necessary to point out what

[961] ECtHR judgment in Halford v. the United Kingdom from 25 June 1997 (Application No. 20605/92), par. 45.
[962] Ford, 2000, p. 31.
[963] ECtHR judgment in Halford v. the United Kingdom from 25 June 1997 (Application No. 20605/92, par. 44.
[964] Otto, 2019, p. 54.

forms of employee monitoring have been recognised by the Strasbourg court as interfering with the right to privacy at this point.

As can be seen from the *Niemietz* and *Halford cases*, such forms certainly include monitoring an employee's telephone calls and correspondence. In addition, these include: checking the employee's company email account[965] and personal files stored on the company computer,[966] monitoring electronic communications[967] and the employee's activity on the Internet,[968] video monitoring,[969] geolocation monitoring[970] and sobriety tests[971].

3.2. The ECtHR's Approach to Employee Privacy in Light of Recent Cases Concerning Workplace Monitoring[972]

In recent years, the number of cases before the ECtHR concerning employee privacy in the context of workplace monitoring has been steadily increasing. This is due to changing conditions in the labour market, the development of new technologies, the emergence of new forms of work, and above all, the erosion of the dichotomous division between the private and public spheres,[973] which has been confirmed in the case law of the Strasbourg court itself.[974]

In this section, I will focus on a brief analysis of three cases related to the topic of workplace monitoring, which have lately been widely discussed in doctrinal debates and in the case law of the Visegrad Group countries. These cases are: *Bărbulescu v. Romania*, *López Ribalda and Others v. Spain* and *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, and their resolution is a matter of striking the just balance between the rights and interests of employees – the right to respect for their private lives – and the interests and rights of employers – namely, monitoring

965 ECtHR judgment in Copland v. the United Kingdom from 3 April 2007 (Application No. 62617/00).
966 ECtHR judgment in Libert v. France from 22 February 2018 (Application No. 588/13).
967 ECtHR judgment in Bărbulescu v. Romania from 5 September 2017 (Application No. 61496/08).
968 ECtHR judgment in Copland v. the United Kingdom from 3 April 2007 (Application No. 62617/00).
969 ECtHR decision in Köpke v Germany from 5 October 2010 (Application No. 420/07); J ECtHR judgment in Antović and Mirković v Montenegro from 28 November 2017 (Application No. 70838/13); ECtHR judgment Lopez Ribalda and Others v Spain from 17 October 2019 (Application Nos. 1874/13 and 8567/13).
970 ECtHR judgment in Florindo de Almeida Vasconcelos Gramaxo v. Portugal from 13 December 2022 (Application No. 26968/16).
971 ECtHR decision in Madsen v. Denmark from 7 December 2002 (Application No. 58341/00); ECtHR decision in Wretlund v. Sweden from 9 March 2004, (Application No. 46210/99).
972 Based on this fragment, sections authored by Tomasz Mirosławski were prepared and published in the following articles: Barański, M. and Mirosławski, T. (2023) 'Geolocation Monitoring of an Employee from the Perspective of Article 8 of the ECHR', *Acta Univ. Sapientiae, Legal Studies*, 12(2), pp. 3-10, 14-15; Barański, M. and Mirosławski, T. (2025) 'The Principle of Proportionality in the Jurisprudence of the European Court of Human Rights in Cases Concerning Workplace Monitoring', Review of European and Comparative Law, 63(4), pp. 184-202.
973 Arabadjieva and Franklin, 2023, pp. 61-81.
974 Moreham, N.A. 2008, pp. 44-45.

employees, which stems from the employer's obligation to organise process of work appropriately[975].[976]

These cases are a prime example of how the doctrine of interpreting the ECHR as a "living instrument" works in practice, adapting the meaning of the rights contained therein to "present-day conditions"[977] by the ECtHR.

In *Barbulescu v. Romania*, two different judgments were issued, the first by the Fourth Section of the Court and the second by the Grand Chamber. A comparison of the two judgments provides a detailed overview of the standards for the protection of employees' right to privacy established by the ECtHR in the context of monitoring electronic communications.

In its first judgment, the court ruled that there had been no violation of Article 8 of the Convention. In justifying its position, the court emphasised that monitoring by the employer of an employee's activity on an electronic messenger intended for work-related purposes, as a result of which it came to light that the employee also used the messenger for private purposes, falls within the disciplinary powers of the employer laid down in the Romanian Labour Code.[978] Furthermore, the court found that the employer's willingness to verify whether employees were performing their duties properly was reasonable and that, in the case of the monitoring in question, only communications on Yahoo Messenger were checked, while other files stored on the employee's computer remained untouched.[979] Therefore, its scope was limited, and the manner in which it was carried out was proportionate.[980]

Comparing this judgment to the previously cited landmark cases of *Niemietz* and *Halford*, it is clear that the court completely failed to address the specific privacy standards that apply to the employee, namely the ability to establish relationships with the outside world and other people, as well as "reasonable expectations of privacy." This was confirmed by the partially dissenting opinion expressed by Judge Pinto de Albuquerque, in which he criticised the court's narrow reasoning.

The Judge indicated that the majority of the ECtHR and domestic courts overlooked the important facts which should have been analysed in the realm of the case, such the non-

[975] Dörre-Kolasa, 2016, pp. 259-260; Baran, 2016, pp. 35-36.
[976] Barański and Mirosławski, 2025, p. 186.
[977] ECtHR judgment in Tyrer v. the United Kingdom from 25 April 1978 (Application No. 5856/72), para. 31.
[978] ECtHR judgment in Tyrer v. the United Kingdom from 25 April 1978 (Application No. 5856/72), para. 56.
[979] ECtHR judgment in Tyrer v. the United Kingdom from 25 April 1978 (Application No. 5856/72), para. 59.
[980] ECtHR judgment in Tyrer v. the United Kingdom from 25 April 1978 (Application No. 5856/72), para. 60.

existence of an Internet surveillance policy, duly implemented and enforced by the employer, the personal and sensitive nature of the employee's communications that were accessed by the employer, and the wide scope of disclosure of these communications during the disciplinary proceedings brought against the employee.[981] In his opinion, Judge Pinto De Albuquerque paid particular attention to the employer's obligation to adopt a clear internal policy governing the use of the Internet and digital communication tools at work. Although the content of such policies may differ between companies according to their operational requirements, they must always explicitly set out employees' rights and responsibilities. This includes specifying the permitted extent of internet use, the forms of monitoring applied, the procedures for securing, using, and destroying data, and identifying who is authorised to access it.[982] Nevertheless, the exercise of such a policy should be in line with the principles of necessity and proportionality. In practice, it means that before introducing any monitoring measure, an employer should verify that its benefits outweigh the intrusion into the privacy of the employee and third parties communicating with him or her.[983] Accessing or analysing an employee's communications, including metadata, without consent should occur only in exceptional cases and with judicial authorisation. Monitoring must be targeted and based on well-founded suspicions, as broad, unrestricted surveillance is excessive;[984] the least intrusive methods should always be preferred, with filtering generally more appropriate than blocking.[985] Collected data may be used only for its original purpose, must be securely protected from misuse or unauthorised access,[986] shared only with those directly concerned, and deleted once no longer necessary[987].[988]

The demand to establish internal policies on internet use is consistent with, among other things, the strongly emphasised postulate within the Hungarian model of workplace monitoring, which calls on employers to introduce internal policies on the use of electronic devices and workplace monitoring.[989]

---

[981] Partly Dissenting Opinion of Judge Pinto de Albuquerque, Bărbulescu v. Romania (Application No. 61496/08), para. 2.
[982] Partly Dissenting Opinion of Judge Pinto de Albuquerque, Bărbulescu v. Romania (Application No. 61496/08), para. 10.
[983] Working document on the surveillance of electronic communications in the workplace, 29 May 2002, 5401/01/EN/Final WP 55, p. 13; Recommendation CM/Rec(2015)5, para. 20.1.
[984] ILO code of practice on the protection of workers' personal data indicates, 1997, para. 6.14.2.
[985] Recommendation CM/Rec(2015)5, para. 14.2.
[986] Recommendation CM/Rec(2015)5, para. 12.1.; Recommendation No. (89)2, para. 13.
[987] Recommendation CM/Rec(2015)5, para. 13.1.; Recommendation No. (89)2, para. 14.
[988] Partly Dissenting Opinion of Judge Pinto de Albuquerque, Bărbulescu v. Romania, Application No. 61496/08, para. 13.
[989] A Nemzeti Adatvédelmi és Információszabadság Hatóság, 2016, p. 25, 28, 30, 31; Kártyás, Répáczki, Takács, 2016, p. 67.

The lack of such a policy may lead to abuse by employers, who will behave like a distrustful Big Brother with access to monitoring not only the work but also the private lives of employees, leading to the commodification of the employee.[990]

Against the background of the judgment of the Fourth Chamber, Judge Pinto's partially dissenting opinion seems much more insightful with regard to the standards guaranteeing respect for the privacy of employees. The judge indirectly took into account the inequality between the parties to the employment relationship and drew attention to the sensitive nature of the messages monitored. It can therefore be said that the dissenting opinion was delivered in the spirit of the so-called contextual approach and became the starting point for the subsequent judgment of the Grand Chamber.[991]

In its judgment, the Grand Chamber of the ECtHR ruled that employers do indeed have a legitimate interest in ensuring the smooth running of the company, and that this can be done by establishing mechanisms for monitoring that their employees are performing their professional duties adequately and with the necessary diligence.[992] Nevertheless, such a mechanism must satisfy the requirements of proportionality and meet appropriate standards in order to avoid arbitrariness. In this regard, the court has developed six criteria that should be taken into account by national courts when assessing the admissibility of workplace monitoring. These criteria represent a breakthrough in the context of assessing employee privacy in the workplace and can be considered a new instrument in ECtHR doctrine. They are as follows:

1. whether the employee has been notified of the possibility of monitoring their correspondence and other communications, and of the implementation of such measures;
2. the extent of the employer’s monitoring and the degree of intrusion into the employee’s privacy;
3. whether the employer has provided legitimate reasons to justify the monitoring and access to the actual content of communications;
4. whether it would be possible to use less intrusive methods of monitoring instead of directly accessing the content of the employee’s communications;
5. what the consequences of the monitoring are for the employee, and whether the monitoring results contributed to achieving its stated objectives;

[990] Partly Dissenting Opinion of Judge Pinto de Albuquerque, Bărbulescu v. Romania, Application No. 61496/08, para. 15.
[991] Barański and Mirosławski, 2025, p. 189.
[992] ECtHR judgment in Case Bărbulescu v. Romania from 5 September 2017 (Application no. 61496/08), para. 127.

6. whether the employee had been provided with adequate safeguards, especially when the monitoring was of an intrusive nature.[993]

The Strasbourg court ruled that the competent national authorities had failed to properly assess any of the criteria of the above "test of the admissibility of employee monitoring"[994] and pointed out that they did not afford adequate protection of the applicant's right to respect for private life and correspondence and failed to strike a fair balance between the interest at stake. Therefore, it should be stated that there has been a violation of Article 8 of the Convention.[995]

It should also be noted that in this case, the court approved the concept of privacy extending beyond the "inner circle" of the individual, as stated in *Niemietz v. Germany.*[996]

In the *López Ribalda and Others v. Spain,* two opposing judgments were also issued. In the first judgment issued by the Third Section of the ECtHR, the court indicated that there had been a violation of Article 8 of the Convention and that the domestic courts had failed to strike a fair balance between the competing rights and interests of the employees – protection of their privacy and the employer – protection of his property. The Court justified its position by finding that the covert video monitoring was not based on concrete theft suspicions against specific employees but instead targeted all checkout staff. It further noted that the hidden monitoring violated domestic law, as employees had not been given prior, explicit notice of a system collecting their personal data. The Court also considered the duration of the monitoring excessive and held that the employer's interests could have been safeguarded through less intrusive measures, or at the very least, that the measures used could have been safeguarded by giving employees general prior notice of the possibility of their use.[997]

Regarding the judgment, a dissenting opinion was issued by Judge Dedov. Judge Dedov pointed out that although covert monitoring constitutes a significant invasion of an employee's privacy, it would be wrong to interpret the Convention in such a way that it would protect individuals from facing the consequences of their wrongdoing (in this case, theft). Offensive behaviour cannot be covered by the scope of protection of the right to privacy, as priority must be given to the public interest.[998]

---

[993] ECtHR judgment in Case Bărbulescu v. Romania from 5 September 2017 (Application no. 61496/08, para. 121.
[994] ECtHR judgment in Case Bărbulescu v. Romania from 5 September 2017 (Application no. 61496/08, para. 133-140.
[995] ECtHR judgment in Case Bărbulescu v. Romania from 5 September 2017 (Application no. 61496/08, para. 141.
[996] ECtHR judgment in Case Bărbulescu v. Romania from 5 September 2017 (Application no. 61496/08, para. 70.
[997] ECtHR judgment in López Ribalda and Others v. Spain from 9 January 2018 (Applications Nos. 1874/13 and 8567/13), para. 68-69.
[998] Dissenting Opinion of Judge Dedov, López Ribalda and Others v. Spain, Applications Nos. 1874/13 and 8567/13, pp. 32-34.

In its judgment, the Grand Chamber, in assessing whether covert surveillance exceeded the limits of a proportionate interference with the privacy of employees, relied on the six criteria developed by the ECtHR in the *Bărbulescu*; however, indicating that these criteria must be applied taking into account the specificity of the employment relations and the development of new technologies, which may enable measures to be taken that are increasingly intrusive in the private life of employees.[999]

The Strasbourg court pointed out that the national employment courts had carefully weighed the interests of employees and employer, referring to the proportionality assessment criteria developed by the Spanish Constitutional Court, which largely correspond to those resulting from the practice of the ECtHR. National courts examined whether the video surveillance pursued a legitimate aim and whether the means used were suitable and proportionate. In particular, they found that the employer's legitimate objective could not have been achieved through measures that were less intrusive to the applicants' rights.[1000]

Nevertheless, the domestic courts did not attach much importance to the fact that the employer had failed to fulfil his duty to inform his employees, stating that this circumstance did not exceed the limits of proportionality of the interference with the employees' privacy. Referring to the position of the domestic courts, the ECtHR pointed out that only an overriding requirement relating to the protection of significant public or private interests could justify the lack of prior information.[1001] However, when it comes to the present case, the specific circumstances, especially the degree of intrusion into the applicants' privacy and the legitimate reasons for the installation of cover video monitoring, in the opinion of the ECtHR, justify the position of the national authorities that the interference with the applicants' privacy was proportionate. The court noted that not every slight suspicion of misconduct on the part of an employee justifies the use of covert surveillance, but in this case, reasonable suspicion of serious misconduct on the part of the employees and the employer's losses justify the use of this form of surveillance. This conclusion is all the more significant in situations where the suspicion of misconduct is directed not only at one employee but at an entire group, which creates an atmosphere of mistrust in the workplace.[1002] Therefore, the court ruled that there had

[999] ECtHR judgment in López Ribalda and Others v. Spain from 17 October 2019 (Applications Nos. 1874/13 and 8567/13), para. 116.
[1000] ECtHR judgment in López Ribalda and Others v. Spain from 17 October 2019 (Applications Nos. 1874/13 and 8567/13), para. 132.
[1001] ECtHR judgment in López Ribalda and Others v. Spain from 17 October 2019 (Applications Nos. 1874/13 and 8567/13), para. 133.
[1002] ECtHR judgment in López Ribalda and Others v. Spain from 17 October 2019 (Applications Nos. 1874/13 and 8567/13), para. 134.

been no violation of Article 8 of the Convention, thereby upholding the position expressed by Judge Dedov in the dissenting opinion cited above.

The last case discussed in this section is *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, which is the most recent case in terms of ECtHR case law on employee monitoring and the first to address the issue of employee monitoring through geolocation devices.

This case concerned the applicant's dismissal on the basis of data obtained from a geolocation system installed in a vehicle provided by his employer to perform his duties as a medical representative, which he was also permitted to use for private purposes. The applicant argued that the processing of GPS data and his dismissal based on that information violated his right to respect for private life (Article 8 of the Convention). He further claimed that the domestic proceedings relating to his dismissal were unfair and that the final decision breached the principle of legal certainty (Article 6 §1 of the Convention).[1003]

What is particularly important in this case is that the GPS monitoring system installed in the employee's car was kept on 24/7 for three years.[1004]

In the present case, two competing rights were weighed up: the employee's right to respect for his private life and the employer's right to control expenses arising from the use of vehicles entrusted to the employee.[1005] The Portuguese national courts gave greater weight to the latter right, although the Court of Appeal indicated that data collected through GPS monitoring for the purpose of checking compliance with working hours should be considered illegal, as Article 20(1) of the Portuguese Labour Code prohibits remote monitoring of work performance. At the same time, the Court of Appeal stated that not all the geolocation data collected by the employer was unlawful, as data recording travelled kilometres (including kilometres outside working hours) did not constitute remote monitoring of the employee's professional activity.[1006] From the court's position, it can be concluded that data on kilometres served solely for monitoring the company's property. The position of the Court of Appeal was confirmed by the ECtHR, which pointed out that the domestic court, by limiting the retained data only to mileage data, reduced the interference with the employee's private life to what was strictly necessary to

[1003] ECtHR judgment in Florindo de Almeida Vasconcelos Gramaxo v Portugal from 13 December 2022 (Application No. 26968/16), para. 1.
[1004] Joint dissenting opinion of judges Motoc, Pastor Vilanova and Guerra Martins, *Florindo de Almeida Vasconcelos Gramaxo v Portugal,* Application No. 26968/16, para. 10.
[1005] ECtHR judgment in Florindo de Almeida Vasconcelos Gramaxo v Portugal from 13 December 2022 (Application No. 26968/16), para. 115.
[1006] ECtHR judgment in Florindo de Almeida Vasconcelos Gramaxo v Portugal from 13 December 2022 (Application No. 26968/16), para. 119.

achieve the legitimate aim of monitoring the company's expenses.[1007] Therefore, taking into account the criteria for the admissibility of monitoring set out in the *Bărbulescu* case, the majority of ECtHR judges considered the interference with the employee's privacy through GPS monitoring to be proportionate and not in violation of Article 8 of the Convention,[1008] thus confirming (in accordance with point 4 of *Bărbulescu* test) that other less intrusive forms of monitoring than continuous 24-hour geolocation monitoring were not adequate to measure the number of kilometers traveled by the employee.[1009]

This judgment has been strongly criticised by legal doctrine[1010] and by certain judges of the ECtHR, who decided to submit a joint dissenting opinion to the judgment. An analysis of this opinion reveals the complexity of the standards related to the protection of employee privacy.

Firstly, Judges Motoc, Pastor Vilanova, and Guerra Martins pointed out that, in their opinion, the balance between the employee's and employer's rights and interests had been poorly achieved in this case. Their position is justified by the fact that the employer had the ability to monitor the employee 24 hours a day, and therefore also monitored him during periods when he was not working. The employee was constantly monitored for three years, which, according to the judges, clearly exceeds the minimum threshold of severity required by the Court's case law.[1011]

Moreover, it should be indicated that the focus of geolocation monitoring in the sphere of employment, at least in theory, should be limited only to the work tools and other objects entrusted to the employees by the employer. This was also the position taken by the national courts and the ECtHR in this case. Nevertheless, it is obvious that the geolocation of a vehicle enables the geolocation of the driver,[1012] which in turn enables obtaining information about his or her lifestyle.[1013] This possibility varies depending on when and for how long GPS monitoring can be used. Considering that in the *Florindo de Almeida Vasconcelos Gramaxo v Portugal* case, the GPS was turned on all the time and the employee was unable to turn it off, even during

[1007] ECtHR judgment in Florindo de Almeida Vasconcelos Gramaxo v Portugal from 13 December 2022 (Application No. 26968/16), para 120.
[1008] ECtHR judgment in Florindo de Almeida Vasconcelos Gramaxo v Portugal from 13 December 2022 (Application No. 26968/16), para. 119-125.
[1009] ECtHR judgment in Florindo de Almeida Vasconcelos Gramaxo v Portugal from 13 December 2022 (Application No. 26968/16), para. 40, 122.
[1010] See: Molè and Mangan, 2023, pp. 694-700.
[1011] Joint dissenting opinion of judges Motoc, Pastor Vilanova and Guerra Martins, *Florindo de Almeida Vasconcelos Gramaxo v Portugal,* Application No. 26968/16, para. 10.
[1012] Joint dissenting opinion of judges Motoc, Pastor Vilanova and Guerra Martins, *Florindo de Almeida Vasconcelos Gramaxo v Portugal,* Application No. 26968/16, para 6.
[1013] Zannoni, 2018, p. 311.

his free time, the risk of the employer obtaining data about the employee's private life was enormous.

In a dissenting opinion, it was also pointed out that both the majority of the ECtHR and the domestic courts failed to fulfil the obligation set out in the fourth point of the test developed in *Bărbulescu*,[1014] namely to examine whether it was possible to achieve the intended objective by using a less intrusive form of monitoring than continuous GPS monitoring. This objection takes on even greater significance in the context of the fact that the Portuguese DPA, in its resolution 7680/2014 of 28 October 2014, explicitly stated that the use of geolocation outside working hours, as well as when the vehicle is used for private purposes, cannot be accepted. Therefore, the employer should introduce a system (usually in the form of a switch) that allows the GPS in the vehicle to be switched between "work" and "private" modes.[1015]

Taking into account the above cases, and in particular the last one, it is visible that privacy protection standards in ECtHR case law are constantly evolving, and their interpretation depends on many factors that constitute the circumstances of a particular case. However, in order to define the core of the current protection of employees' privacy in the context of monitoring, it would certainly be necessary to refer to two complementary concepts - privacy as a sphere extending beyond the employee's inner circle, enabling him or her to establish relationships with other people and the outside world even during work, as well as the "reasonable expectation of privacy" developed in the cases of *Niemietz v. Germany* and *Halford v. UK*. This core was expanded in 2017 by the admissibility test for a given form of monitoring consisting of six criteria expressed in the *Bărbulescu v. Romania*, which is currently referred to, more or less directly, in every subsequent case in front of the ECtHR concerning monitoring in the workplace.

4. Employee's Right to Privacy as a Personal Right

The final argument, and simultaneously the conclusion of this chapter, highlighting the fact that the right to privacy also extends to employees and applies during working hours, is the nature of this right as a personal right.[1016] This means that this right is a non-pecuniary right, binding without exception and effective *erga omnes*; consequently, all third parties are obliged to refrain

[1014] ECtHR judgment in Bărbulescu v. Romania from 5 September 2017 (Application No. 61496/08), para. 121.
[1015] Joint dissenting opinion of judges Motoc, Pastor Vilanova and Guerra Martins, Florindo de Almeida Vasconcelos Gramaxo v Portugal, Application No. 26968/16, para. 17; ECtHR judgment in Florindo de Almeida Vasconcelos Gramaxo v Portugal from 13 December 2022 (Application No. 26968/16), para. 81.
[1016] Liszcz, 2018, p. 166.

from any infringements of this right.[1017] The significance of this classification should also be viewed in the light of Szpunar's definition of personal goods, according to which personal rights encompass the intangible values associated with an individual's personality that are widely recognised in society.[1018] In a similar vein, Petrik addresses personal rights, pointing out that their primary purpose is to guarantee the freedom of expression of personality and to prevent infringements within the limits set by the community.[1019] These definitions, by referring to the community's standards and social acceptance of values protected by personal rights, highlight their objective nature, which is particularly significant in the event of a potential infringement. In practice, what is also confirmed by jurisprudence and the doctrine, this means that an infringement of a particular personal right depends on objective criteria (as a rule determined by public reaction), rather than on the subjective feelings of the concerned individual.[1020] This is particularly important in the case of such a personal right as the right to privacy, since it prevents unjustified claims which might result in the overload of the courts with a large number of unfounded lawsuits.[1021]

The personal character of an employee's right to privacy is recognised in all the legal systems of the Visegrad Group countries. However, the approach taken by individual national legislators in defining the nature of this right is not uniform.

In Hungary, the personal nature of an employee's right to privacy is enshrined in the Labour Code and is also derived from provisions of the Civil Code and the Act LIII of 2018 on the Protection of Private Life.

Under the Hungarian Labour Code, the issue of personal rights is regulated in Section 9. The key provision of this section is paragraph 1, which stipulates that in relation to the protection of the personal rights of employees and employers, the provisions of the Civil Code apply.[1022]

The Civil Code explicitly includes private life in the list of values protected by personal rights set out in Section 2:42, stating that everyone is, in principle, entitled to it, although in exercising this right, restrictions resulting from the law and the rights of others must be taken into account.[1023] What is crucial in the context of an employment relationship is that the following provision specifies that a breach of personal rights should, in particular, be

---

[1017] Grzybowski, 1957, p. 17.
[1018] Szpunar 1979, 106.
[1019] Petrik, 2014, pp. 173 – 174.
[1020] Kuba, 2014, 3.3. Poszanowanie przez pracodawcę dóbr osobistych pracownika; Judgment of the Polish Supreme Court of 16 January 1976, II CR 692/75; Judgment of the Polish Supreme Court of 26 October 2001, V CKN 195/01; Judgment of the Polish Supreme Court of 5 April 2002, II CKN 953/00.
[1021] Kalus 2018, Art. 23.
[1022] Section 9 (1) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[1023] Section 2:42 (1) of Act V of 213 on the Civil Code; See also: Koltay, 2023, pp. 81-82.

understood as a breach of privacy and the right to the protection of personal data.[1024] Such a breach of privacy will occur when the interference with this right is unjustified and arbitrary.[1025] An interference should be regarded as arbitrary if it is clearly contrary to the will and intention of the person concerned, and if such interference is not justified even after careful consideration of the circumstances.[1026] On the other hand, given that an employment relationship often requires certain restrictions on the right to privacy, as exemplified by the main subject of the thesis, namely workplace monitoring, the labour code stipulates that personal rights may be restricted where it is absolutely necessary for reasons directly related to the employment relationship and proportional in terms of its goals.[1027] These conditions mean, respectively, that without imposing a specific restriction, the employer would not be able to fulfil its obligations arising from the employment relationship in the narrow sense (focusing primarily on the rights and obligations of the parties to the relationship).[1028] Furthermore, any measures that restrict an employee's privacy must be preceded by an assessment of the balance between the employee's interests and the disadvantages caused to the employee, so as to ensure that the restriction in question complies with the principle of proportionality.[1029] It is of the utmost importance that the employee should be informed in advance, in writing, of the circumstances indicating the necessity and proportionality of the restriction of his or her personal rights. Furthermore, the information should also specify the manner, conditions and anticipated duration of the restriction.[1030] This obligation has significant implications for the information provided by the employer to the employee in situations involving the use of workplace monitoring. Moreover, as a general rule, an employee may not waive his or her right to privacy in advance.[1031]

In addition to the labour and civil codes, the personal character of the right to privacy is also emphasised in the 2018 Act LIII on the protection of privacy, which constitutes a specific reference to Article VI of the Hungarian Fundamental Law.[1032] This act introduces in a direct manner a new approach to privacy protection, as it recognises that modern technological development has changed the way people interact with each other; therefore, the protection of privacy is no longer confined merely to the physical world, but also extends to the online sphere,

[1024] Section 2:43 (b) and (e) of Act V of 213 on the Civil Code.
[1025] Lukács, 2021, p. 47.
[1026] Judgment of Kúria (Curia/Supreme Court), BH 2001.2.61.
[1027] Section 9 (2) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[1028] T/4786. számú törvényjavaslat a Munka Törvénykönyvéről, p. 100; Kardkovács, 2014, p. 52.
[1029] Kardkovács, 2014, p. 52.
[1030] Section 9 (2) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[1031] Section 9 (3) of Act I of 2012 on the Labor Code (Hungarian Labour Code).
[1032] Lukács, 2021, p. 50.

including social media.[1033] This stance provides an essential backdrop to the definition of the right to privacy stated in the act, according to which the right to privacy constitutes a part of the right to free development of personality, which might be expressed in the freedom to responsibly and individually form one's life and, among other things, shape social contacts.[1034] In light of the preamble, such contacts also extend to contacts established online. This definition of the right to privacy closely resembles that set out in the case law of the European Court of Human Rights in Strasbourg. The regulation, similarly to the Hungarian Civil Code, combines privacy with the protection of personal data, as it stipulates that any misuse of personal data constitutes a violation of the right to privacy.[1035] Furthermore, the Act stipulates that the protection of the right to privacy falls within the scope of the protective measures designed to safeguard personal rights as set out in the Civil Code.[1036]

In turn, the Czech legislator has adopted a distinctive approach by not including a general provision in the Labour Code relating to the protection of an employee's personal rights, whilst listing privacy among the protected values. Instead, the personal nature of the right to privacy is derived from the title of chapter VII of the labour code – "Protection of an Employer's Property Interests and Protection of an Employee's Personal Rights."[1037] This chapter consists solely of Section 316, which is discussed in detail in this thesis, as it forms the basis of the Czech model of workplace monitoring. The adopted solution most literally illustrates the nature of the right to privacy as a personal right, linking it directly to the issue of monitoring.

Naturally, employees' right to privacy is also protected under civil law, since, as Section 3 (2) (a) of the Czech Civil Code states, everyone has the right to protect their life and health, as well as freedom, honour, dignity and privacy.[1038] As Sehnálek indicates, the mentioned provision is merely a repetition of the constitutional rules on the protection of privacy; therefore, it should be rather perceived as the legislator's effort of highlighting the importance of privacy protection and drawing attention to its horizontal application.[1039] Further provisions of the Civil Code set out more detailed protection of the right to privacy. Section 81, which serves as a general clause, stipulates that privacy is one of the values enjoying special protection.[1040] This provision forms the basis for Section 86, which relates more directly to the

[1033] Preamble of the Act LIII of 2018 on the protection of privacy.
[1034] Section 8 (1) of the Act LIII of 2018 on the protection of privacy.
[1035] Section 8 (2) of the Act LIII of 2018 on the protection of privacy.
[1036] Section 12 of the Act LIII of 2018 on the protection of privacy.
[1037] Chapter VII of the Czech Labour Code (full translation) No. 262/2006 Coll., as amended "Zákoník práce".
[1038] Section 3 (2) (a) of Act of 3 February 2012 the Civil Code, 89/2012 Sb.
[1039] Sehnálek, 2023, p. 244.
[1040] Section 81 (2) of Act of 3 February 2012 the Civil Code, 89/2012 Sb.

issue of privacy protection, indicating its *erga omnes* application as it states that no one has the right to intrude on another person's privacy without a legal justification. In particular, without that person's consent, it is forbidden to enter their private property, monitor or record their private life through audio or video, use recordings of their private life made by others, or share such recordings. Personal documents of a private nature are afforded the same level of protection. This regulation attaches great importance to consent as the basis for restricting the right to privacy; nevertheless, it should be noted that, in the case of workplace monitoring, the basis for such a restriction is, as a rule, not the employee's consent but rather the employer's legitimate interest.

As is the case with the Czech Labour Code, Slovak labour law also lacks a provision that would comprehensively address the protection of an employee's personal rights. This does not, however, alter the fact that the Slovak Labour Code provides for the protection of certain aspects of personal rights, including the right to privacy.[1041] Such protection is certainly provided for by Article 11, which constitutes one of the main principles of Slovak labour law covering the issue of the protection of employees' personal data, stipulating that only data relating to the employment relationship in the wider sense may be collected and processed, as well as Section 13(4), which regulates the issue of workplace monitoring. However, given that civil law with regard to personal rights constitutes *lex generalis* in relation to labour law, and that the Labour Code itself refers to the application of the provisions of the Civil Code,[1042] employees may also rely on the protection provided for in the Civil Code to safeguard their right to privacy.

Under the Civil Code, the protection of privacy is regulated in Sections 11 – 16. Section 11 of the Civil Code states that everyone has a right to the protection of their personality, of which an important element is privacy.[1043] It can be deduced from the subsequent provisions that elements of privacy include, amongst other things, personal documents, likenesses, photographs, and visual and audio recordings relating to a natural person or his or her personal opinions.[1044] As part of judicial protection against unlawful infringements of privacy, an individual may seek: 1. the cessation of such infringements, 2. the elimination of such infringements, and 3. appropriate redress, and in some cases even compensation for harm

[1041] Šmigová, 2023, p. 187.
[1042] Section 1 (4) of the Slovak Labour Code.
[1043] Section 11 of the Slovak Civil Code, 40/1964 Zb.
[1044] Section 12 (1) of the Slovak Civil Code, 40/1964 Zb.

suffered.[1045] These measures may be applied separately or jointly, depending on the circumstances of the case.[1046]

A particularly interesting perspective on the protection of employees' personal rights, including the right to privacy, is provided by the Polish legal system, and above all by the accompanying legal doctrine and case law. This is because Article 11^1 of the Polish Labour Code stipulates that an employer is obliged to respect the dignity and other personal rights of an employee.[1047] It may seem that, in light of Articles 23 and 24 of the Polish Civil Code, which guarantee general protection of personal rights, this article appears superfluous; however, as Kuba points out, its scope in the context of employment is broader. On this basis, the employer must not only refrain from infringing employees' personal rights, but is also obliged to create such conditions in the workplace that effectively promote respect for employees' personal rights.[1048]

Article 11^1 PLC does not set out a list of personal rights. Such a catalogue is provided in Article 23 of the Polish Civil Code; however, it does not explicitly mention the right to privacy.[1049] Nevertheless, this does not mean that privacy is not a protected personal right under Polish law. As the Supreme Court points out, the list set out in the Civil Code is not exhaustive and also includes personal rights relating to private and family life, as well as the sphere of intimacy.[1050] Furthermore, case law has established that every person's private life is always subject to full legal protection.[1051] It should also be noted that the recognition of the right to privacy as a distinct personal right has been largely driven by legal scholarship. One of the pioneers of research on privacy as a separate personal right was Kopff, who stated that

"A personal right in the form of private life is everything which, by virtue of an individual's justified separation from the general public, serves to develop his or her physical and mental personality and to maintain his or her achieved social position."[1052]

[1045] Section 13 (1) of the Slovak Civil Code, 40/1964 Zb.
[1046] Šmigová, 2023, p. 174.
[1047] Article 11^1 of the Polish Labour Code of 1974 (Dz.U.1974.24.141). It is important to state that the Polish legislator has given this provision the status of a fundamental principle of labour law by including it in Chapter II of the Labour Code, which is dedicated to list such principles.
[1048] Kuba, 2014, 3.3. Poszanowanie przez pracodawcę dóbr osobistych pracownika.
[1049] Article 23 of the Polish Civil Code (Dz. U. 1964 Nr 16 poz. 93) only states that "an individual's personal rights, such as, in particular, health, liberty, honour, freedom of conscience, name or pseudonym, image, confidentiality of correspondence, inviolability of the home, and scientific, artistic, inventive and innovation-related works, are protected by civil law, irrespective of the protection provided by other provisions."
[1050] The judgment of the Polish Supreme Court of 18 January, 1984, I CR 400/83.
[1051] The judgment of the Polish Supreme Court of 11 March, 1986, I CR 4/86.
[1052] Kopff, 1972, p. 32.

Currently, the view that privacy must be treated as a distinct personal right has been widely accepted by the doctrine.[1053] This approach to privacy confirms the position expressed by the Supreme Court that everyday practice is constantly giving rise to new categories of personal rights,[1054] which to some extent resembles the "living instrument" doctrine applied by the European Court of Human Rights. After all, the link between the two concepts is not without merit, given the similarities between the nature of personal rights and of human rights. Moreover, in this context, it should be noted that in the 2018 draft of the new Polish Labour Code, employees' rights were designated as human rights,[1055] which is not without significance in relation to the right to privacy.

In view of the above, it should therefore be noted that, although neither the Polish Labour Code nor the catalogue of personal rights set out in the Polish Civil Code explicitly mentions the right to privacy, this right is in fact a personal right. The consequence of this classification for employees is that their privacy benefits from protection under both labour law and civil law. Furthermore, taking into account the various aspects of employees' right to privacy present in the legal systems of the other Visegrad Group countries, it should be noted that, in addition to labour law and civil law, it is also protected under human rights law, constitutional law, and data protection law.

To conclude the line of reasoning, which has led to the conclusion that privacy is undoubtedly an integral part of an employee's personal rights, it is worth briefly highlighting one further point. As noted at the beginning of this chapter, individual autonomy is regarded as the essence of privacy on the Old Continent.[1056] This autonomy may, however, be restricted in justified cases, including in the workplace, where, for instance, due to organisational reasons, the employer decides that the use of measures of monitoring is necessary. However, is there an area of an employee's privacy that cannot, under any circumstances, be subject to the employer's intervention?

Kopff points out that within the sphere of privacy, a distinct subset can be identified – the area of intimacy. This area encompasses personal experiences, facts and feelings that are rarely even shared with those closest to us, and whose disclosure is often associated with feelings of

[1053] See: Wujczyk, 2012, 2.2.4. Prywatność jako dobro osobiste; Kuba, 2014, 3.3. Poszanowanie przez pracodawcę dóbr osobistych pracownika; Pryciak, 2010, pp. 223.
[1054] The judgment of the Polish Supreme Court of 9 July 2009, II PK 311/08.
[1055] Art. 1 (1) of the draft of the new Polish Labour Code of 14 March 2018.
[1056] Liszcz, 2018, p. 165.

embarrassment, shame and distress.[1057] It is traditionally accepted that the private sphere encompasses information relating to an individual's emotional state and feelings, health, addictions, sex life and sexual orientation[1058], family ties, religious beliefs, etc., and that it deserves full legal protection.[1059]

Currently, in the context of the area of intimacy, it is possible to refer to the list of special categories of personal data set out in Article 9 of the GDPR, the processing of which is, as a rule, prohibited. Such a list includes data disclosing racial or ethnic origin; political opinions; religious or philosophical beliefs or trade union membership; genetic data; biometric data, whose purpose of processing is to unambiguously identify a natural person; health data and data concerning a sex life or sexual orientation.[1060] Nevertheless, even with regard to this data, the Regulation provides for the "exceptional" possibility of processing it in specific cases indicated in paragraph 2 of Article 9 GDPR.[1061]

Leaving aside the controversy associated with such a broad definition of specific categories of personal data and the inclusion in the list, for example, information about trade union membership, which is not necessarily considered intimate, the approach adopted by the European legislator highlights a broader issue stemming from the direction in which the modern world is developing.

In earlier times, before the widespread availability of the Internet, mass transport and the emergence of the global economy, the sphere of intimacy was protected by clearly defined boundaries linked to the existing social hierarchy and characteristic class divisions, and even by physical barriers such as state borders. Owing to technological advances and the accompanying social changes, these barriers have been completely dismantled or significantly reduced, which has certainly brought many positive effects, but also significant negative consequences. Globalisation, the shape of the increasingly international labour market, the volume of social and economic connections between countless entities, and the accompanying need for regulation by nation states and international organisations, have resulted in a situation where, in practice, it is difficult to define a sphere of an employee's privacy in relation to which it can be said with certainty that there will under no circumstances be a need for the employer to intervene in it.

[1057] Kopff, 1972, p. 32.
[1058] ECtHR stated that sexual life is the most intimate aspect of private life. See: ECtHR judgment in case of Dudgeon v. the United Kingdom from 22 October 1981 (Application no. 7525/76), 52.
[1059] Sut, 1994, p. 103; Kuba, 2014, 3.3. Poszanowanie przez pracodawcę dóbr osobistych pracownika; Liszcz, 2018, p. 164.
[1060] Article 9 (1) of the GDPR.
[1061] Article 9 (2) of the GDPR.

This situation is not improved by employers' growing interest in employees' "soft skills"[1062] and personal traits, as mentioned in Chapter I of the thesis, nor by the nature of contemporary mass culture, which virtually rewards personal exhibitionism. Therefore, in order to protect individuals, including employees, from excessive intrusion into their intimate sphere, often brought about by their own more or less conscious actions, one must agree with Liszcz that, with regard to the intimate sphere, a general factual presumption should be adopted, assuming that it is every person's intention to protect the intimate details of his or her life from disclosure, and that it is the third party seeking to use such intimate information who bears the burden of proving that the person in question does not keep them secret from others.[1063]

[1062] See also: Barański and Mirosławski, 2026
[1063] Liszcz, 2018, p. 165.

Chapter IV. Axiological Considerations on Workplace Monitoring

1. Monitoring and the Protective Function of Labour Law - Scope of Monitoring and the Axiological Basis of Labour Law

1.1. Human Dignity

As Immanuel Kant indicated in “Fundamental Principles of the Metaphysics of Morals”:

“In the kingdom of ends, everything has either Value or Dignity. Whatever has a value can be replaced by something else which is equivalent; whatever, on the other hand, is above all value, and therefore admits of no equivalent, has a dignity. Whatever has reference to the general inclinations and wants of mankind has a market value; whatever, without presupposing a want, corresponds to a certain taste, that is to a satisfaction in the mere purposeless play of our faculties, has a fancy value; but that which constitutes the condition under which alone anything can be an end in itself, this has not merely a relative worth, i.e., value, but an intrinsic worth, that is dignity. Now morality is the condition under which alone a rational being can be an end in himself, since by this alone is it possible that he should be a legislating member in the kingdom of ends. Thus morality, and humanity as capable of it, is that which alone has dignity (…).”[1064]

The personalism expressed in Kant’s thought has permeated labour law theory and contributed to the development of the concept of the personalistic dimension of human labour, which has significantly influenced the arguments present in this thesis.

Personalistic dimension of human labour can be boiled down to the statement that “the object of transaction in an employment relationship is not a commodity but the human being as such”[1065], which, in other words, means that when performing labour, it is not an object of property that is delivered but the person who performs the labour, therefore creating the property.[1066] Sinzheimer, known as the father of German labour law, pointed out that “labour is man himself in the state of working. Labour is a source of property but not an expenditure of property.”[1067]

[1064] Kant, 1785(1889)(2011), p. 57.
[1065] Weiss, 2011, p. 44.
[1066] Sinzheimer, 1927, p. 3
[1067] Sinzheimer, 1927, p. 3.

The act of working is not limited to performing or assisting in a specific task or object but involves placing one's entire self at the employer's disposal in order to perform a specific job at a designated time and place. Fulfilling the role of an employee does not mean that the rest of our personality is switched off at the same time, nor that the social relationships that bind us are suspended for the duration of work.[1068] The impossibility of separating labour from the person performing it, combined with the fact that every human being possesses inherent dignity, means that labour cannot be treated as a commodity subject to standard market exchange.

As a pioneer[1069] of the thought on the de-commodification of labour is the Irish economist Dr John Kells Ingram, who in 1880 at the British Trades Union Congress in Dublin, delivered a speech entitled "Work and the Workman", in which he stated that perceiving labour solely as a commodity strips it of the moral foundation on which the relationship between employee and employer should be based, leaving it entirely at the mercy of so-called laws of the market.[1070]

On the other hand, a rigid criticism of the commodification of labour, grounded in the concept of inherent human dignity, is particularly prominent in the social teaching of the Catholic Church. Pope John Paul II, in a key encyclical for working people, "Laborem Exercens", argues that exclusive focus on the objective dimension of work leads to a reversal of the proper order of values. Pope indicates that reducing labour to a mere commodity or "labour force" is particularly driven by the ideology of materialistic economism, which prioritises production over the person. That, in turn, leads to treating man as a tool of production, while according to the Book of Genesis, he alone, disregards the work he does, should be treated as its active subject, genuine maker and creator.[1071]

The position expressed by John Paul II is by no means an isolated one; rather, it reflects a line of thought that has been systematically developed within the Catholic Church, standing in opposition to the primacy of economism and materialism. This stance was articulated prior to the publication of "Laborem Exercens", most notably in Pope Leo XIII's "Rerum Novarum"[1072] and Pius XI's "Quadragesimo Anno"[1073]. Subsequently, the social doctrine concerning the dignity of the working people was further developed by John Paul II's successors, particularly

[1068] Liszcz, 2018, p. 33.
[1069] Nevertheless, it should be noted that the inspiration for formulating a comprehensive theory of the decommodification of labour comes from Karl Marx, who was the first to describe in detail the phenomenon (which Marx termed an 'illusion') of commodity fetishism present in the capitalist mode of production, and pointed out that it leads to the reification of the labour force, that is, a situation in which human beings, real subjects, appear in the labour process as commodities bought and sold on the market according to the rules dictated by the law of value - See: Kołakowski, L., 1976(2000), pp. 331-337.
[1070] Ingram, 1880, p. 5-6.
[1071] Pope John Paul II, 1981(2021), para. 7, pp. 25-26.
[1072] Published on 15 May 1891.
[1073] Published on 15 May 1931.

Pope Francis, in his encyclicals "Laudato Si'"[1074] and "Fratelli Tutti"[1075] and Leo XIV's in the encyclical "Magnifica Humanitas"[1076].

Pointing to the inseparable bond between work and the worker, Leo XIII describes labour as both personal and necessary - it belongs to the worker as an expression of the self, and its fruits enable survival, which is an indisputable law of nature that must not be defied.[1077]

The teaching on the need to uphold human dignity in the context of work, articulated by the aforementioned successors of St. Peter, found fertile ground in the Visegrad Group countries during the period of Soviet-style dictatorships, a notable example of which is the figure of the Polish Blessed and Martyr of the Catholic Church, Father Jerzy Popiełuszko, known as the workers' chaplain. As an illustration of Father Popiełuszko's concern for and struggle for the dignity of working people, the following quote from a homily He gave on 24 April 1983 at St Stanislaus Kostka's Church in Warsaw during one of the famous "Masses for the Homeland" serves as a good example:

"Work is an indispensable part of human life. It is meant to serve people and to ennoble them. Therefore, people must not become slaves to work, nor should they be viewed solely in terms of their economic value. In one's personal, social or professional life, one cannot build everything solely on materialism. Material things must not take precedence over the spiritual side of human nature."[1078]

Analysing the above, we can therefore see that in both intellectual traditions - secular and ecclesiastical - there is a strong conviction that human labour is a value in itself, and that any attempt to commodify it, or to subject it exclusively to market "forces", would lead to a violation of the dignity of the worker, which stems from the very fact of being human. Liszcz describes this approach to the nature of work as ethical (personalistic), in contrast to the economic (commodity-based) approach, and argues that the dignity of the worker can only be protected on the basis of an ethical conception of human labour.[1079]

Eventually, the impact of the above ideas became apparent at the normative level. Under international law, in the Universal Declaration of Human Rights and the International Covenant on Economic, Social and Cultural Rights, human dignity is invoked as the basis for all the

1074 Published on 18 June 2015.
1075 Published on 4 October 2020.
1076 Published on 25 May 2026.
1077 Pope Leo XIII, 1891, para. 34, p. 46.
1078 Fr. Popiełuszko, 1983.
1079 Liszcz, 2018, p. 26.

inalienable rights of human beings enshrined in these acts.[1080] Under EU law, it is stated that human dignity is one of the fundamental values of the EU.[1081] Furthermore, the entire first chapter of the Charter of Fundamental Rights of the European Union is devoted to human dignity; according to this, dignity is inviolable and must be respected and protected, and in particular comprises the right to life, the right to personal integrity, the prohibition of torture and inhuman or degrading treatment or punishment and the prohibition of slavery and forced labour.[1082] It should also be noted that, although the concept of human dignity (apart from Protocol No. 13) is not explicitly mentioned in the European Convention on Human Rights, it nevertheless plays a significant role in the case law of the European Court of Human Rights.[1083] In turn, with respect to a more detailed understanding of dignity in relation to the individual employee, this is enshrined in the principle that labour should not be treated merely as a commodity, set out in the 1919 Treaty of Versailles establishing the ILO.[1084] The European Social Charter also explicitly states that all workers have the right to dignity at work.[1085]

Moreover, human dignity has also become the axiological foundation of human rights and freedoms, including the employment sphere, within the constitutional systems of all V4 countries. The constitutions of the Visegrad Group countries recognise that dignity is an inherent value of every human being and is therefore inviolable.[1086] Nevertheless, among these four countries, the Hungarian constitutional provision stands out in particular, as it explicitly refers to the need to respect the dignity of employees at work.[1087] Nevertheless, it should be noted that the constitutional concept of dignity has primarily a vertical dimension, that is, referring to the relationship between the individual and the public authorities. This dimension

---

[1080] Universal Declaration of Human Rights of 10 December 1948, preamble; International Covenant on Economic, Social and Cultural Rights of 16 December 1966, preamble.

[1081] Article 2 of the Consolidated Version of the Treaty on European Union of 26 October 2012, C 326/13.

[1082] Chapter 1 of the CFREU.

[1083] See: Fikfak and Izvorova, 2022, pp. 1-24.

[1084] Article 427 of the Part XIII of the Treaty of Peace of Versailles of 28 June 1919.

[1085] Part I (26) of the European Social Charter (Revised) of 3 May 1996, ETS No. 163.

[1086] Article 30 of the Constitution of the Republic of Poland of 2 April 1997; Article 12 of the Constitution of the Slovak Republic of 1 September 1992; Article 1 of the Charter of Fundamental Rights and Freedoms of the Czech Republic of 16 December 1992; Article II of the Fundamental Law of Hungary of 25 April 2011.

[1087] Article XVII (3) of the Fundamental Law of Hungary of 25 April 2011 states that “every employee shall have the right to working conditions which ensure respect for his or her health, safety and dignity.”

is outlined in the provisions themselves[1088] and confirmed in constitutional law literature[1089]; in practice, it means that state authorities must refrain from actions that would lead to a violation of human dignity (negative aspect), and should also take measures to ensure that the individual's dignity is respected (positive aspect).

1.2. Worker's Dignity

In view of the above, there is no doubt that the human dignity enshrined in the constitutional systems of the V4 countries serves, in a sense, as a starting point for the protection of dignity in the context of employment relations. Nevertheless, a distinction must be drawn between human dignity as such and the dignity of the worker, as enshrined in labour law.

The primary reason for this distinction lies in their affiliation with two distinct concepts of dignity: personal dignity (axiological-ontic) and personality dignity (empirical). Under the first conception, dignity is understood as an inherent value to which every human being is entitled by virtue of the fact that human beings, by their very nature, are rational, free beings endowed with a conscience, and thus occupy a special place in the world. Such dignity is a permanent, universal and inalienable value, and certainly includes the dignity enshrined in the respective constitutions and constitutional acts of the Visegrad Group countries. Worker dignity, on the other hand, stems from the fact of being a working person; it is therefore not inherent and permanent, and consequently, it should be classified under the second concept, which holds that dignity is a perfection born of morally valuable action and embedded in one's character. It is achieved through upbringing, personal self-improvement or the influence of the social environment.[1090]

Secondly, the specific nature of workers' dignity in relation to human dignity stems from the very fact of the creation of a branch of law known as labour law. As Pope Pius XI pointed out:

[1088] Firstly, the basis for this can be found in the 'inviolability' of dignity as expressed in all four constitutional orders; and secondly, the state's duty to respect and guarantee dignity is particularly evident from the second sentence of Article 30 of the Polish Constitution
("it [human dignity – author's note] is inviolable, and its respect and protection is the duty of public authorities") and in Article 19(1) of the Slovak Constitution and Article 10 (1) of the Czech Charter of Fundamental Rights and Freedoms, which read in the same way – "Everyone shall have the right to maintain and protect his or her dignity, honour, reputation and good name."
[1089] Poland - See: Garlicki, 2016, Art. 30; Lis-Staranowicz and Dobrowolski, 2022, p. 104; Slovakia - See: Ľalík, 2019, pp. 800-803; Czech Republic - See: Benák, Vyhnánek and Zahumenský, 2019, pp. 205-209; Hungary: Deli and Kukoreli, 2019, p. 396; Tóth, 2003, pp. 255-361.
[1090] Mrozek, 2014, p. 43; See also: Musiała, 2019, p. 124; Liszcz, 2018, pp. 22-23.

"A new branch of law, wholly unknown to the earlier time, has arisen from this continuous and unwearied labour to protect vigorously the sacred rights of the workers that flow from their dignity as men and as Christians. These laws undertake the protection of life, health, strength, family, homes, workshops, wages and labor hazards, in fine, everything which pertains to the condition of wage workers, with special concern for women and children."[1091]

Labour law doctrine itself holds that the primary purpose of labour law is to safeguard the dignity of the employee as the weaker party in the employment relationship, by protecting rights and freedoms such as: freedom of work, the right to work, the right to protection of life and health, the right to fair and equitable remuneration, freedom of conscience and religion, the right to an undisturbed family life, the right to protection of honour, the right to privacy, the right of association, and the right to strike.[1092]

Thirdly, just as the general duty to respect human dignity and to take measures to safeguard it rests, under the constitutional order, with the public authorities, in the case of the dignity of the worker, this duty falls primarily on the employer, who is responsible for working conditions and the organisation of the work process.[1093]

The key argument in favour of the need to single out, and in a sense distinguish, worker dignity from universal human dignity appears to be the very intention of national legislators, particularly the Polish one, as Article 11^1 of the Polish Labour Code explicitly states that an employer shall respect the dignity and other personal rights of an employee. On the other hand, the labour codes of the other Visegrad Group countries do not explicitly refer to the obligation to respect the dignity of the employee, which does not mean that such an obligation does not exist. In the Hungarian Labour Code, the need to protect the dignity of the employee can be inferred from Section 9, which reflects the civil law protection of the personal rights of the employee (and the employer).[1094] In contrast, the Slovak and Czech Labour Codes are characterised by an indirect model of protecting the dignity of employees through other institutions of labour law such as the prohibition of discrimination or the protection of

[1091] Pope Pius XI, 1931, para. 28, p. 22.
[1092] Liszcz, 2018, p. 26.
[1093] Góral writes that "the employer is obliged to "respect" the dignity and other personal rights and this cannot be reduced solely to an obligation to refrain from violating them. Respect for dignity and personal rights of employees means that the employer should take care of appropriate working environment which favours development of proper interpersonal relations." - Góral, 2016, pp. 57-58; See also: Musiała, 2019, p. 127.
[1094] Section 9 (1) of the Act I of 2012 on the Labour Code (Hungarian Labour Code) states that for the protection of the personal rights of the employee and the employer, if this law does not provide otherwise, Act V of 2013 on the Civil Code (Hungarian Civil Code) must be applied.

employee's privacy.[1095] It is significant that Chapter VIII of the Czech Labour Code, which includes Section 316 relating primarily to the issue of monitoring and the protection of employees' personal data, is entitled "Protection of an Employer's Property Interests and Protection of an Employee's Personal Rights", which indirectly defines the conceptual scope of an employee's personal rights, including his or her dignity.

Looking at the above models of regulating workers' dignity under the labour laws of Poland, Slovakia, the Czech Republic and Hungary, the conclusion that emerges is that, of these four countries, Polish regulation is characterised by the highest degree of axiological autonomy and commitment to values.

To understand exactly what worker dignity is, it is worth quoting the words of its architect in the context of Polish labour law – J. Jończyk, who pointed out that it concerns "a sense of self-worth based on the reputation of a competent professional and conscientious employee within the employee's close environment, and on the recognition of their contribution, abilities, skills and work by immediate and senior managers."[1096] Dignity, understood in this way, can often be violated as a result of an employer's misuse of his or her managerial powers, for example, when giving instructions to employees in an offensive manner, making erroneous assessments of employees that lead to negative consequences for them, or imposing disciplinary penalties unlawfully.[1097]

In addition to the examples of potential infringements of an employee's dignity listed above, there is one further issue which is crucial from the perspective of this thesis and which has become of immense significance in recent years. This concerns, namely, the possibility of a violation of an employee's dignity due to an infringement of their privacy[1098] resulting from the improper and disproportionate use by employers of workplace monitoring measures, a topic which has already been discussed in detail in earlier sections of this study, particularly in Chapter Two, and which is explored further in the following sections, especially in relation to technological development. Performing work, and in particular performing it properly, frequently goes beyond the strict fulfilment of tasks assigned by the employer; hence, a person's entire subjectivity is involved in the work. This, in turn, leads to an increasing likelihood of the employer interfering in the employee's private life outside the scope of the employment relationship.[1099] If we add to this the modern forms of monitoring that significantly facilitate

---

1095 Ľalík, 2019, p. 805.
1096 Jończyk, 1965, p. 135.
1097 Góral, 2016, pp. 58-59; Liszcz, 2018, p. 154.
1098 See: Liszcz, 2018, pp. 160-173.
1099 Wujczyk, 2012, Wstęp.

such interference, we can see that the dignity of the employee, in the context of workplace monitoring, requires special protection.

1.3. Protective Function of Labour Law

In the search for axiological grounds within labour law for protecting workers' dignity through ensuring respect for their privacy, which is coming under increasing pressure to be infringed, the focus should turn to the protective function of labour law.

The protective function of labour law, alongside its organisational function, which involves ensuring the smooth organisation of work by defining management powers and employees' duties, as well as measures to prevent breaches of these, is the fundamental function of labour law.[1100] This function is emphasised in the labour law literature of all Visegrad Group countries[1101] and, in its traditional interpretation, involves counteracting the exploitation of the actual market imbalance between the parties to an employment relationship to impose socially unacceptable terms of employment on employees, and guaranteeing employees' rights which they would not have been able to negotiate on their own when concluding an individual employment contract.[1102] In other words, it can be said that the protective function serves the need to protect the employee as the weaker party in the employment relationship,[1103] whilst also providing the rationale for the emergence of labour as a distinct branch of law.[1104]

When considering the protective function from a historical perspective, it should be noted that it has gone through various stages, during which it has at one time dominated and at other times been overshadowed by the organisational function. The sinusoidal nature of the role played by the protective function in the development of labour law has been and continues to be influenced by factors such as a country's level of economic growth, its social structure, its

[1100] Szubert, 1971, p. 567.
[1101] Poland - See: Szubert, 1971, pp. 567-583; Zieliński, 1986, pp. 37-40; Jończyk, 1995, pp. 25-27; Pisarczyk, 2010, pp. 15-45; Slovakia - See: Barancová, 2019, pp.41-42; Barancová, 2020, pp. 47-60; Dolobáč, 2022, p. 41; Zofcinova, 2015, pp. 45-53; The Czech Republic - See: Štefko and Pichrt, 2015, p. 41; Štefko, 2022, pp. 135-162; Hungary - See: Jakab, 2022, pp. 205-226; Gyulavári, 2014a, pp. 82-103.
[1102] Skąpski, 2006, 2.3. Tradycyjna typologia funkcji prawa pracy.
[1103] Kahn-Freund wrote that "[t]he main object of labour law has always been, and we venture to say will always be, to be a countervailing force to counteract the inequality of bargaining power which is inherent and must be inherent in the employment relationship. Most of what we call protective legislation—legislation on the employment of women, children and young persons, on safety in mines, factories, and offices, on payment of wages in cash, on guarantee payments, on race or sex discrimination, on unfair dismissal, and indeed most labour legislation altogether— must be seen in this context. It is an attempt to infuse law into a relation of command and subordination." - Kahn-Freund, 1983, p. 18; see also: Zieliński, 1986, p. 39; Jakab, 2022, p. 2009.
[1104] Pisarczyk, 2010, p. 19.

economic policy model, the specific conditions and needs of a given period,[1105] and, in recent years, the rapid acceleration of technological development, which has a direct impact on the labour market.

It seems that we are currently experiencing a period in which the protective function of labour law is perceived by many as something problematic, outdated, as it hinders economic growth and restricts the freedom of the parties to an employment relationship to determine the terms of employment on their own. Industry 4.0 (current stage of global economic development) is characterised by a distinctive deconstruction of the world of work. This is reflected in a significant loosening of working arrangements compared to previous times. Remote working and platform work have now become virtually common forms of performing work. Many new forms of work fall outside the traditional framework of an employment relationship. This, combined with the phenomena of advanced employee monitoring and new management mechanisms such as automated or algorithmic management, results in a significant reduction in the protection afforded to people performing work.[1106] It is also significant that, against the backdrop of these changes, the so-called "flexicurity" strategy has emerged, the aim of which is to simultaneously strengthen flexibility and security for the benefit of both parties to the employment relationship.[1107] In practice, however, the concept of flexicurity is often used to loosen labour regulations, overlooking the need to provide employees with adequate protection.[1108]

Following the view expressed by Szubert, it should be argued that in challenging situations, which, on the one hand, may involve the country facing economic difficulties, but on the other, increased pressure on employees resulting from rapid economic development, labour law norms aimed at protecting the dignity of the employee should not lose their significance; on the contrary they should become even more important and gain greater recognition.[1109]

Labour law is characterised by a particularly dynamic nature, involving the adoption of new legal solutions and, until recently, the expansion of its scope of application. This dynamism stems from the fact that labour law is deeply rooted in socio-economic conditions that are subject to constant change.[1110] Consequently, it can be said that labour law does not "exist" but is constantly "becoming".[1111] This characteristic enables it to respond rapidly to emerging

---

[1105] Szubert, 1971, p. 568.
[1106] Ter Haar, 2025, pp. 48-49.
[1107] Council of the European Union, 2008, Report of the Mission for Flexicurity, 17047/1/08 REV 1, p. 3.
[1108] See more in: Barański, 2022b, pp. 9-29.
[1109] Szubert, 1971, p. 571.
[1110] Zieliński, 1986, pp. 34-35.
[1111] Szubert, 1972, p. 44.

challenges, but it must be borne in mind that any change taking place in the labour market and the associated amendment of labour law must be considered in terms of its impact on the primary objective of labour law, which is the protection of the employee.[1112]

Just as labour law has in the past succeeded in liberating itself from the constraints of private law, responding to the needs of wage earners,[1113] today, in an increasingly digital world, labour law must seek new ways to safeguard the dignity of workers.[1114] To achieve this, it is essential to consider the dignity of the worker as the axiological foundation of labour law within the context of the 21st-century labour market, and in particular the challenges posed by the development of new technologies,[1115] as this thesis illustrates in detail by examining the relationship between an employee's right to privacy and forms of workplace monitoring.

In concluding this section, it must be clearly stated that only work which takes into account and respects the dignity of the person performing it can contribute to the building of the power of the state and the nation;[1116] for, as John Paul II pointed out, "although it is true that man is destined and called to work, work is nevertheless "for man", and not man "for work""[1117]. Analysing the current state of affairs, it seems that, in many cases, pure economic profit has overshadowed the significance of this maxim and, instead of seeing a human being in the employee, many employers (particularly international corporations) view him or her as a collection of data, a tool for work that can be subjected to constant monitoring and pressure to increase efficiency.

2. Subordination to the Employer vs Subordination to the Monitoring System – Growth of Technological Subordination in the Work Process

2.1. Subordination as a Fundamental Feature Defining the Employment Relationship in the Visegrad Group Countries

The performance of dependent work by an employee, i.e. work in which there is a relation of subordination between the employee and the employer, is a fundamental feature of the employment relationship in all Visegrad Group countries. The concept of subordination is most

[1112] Pisarczyk, 2010, p. 20.
[1113] Zieliński, 1986, p. 35.
[1114] An example of this kind of search is the innovative work written by Michał Barański: Barański, 2022c, pp. 85-93.
[1115] Mitrus, 2014, p. 141.
[1116] Musiała, 2019, pp. 97-98.
[1117] Pope John Paul II, 1981, para. 6, p. 23.

often analysed in terms of distinguishing between work performed within the framework of an employment relationship and work performed within the framework of other legal relationships (most often civil law contracts). However, subordination is also important regarding the issue of monitoring in the workplace, as it can be argued that it is this feature of the employment relationship that gives rise to the employer's control powers. Therefore, the following part of the thesis will be devoted to the analysis of subordination in this context, and more specifically to considerations of how the traditional concept of subordination is being transformed by technological changes in the workplace and what role workplace monitoring plays within these changes.

With regard to Polish labour law, the element of subordination stems from Article 22 of the Labour Code, which states that "by establishing an employment relationship, the employee undertakes to perform work of a specific type for the employer and under the employer's direction, at a place and time designated by the employer, and the employer undertakes to employ the employee in return for remuneration."[1118] In the case of the Czech Republic and Slovakia, employee subordination derives from the concept of *závislá práca* (dependent work), which is indicated in Section 2 (1) and (2) of the Czech Labour Code[1119] and Section 1 (2) of the Slovak Labour Code[1120]. In turn, the Hungarian legislator in Section 42 (2) (a) of the Labour Code explicitly referred to the essence of subordination, stating that within the framework of the employment relationship, the employee is obliged to perform work under the direction of the employer.[1121]

The laconic nature of the above regulations concerning employee subordination has resulted in the development of this concept primarily in the doctrine and case law of the Visegrad Group countries.

In one of its landmark rulings concerning subordination in employment relationships, the Polish Supreme Court indicated that subordination is a structural feature of an employment relationship, and in order to determine whether this feature is present within a given legal relationship, attention should be paid to elements such as: specified working hours and place of

[1118] Article 22 §1 of Act of 26 June 1974 Dz.U. 2025.277 Labour Code (Polish Labour Code).
[1119] (1) "Dependent work" ("*závislá práca*") means work that is carried out within the relationship of the employer's superiority and his or her employee's subordination in the employer's name and according to the employer's instructions (orders) and that is performed in person by the employee for his employer. (2) Dependent work is performed for wage, salary or other remuneration for work done, at the employer's cost and liability, at the employer's workplace or some other agreed place within the working hours. – Section 2 (1) and (2) of the Czech Labour Code [LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce"].
[1120] Dependent work is work performed in a relationship of superiority of the employer and subordination of the employee, personally by the employee for the employer, according to the employer's instructions, on his or her behalf. – Section 1 (2) of the Slovak Labour Code.
[1121] Section 42 (2) (a) of the Hungarian Labour Code.

work; signing an attendance sheet, the employee's subordination to work regulations and management instructions regarding the place, time, and manner of performing work, and the obligation to comply with work standards; the obligation to follow the instructions of supervisors; shift work and constant availability; precise determination of the place and time of performing the assigned task and performing it under the supervision of a manager.[1122] With this ruling, the Supreme Court emphasised the importance of subordination, giving it the status of a key feature determining the employment relationship, and, in a sense, defined it by designating the elements used to identify it.

However, in order to touch upon the essence of subordination and define what subordination itself is, which is crucial for the subsequent analysis of changes affecting the understanding of this concept, it is necessary to refer to the considerations found in the literature, according to which subordination means, on the one hand, the employer's authority to issue directions and instructions regarding the performance of work by the employee (the so-called directive authority of a supervisor)[1123], and on the other hand, the employee's obligation to comply with the instructions of their supervisor and to behave in accordance with certain organisational and legal discipline prevailing in the workplace.[1124]

Considerable attention is attached to the criteria for classifying a legal relationship as an employment relationship, which essentially constitute the characteristic of subordination, in Hungarian labour law doctrine. This is primarily due to the fact that in 2005, based on court practice, the Ministry of Labour and the Ministry of Finance issued a guidelines decree on the legal classification criteria for employment relationships.[1125] The guidelines have not been legally binding since 2011, but they have been permanently incorporated into Hungarian labour law doctrine and labour law case law.[1126] In accordance with the guidelines, the classification criteria can be divided into two groups: primary criteria, which in themselves can determine whether an employment relationship exists, and secondary criteria, which are not necessarily decisive in themselves and can often only be used in conjunction with other criteria indicating the existence of an employment relationship in order to classify a legal relationship as an employment relationship.

The group of primary criteria includes:

[1122] Judgment of the Polish Supreme Court of 25 November 2005, I UK 68/05.
[1123] Jończyk, 1995, p. 121.
[1124] Ćwiertniak, 2016, p. 122; Barański, 2022d, p. 165.
[1125] 7001/2005. (MK 170.) FMM-PM együttes irányelv a munkavégzés alapjául szolgáló szerződések minősítése során figyelembe veendő szempontokról.
[1126] Gyulavári, 2024, p. 933. See also: Gyulavári, 2019, p. 33; Kun, 2021, p. 53.

- the nature of the activity, the definition of tasks as job duties;
- personal obligation to perform work;
- obligation of the employer to employ and of the employee to be available;
- subordinate-superior relationship between employee and employer.

The group of secondary criteria includes:

- employer’s right to manage, give instructions, and monitor;
- employer’s right to determine the duration of work and the work schedule
- the place of work
- remuneration for work performed
- use of the employer's work equipment, resources, and raw materials;
- ensuring safe working conditions that do not pose a health hazard;
- written form of an employment contract.

Nevertheless, this distinction of criteria for classifying a given legal relationship as an employment relationship has been severely criticised in legal doctrine. It is pointed out that the division into primary and secondary criteria is erroneous, as the guidelines themselves refer to the need for a comprehensive assessment of the circumstances under which a given legal relationship is established. Therefore, it would be more appropriate to refer to the characteristics of the relationship that require a more thorough assessment and those for which a more superficial assessment is sufficient. It should also be noted that individual characteristics are closely related to each other, which means that, for example, separating the characteristic of subordination (primary group) and the employer's right to give instructions (secondary group) is completely unjustified.[1127]

Furthermore, Gyulavári points out that subordination is a central feature of the employment relationship and has many aspects that together constitute it. Therefore, dividing these aspects according to the criteria of significance should be considered a misguided approach that leads to a misunderstanding of the concept of subordination.[1128]

It is thus apparent that subordination within the meaning of the Hungarian labour law system is similar to that found in the Polish labour law system. In both countries, it is a fundamental feature of the employment relationship[1129] and includes many designations that may be subject to individual assessment, but ultimately lead to one goal: determining whether subordination

[1127] Bankó, 2008, p. 211.
[1128] Gyulavári, 2014b, p. 128.
[1129] As indicated in Hungarian legal literature, economic and organisational subordination has been the dogmatic foundation of labour relations within the Hungarian labour law system for over a hundred years. – See: Sipka and Zaccaria 2019, p. 52.

existed in a given legal relationship under which the work was performed and, if so, to what extent.

However, to grasp the essence of subordination as it is understood in Hungary, we must refer to the employer's unilateral right to control and issue instructions to the employee throughout the entire work process, who must perform his or her work in accordance with these instructions.

“The employer is the master who gives orders, while the employee serves. The latter places his raw labour power at the disposal of the former, along with his entire working time, so that, since the overwhelming majority of workers have no property of their own, they depend on the employer for their livelihood and that of their families, and as a result, they become strongly dependent on him."[1130]

The above quotation comes from old Hungarian literature on labour law and can certainly be criticised for its oversimplification (especially from today's perspective) and certain ideological influences characteristic of the labour laws of the so-called socialist bloc countries. However, it cannot be denied that it captures the specific nature of the relationship of subordination very well. Moreover, this quotation is particularly valuable because it gives subordination a historical dimension, indicating that this feature has been part of human labour for centuries.

With regard to the Czech Republic and Slovakia, the concept of subordination does not vary significantly between these countries and does not differ substantially from that expressed in the Polish and Hungarian labour law systems.

Štefko points out that subordination, or more precisely the concept of dependent work, is a central element of Czech labour law, determining its character. According to the author, the labour law consists of regulations covering the legal relationship between the employer (in the old terminology “master”) and employee (in the old terminology “servant”). What really lies at the heart of an employment relationship is the sale of an employee’s labour to his or her employer.[1131][1132] In turn, Zafcinova states that the principle of subordination (understood as an

[1130] Tóth, 1956, p. 222.
[1131] Štefko, 2022, p. 136.
[1132] This position taken by Stefko, as well as the above-mentioned quote from Hungarian literature on labour law from the 1950s (and the fact that it is also present in contemporary literature, see: Gyulavári, 2019, p. 34) indicate that, in fact, the perception of work has not changed for centuries, which is a certain implication of feudal times and the early period of industrial capitalism. Many legal scholars do not want to engage in such considerations, believing that their work should not take on a philosophical or even political character, thus departing from the field of legal analysis. However, it should be noted that such a perception of the relationship between the parties to an employment relationship, and above all the use of the terms “master” and “servant” in relation to the parties

employer's superiority and employee's subordination) should be considered as a fundamental principle of the employment relationship in Slovakia, setting it apart from other legal relations.[1133] The dominant position of subordination results in a lack of factual equality between the parties to the employment relationship.[1134] Barancová rightly draws attention to another implication of subordination, namely, the economic dependence of the employee, which means that the employee is able to satisfy his or her basic material needs by means of the remuneration received for his or her work.[1135]

In view of the above, it should be noted that the understanding of the principle of subordination is consistent across all Visegrad Group countries. It is a fundamental feature determining the classification of a given legal relationship within which work is performed as an employment relationship defined in the labour codes of the V4 countries, and can be illustrated by a dependency in which the employer is entitled to issue instructions to the employee and control the entire work process, and the employee is obliged to comply with such instructions and perform his or her work tasks with due diligence. Nevertheless, the principle of subordination is constantly evolving, adapting to changes in the modern labour market – the emergence of new forms of work, the emphasis on employee flexibility and increasingly advanced monitoring technologies.

2.2. The Evolution of the Concept of Employee Subordination

The origins of the above understanding of subordination as a strict dependency of the employee on the employer, primarily in terms of the tasks assigned to them and the type and manner of work performed, can be traced back to the so-called factory model of labour relations. The features of this model were evident (and to some extent still are) both in Western Europe, where at least until the late 1960s the dominant model of production was the so-called Fordist

---

to this relationship, certainly has a significant impact on the social subconscious, which in turn translates into the appropriate shaping of legal regulations, and, above all, which is extremely important in the context of workplace monitoring, on the development of new technologies, whose mechanisms of operation may continue to perpetuate the role of master and servant in the workplace. Many will point out that this is what capitalism is all about, as it is based on inequality resulting from the fact of possessing or not possessing capital, and they are right. However, did the system known as "real socialism" (name used in the Polish People's Republic), which prevailed in Central and Eastern Europe for over four decades, succeed in eliminating the master-servant relationship in labour relations? As the experience of the V4 countries shows, it did not. Therefore, it should rather be pointed out that the current relationship between employer and employee is an inherent feature of any economic system based on purely material premises. Only a system that would place the human being, or, referring to a more local perspective, the nation, at the centre, going beyond pure economism, could eliminate such an unequal relationship.

[1133] Zofcinova, 2015, p. 49.

[1134] Zofcinova, 2015, p. 49; Barancová, 2019, p. 35.

[1135] Barancová, 2019, p. 35.

model,[1136] and in most Central and Eastern European countries (including the V4 countries), where until the end of the 1980s a centrally planned economy prevailed[1137]. These models were based on mass production and large enterprises, where tasks were strictly divided, and there was a clearly defined hierarchy based on the surveillance of the workforce.[1138]

Nevertheless, at the end of the last and beginning of this century, these models of work organisation began to lose their significance and undergo transformation. As Supiot points out in his report, this change is primarily due to three key factors: 1. increased work specialisation, 2. the development of competence in the open market, and 3. rapid technological development.[1139] Such changes have twofold effects. On the one hand, the development of new forms of work, such as remote work and platform work, and the growing demand for creative and managerial professionals have resulted in increased employee autonomy, which in turn has translated into a need to broaden the concept of subordination so that an increasingly wider range of people performing work can be included within the realm of employment relationship. This trend has been expressed in the concept of "autonomous subordination" (present primarily in Poland) or in the concept of "economic dependence," which has similar effects (discussed in other Visegrad Group countries, especially Hungary). On the other hand, however, especially in recent times, technological developments in the field of employment have enabled employers to increasingly interfere in the private lives of employees and subject them to extensive control, which in turn might be demonstrated in the concept of technological subordination[1140].[1141]

2.3. Broadening the Concept of Subordination

The response to the emergence of new forms of work and the expansion of the catalogue of legal relationships within which work is currently performed is the concept of autonomous subordination, promoted primarily by a part of Polish labour law doctrine[1142] and jurisprudence of the Supreme Court[1143]. The fact that this concept sprouted in Poland does not mean that it cannot be applied in other Visegrad Group countries, since they share a very similar

[1136] Markantonatou, 2007, pp. 119-129.
[1137] Musiała, 2009, p. 128.
[1138] Supiot, 1999, p. 33.
[1139] Supiot, 1999, p. 34.
[1140] Bąba, 2022, pp. 88-109.
[1141] Barański and Gredka-Ligarska, 2025, p. 21-22.
[1142] Bury, 2006, pp. 57-68.
[1143] Judgments of the Polish Supreme Court: of 7 September 1999, I PKN 277/99; of 7 March 2006, I PK 146/05; of 13 April 2016, II PK 81/15; of 22 September 2020, I PK 126/19.

understanding of subordination in the "classical" sense, and the changes taking place in the labour markets of the V4 countries are comparable.

In this context, it should be noted that the Polish Supreme Court has established a long-standing line of case law on the issue of autonomous subordination. Within this line of jurisprudence, there are slight differences in the interpretation of the concept of autonomous subordination, but its main assumptions, which tend towards the application of this concept as a result of changes in workplace management, remain the same.

The first and therefore groundbreaking judgment of the Supreme Court expressing the concept of autonomous subordination is the ruling of 7 September 1999, I PKN 277/99. Emphasising the importance of the changes taking place in social relations, the Supreme Court pointed out that "the old system of strict hierarchical subordination of the employee and the obligation to comply with the employer's instructions, even in technical matters, is being replaced by a new system of autonomous subordination, whereby the employer assigns tasks to the employee without interfering in the manner in which those tasks are performed. In the new system of subordination, the employer determines the working hours and assigns tasks, while the manner in which these tasks are performed is left to the employee." As an example of a group of employees for whom autonomous subordination is a typical feature, the Court referred to employees performing so-called creative professions. In such professions, employees must be given sufficient leeway by their employer as to how they perform the tasks assigned to them within the framework of their employment relationship.[1144] In its subsequent ruling, the Supreme Court extended the concept of autonomous subordination to include persons holding independent managerial positions. In justifying its position, it pointed out that such persons perform work of a specific nature and that the characteristics of subordination in the traditional sense would not apply to such employees. Employees in managerial positions do not usually have direct superiors who monitor their work and give them instructions. As a rule, they organise their own time, place of work and manner of performing tasks which were generally entrusted to them.[1145] Following the Supreme Court's line of jurisprudence, it is apparent that the Court is repeatedly extending the concept of autonomous subordination to ever wider groups of persons performing work. In its judgment of 13 April 2016, II PK 81/15, the Supreme Court stated that there is currently a visible tendency to "loosen" the rigour of employer management in relation to particular groups of employees or due to the type of work performed. According to the court, for a number of jobs, employers may specify working hours and general tasks, but

[1144] Judgment of the Polish Supreme Court of 7 September 1999, I PKN 277/99.
[1145] Judgment of the Polish Supreme Court of 7 March 2006, I PK 146/05.

the manner in which they are performed is up to the employees themselves. This type of work certainly includes creative and managerial work, which has already been mentioned in previously mentioned Supreme Court rulings. However, the Court does not stop at repeating its already established position, but points out that also in relation to persons performing work on task-based working time, tele-employees/remote-employees and mobile-employees, the permanent issuance of instructions by employers is rather illusory. However, the court points out that greater autonomy for employees does not mean that they are exempt from the obligation to respect the established rules of the organisation and functioning of the workplace. Furthermore, employees performing work within the framework of autonomous subordination will be held accountable for their independent decisions according to stricter rules than employees performing work in a traditional subordination relationship.[1146] Among the Supreme Court rulings that constitute the line of jurisprudence on autonomous subordination, one more Supreme Court ruling of 22 September 2020, I PK 126/19, should be mentioned. In this judgment, the Court made an extremely important observation with implications for the possibility of monitoring employees performing work under autonomous subordination. It pointed out that such employees organise their work themselves and, what is important, are not under the permanent and direct supervision of a person acting on behalf of the employer.[1147][1148] It follows from the above that the possibilities for monitoring such employees are extremely limited and will rather be reduced to periodic checks carried out ex post after the completion or failure to complete a specific task.

When analysing the above case law, it should certainly be considered commendable that, as a result of the loosening of the concept of subordination, from the side of the Supreme Court there is a desire to cover a larger number of people performing work with an employment relationship, which objectively provides the best protection for the interests of employees among all legal relationships within the framework of which it is possible to perform work. It can even be said that this line of jurisprudence has breathed life into demands that emerged in the interwar period for the complete abandonment of subordination as a distinguishing feature of an employment relationship.[1149]

Nevertheless, a closer look at the effects of the Supreme Court's application of the concept of autonomous subordination leads to the need for a critical assessment of them. A broad

---

[1146] Judgment of the Polish Supreme Court of 13 April 2016, II PK 81/15.
[1147] Judgment of the Polish Supreme Court of 22 September 2020, I PK 126/19.
[1148] This position was confirmed in a recent ruling of the Polish Supreme Court of 12 May 2025, I PSK 132/24.
[1149] See: Duraj, 2015, pp. 164-165.

interpretation of subordination may lead to the classification of any legal relationship in which work is performed for someone else as an employment relationship. A characteristic example of this result arising from the above case law is the classification of persons in managerial positions as employees performing their work under an employment relationship. However, it should be borne in mind that managerial positions are very often characterised by a high position in the workplace hierarchy, the absence of direct superiors, a high degree of autonomy and high pay. These factors significantly distinguish managerial positions from positions that are "under management." However, it should be remembered that the essence of the employment relationship is the protection of the weaker party, expressed in the protective function of labour law.[1150] Considering the differences between high-level employees performing managerial functions (who may even be members of the management boards of commercial companies) and employees working, for example, on the production line, it becomes obvious that equalising their situations, and consequently also equalising their level of protection, would lead to a serious blurring of the essence of the employment relationship.[1151] Nevertheless, this "equalisation" not only contradicts the axiological foundations of labour law, but also has significant practical consequences, manifested in the distinction between the situation of employees performing work within the framework of classic subordination and those performing work within the framework of autonomous subordination, to the detriment of the former. Such practical consequences are clearly visible in relation to the issue of employee monitoring. As already indicated above in the example of the Polish Supreme Court judgment of 22 September 2020, I PK 126/19, the concept of autonomous subordination significantly limits the possibility of monitoring employees covered by its scope. Therefore, it should be recognised that persons performing managerial functions will be exempt from at least certain forms of monitoring. However, the situation will be completely different in the case of, for example, employees performing simple physical work, because, as the court pointed out, under no circumstances do such persons perform their work within the framework of autonomous subordination, but are covered by so-called classic subordination.[1152] It should therefore be concluded that such employees may be subject to comprehensive monitoring, obviously within the limits set by the Labour Code. This leads to an absurd situation in which an employee who has no autonomy in the work process is pushed into an even more difficult position in relation to the manager of the workplace. Such a distinction between two categories of employees,

[1150] Matuszak, 2023, p. 100.
[1151] Musiała, A. 2009, p. 130.
[1152] Judgment of the Polish Supreme Court of 22 September 2020, I PK 126/19.

whose legal situation should theoretically be the same, is extremely harmful, unjustified, and contrary to the provisions on monitoring in the workplace, which indicate specific premises as the basis for the possibility of applying particular forms of monitoring, rather than the characteristics of specific work or categories of employees.

In other Visegrad Group countries, there is also a visible trend towards expanding or even replacing employee subordination in the classical sense with other categories, and the rationales for this are similar to those apparent in Poland.[1153] Nevertheless, the doctrine does not accept this phenomenon without criticism.

Gyulavári rightly points out that a broader interpretation of subordination in employment relationships leads to the protection of employment also covering employees with a high degree of independence, e.g. managers, while many employees in difficult situations lose the protection of labour law because they are temporary workers or forced to work on the basis of a fictitious civil law contract.[1154][1155] This situation reflects the paradox that arises when the concept of subordination is loosened.

The proposed solution to this highly contradictory situation is to replace the concept of subordination with that of economic dependence[1156].[1157] The shift from subordination to economic dependence is potentially closer to the objective of labour law, as it serves to protect those in a weaker position.[1158] However, looking at the definition of economic dependence proposed by Wank, according to which an economically dependent person is someone who works only for one party to the contract, without the help of other persons and without own capital or own organisation,[1159] the convergence of this concept with the indicated objective of labour law is not apparent. Only when considering the meaning of economic dependence as indicated by Casale, who states that economic dependence exists if the amounts received by the employee constitute his sole or main source of income, if these amounts are paid by a person

[1153] Authors from different V4 countries draw attention to the growing demand for managerial, creative, remote workers and, in general, those whose work is based on performing a specific task without specifying in detail how it should be done – See: Štefko and Pichrt, 2015, p. 50; Dolobáč, 2022, p. 40; Barancová, 2019, p. 35; Nádas, Rab, Sipka, Zaccaria, 2018, p. 19; Gyulavári, 2014b, pp. 157-160.
[1154] Gyulavári, 2014b, p. 159.
[1155] An example of the exclusion of an employee in a weaker position can be found in the judgment of the Hungarian Supreme Court (Kúria/Curia) of December 13, 2023, Mfv.VIII.10.091/2023/7, which stated that a platform worker did not perform his work under an employment relationship but was self-employed, as there was no relationship of subordination to the employer in this case. Gyulavári severely criticised this decision, pointing out that the classic control/subordination test is extremely difficult to pass in the case of platform work, as it is characterised by a completely different relationship between the worker and the platform than the traditional employment - See: Gyulavári, 2024, pp. 936-938.
[1156] More on economic dependence, see: Razzolini, 2010, pp. 267-301.
[1157] Gyulavári, 2014, pp. 159; Nádas, Rab, Sipka, Zaccaria, 2018, p. 19.
[1158] Gyulavári, 2014, pp. 159.
[1159] Wank, 2004, p. 140

or company as a result of the employee's activities, and if the employee does not enjoy economic autonomy and is economically linked to the sphere of activity in which the person or company that can be considered the employer operates,[1160] it can be concluded that the concept of economic dependence actually contributes to the protection of employees in a weaker position. A very similar understanding of economic dependence is presented by Barancová, who points out that this concept is manifested in the fact that an employee secures the basic material conditions for his or her livelihood through remuneration received from the employer.[1161] However, it should be noted that, unlike in the Czech Republic and Hungary, the Slovak legislator, when defining the concept of dependent work, refrained from directly indicating the prerequisite of remuneration for the work performed. Therefore, some authors point out that although economic dependence is an important prerequisite for the existence of an employment relationship, it is not mentioned anywhere in Slovak labour law and thus is not of great significance at this point.[1162] However, this position is not entirely consistent with the actual state of Slovak labour law, as the obligation of payment for work, which is, in a sense, the foundation of economic dependence, stems from Sections 129 and 130 of the Slovak Labour Code.[1163]

Returning to the essence of the definition of economic dependence given above, it should be noted that, on the other hand, it is possible to imagine a situation in which an employee performing a specific job in a manner that leaves no doubt that it is performed within the framework of an employment relationship will have additional sources of income that may even exceed his or her salary resulting from the employment relationship. Depriving such an employee of the protection afforded by labour law on the grounds that, according to the above definition, he or she is not economically dependent on the employer does not seem to be a fair solution. Therefore, it should be noted that when determining the existence of an employment relationship, it is impossible to completely disregard the concept of subordination and the related manner and type of work performed.

[1160] Casale, 2011, p. 26.
[1161] Barancová, 2019, p. 35.
[1162] Schronk, 2017, p. 636.
[1163] Sections 129 and 130 of the Slovak Labour Code.

2.4. Technological Subordination – Return to Strict Monitoring

As previously indicated, the other side of current technological changes is the growing dependence of employees, theoretically on employers, but in practice on the authority resulting from specific technological solutions – algorithms - which are increasingly used in the workplace to streamline management processes. This phenomenon is called technological subordination and is permanently linked to algorithmic management. Therefore, in order to fully understand what technological subordination is, we must first indicate the meaning of algorithmic management.

Algorithmic management involves combining algorithms, understood as computer-programmed procedures that transform input data into desired outputs,[1164] with appropriate technologies that enable the collection of data about employees and use it to automate or at least support workplace coordination functions that were previously performed by human managers.[1165] According to another, but similar definition, the concept of algorithmic management includes organisational practices that are performed entirely or partially without human intervention, among other things, through the application of mathematical formulas.[1166] Algorithmic management methods are designed to guide companies in an effective manner based on data analysis and represent new evidence-based human resource management practices that can be summed up as "*boss ex machina*."[1167] In other words, it can be said that algorithmic management is slowly taking over tasks that were previously performed by our traditional human bosses.[1168]

However, regardless of the definition of algorithmic management, it is essential to consider what changes, apart from taking over tasks previously performed by managers, are associated with this phenomenon in relation to traditional forms of management. At this point, we can identify three areas related to employment that are most affected by the algorithmic innovations: direction (entailing what needs to be done, in what order, what time and with what degree of accuracy); evaluation (entailing the review of workers to correct mistakes, assess performance and identify those who are not performing properly); discipline (entailing the punishment and reward of workers to elicit cooperation and enforce compliance with the direction of the

[1164] Kellogg, Valentine, Christin, 2020, p. 366.
[1165] Baiocco, Fernandez-Macías, Rani, Pesole, 2022, p. 8.
[1166] Bodie, Cherry, McCormic, Tang, 2016, pp. 1-79.
[1167] Aloisi and De Stefano, 2022, p. 59.
[1168] See: Kessler, S. 2022; Aloisi and De Stefano, 2022, p. 58.

labour).[1169][1170] At the heart of the algorithms used in the above areas is innovative algorithmic data analytics, whose distinguishing features are ubiquity and interoperability. This means that modern algorithmic systems are capable of processing information from an extremely wide and increasingly diverse set of information technologies, which allows access to very detailed employee data (such information technologies include increasingly advanced forms of workplace monitoring such as cameras, GPS, computer and mobile device monitoring, voice tone detection, wearables, bossware but also other related technologies - big data analysis and machine learning). Modern data processing systems are also interoperable, which means that they combine data sets to obtain new information about employees, which would not be possible if the analysed sets of data were separate.[1171]

In order to briefly outline how algorithms work within the employment sphere in practice and illustrate what technological subordination actually is and why monitoring is its focal point, we must first refer to the issue of direction.

When it comes to directing employees, algorithms aim to automate this process as much as possible. This is particularly evident in the example of platform work, as platforms in fact shape working conditions – they convert a customer's demands into a specific work process, define the tasks and payment for them, coordinate task allocation (assign them to employees via mobile devices and computers) and also organise quality control and communication channels.[1172] As an example of such algorithmic action, we can look at food delivery platforms, where workers/employees are provided with automated instructions regarding their work via mobile devices. As Ivanova, Bronowicka, Kocher, and Degner point out in their studies on food delivery platforms in Berlin, with an automatic data collection system, platforms can monitor couriers in real time, so if the algorithm detects any deviation from the norm, the employee immediately gets a notification in the app. For example, in the case of Deliveroo, couriers receive a notification if the geolocation on their phones detects that they are not moving, while Foodora delivery drivers, when their delivery time exceeds the average, are asked by the app to

[1169] Kellogg, Valentine, Christin, 2020, pp. 367-369.
[1170] This division resonates strongly with Bąba's position, which draws attention to the disciplinary and regulatory aspects of algorithmic authority. Disciplinary mechanisms of authority concern employees, organising their work in terms of time, place, and pace. Regulatory mechanisms of authority, on the other hand, concern employees viewed from a collective perspective. Both are linked by productivity, which can be applied both to individual employees, who are subject to constant discipline, and to the collective of employees, which the employer regulates (organises) - See: Bąba, 2022, p. 104.
[1171] Otto, M. 2022, p. 146.
[1172] Gerber and Krzywdziński, 2019, pp. 122-124.

end the order or contact their dispatcher. Riders also receive notifications to return to the centre of a given zone to receive a new order.[1173]

However, algorithmic direction is not limited only to platform work, but also extends to more conventional workplaces, where it has an even more severe impact on employees.

As Rozmysłowicz and Krzyżaniak point out in their studies on automatic processing of work performance data and employee evaluation at Amazon's POZ1 warehouse in Poznań, Poland, work in such a warehouse mainly boils down to continuously scanning various types of barcodes when something is placed, removed from the rack, sorted, or unpacked. However, barcodes are not only found on products in the warehouse, but also on their locations on shelves, transport containers, individual employee workstations, and on the employees themselves. Scanning these codes provides the algorithmic system with data that enables it to determine the production quotas that employees should adhere to, while also providing insight into the employee's location in the workplace, breaks, and work pace.[1174] Going beyond warehouse work, there has been a growing trend in the United States for Amazon to install AI-equipped cameras (called Driveri) in company-branded trucks used by external partners to deliver goods to customers. The cameras record 100% of the time when the driver is on the road, and their lenses are directed at the cab, the road ahead and both sides of the vehicle. The company cites safety concerns as justification for using such a system - AI-equipped cameras focus on 16 other road safety issues, including when a driver fails to stop at a stop sign, drives too fast, brakes too hard, does not wear a seatbelt, and even when they yawn. In a situation that the system deems dangerous, an alarm is sounded to remind the employee to obey traffic signs, reduce speeding, or take a break.[1175]

Finally, a prime example of the directive activity of algorithms is bossware, which can be broadly defined as software that enables employers to intensively monitor their employees (through tracking mouse movements, keystrokes, online activity, open applications, etc.).[1176] This type of software is most often used to confirm employee attendance, working hours and productivity.[1177] Moreover, employers are increasingly using so-called automatic schedulers - programmes that automatically assign work schedules to employees by compiling information about the workforce, customer demand and business traffic.[1178] One such programme is Kronos,

1173 Ivanova, Bronowicka, Kocher and Degner, 2018, pp. 12-13.
1174 Rozmysłowicz and Krzyżaniak, 2023, p. 152.
1175 Palmer, A. 2021.
1176 Munn, 2024, p. 105.
1177 Czerniak-Swędzioł, 2025, p. 156.
1178 Wood, 2021, p. 4.

advertised by its creators with the slogan "empower your frontline and optimize every shift with people-first AI and real-time insights. Plan smarter, schedule faster, and lead with confidence."[1179] After analysing how Kronos works, Van Oort concluded that the programme primarily affects the assignment of short shifts to employees and high variability in work schedules.[1180] In 2013, after less than two weeks of using the Kronos system, hundreds of employees at the American clothing chain store Forever 21 were notified that their full-time positions had been converted to part-time and that they would lose their health benefits.[1181] This situation of workforce optimisation vividly illustrates the phenomenon of labour entropy resulting from algorithmic authority. Algorithms ensure that employment itself can continue despite the accompanying constant redundancies and the fragmentation of work into temporary legal relationships.[1182] One more consequence of the application of automatic schedulers or broadly understood bossware is the increasing tendency towards automatic monitoring of the workforce, which is a key effect from the point of view of this thesis –

"In settings where the employee base changes as quickly as the store inventory, the propensity to treat workers like potential criminals becomes amplified. Biometric fingerprinting purports to provide objective time keeping for today's "modern" (i.e. flexible) workforce by preventing time theft and buddy punching, while software that tracks and aggregates cash register transactions encourages employers to quickly pinpoint "exceptions" within a large pool of cashiers, exerting more pressure on an already stressful task."[1183]

Moving on to the analysis of employee evaluation by algorithms, one of the first assessment mechanisms that comes to the fore is the evaluation of platform workers by customers, as is the case with transport or food/shopping delivery platforms, where the customer is asked to rate the driver or delivery person. This assessment mechanism is, in a sense, a ranking of trust in the service provider.[1184] However, the assessment of workers within the platform work is not limited to customer reviews, but is also carried out by the platform itself. An example of this type of activity is the food delivery platform Foodora, which sends couriers a detailed summary of their performance once a month, taking into account the number of absences, average hours

[1179] Website of the Kronos producer: https://www.ukg.com (Accessed: 5 May 2026).
[1180] Van Oort, 2018, p. 9.
[1181] Kaplan, 2015.
[1182] Bąba, 2022, p. 101.
[1183] Van Oort, 2018, p. 9.
[1184] Bakalarz, 2019, p. 14.

worked per week, number of weekend shifts, late logins, deviations from delivery standards, as well as a general indication of how a given courier ranks in percentage terms compared to others, and encourages the courier to improve his or her performance.[1185] Going into further detail about the algorithmic evaluation of Foodora workers, it should be noted that the platform uses six weighted metrics to divide employees into different groups - those who perform better and those who perform worse at deliveries. These metrics, along with their weights, are: number of weekend shifts after 8 pm (30%), average weekly hours (25%), no-shows (25%), percentage of late logins (5%), orders hour deviation (10%), and experience working in the company (5%). In contrast, other delivery platform Deliveroo uses only two indicators within their assessment-sorting system: no-shows and late logins.[1186]

The evaluation mechanisms present in algorithmic management are also very evident in non-platform work, an example of which is Amazon's "POZ1" warehouse. At this workplace, employees are assessed in relation to two quotas: productivity quotas and quality quotas.[1187]

As regards productivity quotas, the basis on which they are determined and how such data is obtained has already been indicated in the previous section on direction. However, due to the need to outline the evaluation carried out on their basis, a few more words should be devoted to production quotas.

These quotas are set for a period of one month based on the individual performance of all warehouse employees in the previous period. In order to do this, the system calculates new productivity indicators at a specified percentile of individual work performance, ranked in ascending order. Nevertheless, not all employees can achieve the minimal threshold. The system anticipates that a certain number of the least productive employees, which the company defines as the 10th percentile, will not meet the productivity standard. The employees who achieve results at this percentile will receive a negative evaluation.[1188]

On the other hand, quality quota means "the number of errors made per one million chances of making an error." These are set by comparison of the weekly rate of errors committed by employees with historical data coming from the same warehouse department. In most cases, errors are detected by the system; however, the detection can also be made by another employee performing the function of quality control. Nevertheless, it is always the system that connects

[1185] Ivanova, Bronowicka, Kocher and Degner, 2018, p. 14.
[1186] Ivanova, Bronowicka, Kocher and Degner, 2018, p. 15.
[1187] Rozmysłowicz and Krzyżaniak, 2023, pp. 152-155.
[1188] Rozmysłowicz and Krzyżaniak, 2023, p. 153.

a specific error with an individual. Quality is presented to employees as an average value, expressed as a percentage of the target value.[1189]

Based on production and quality quotas, an employee may be assessed negatively, neutrally or positively. A negative assessment is given when an employee's performance during the working week is below 100% of the productivity indicator or below 80% of the quality indicator. An employee "deserves" a neutral rating when his or her productivity is at least 100% but no more than 120%, or when the quality of their work is at least 80% but no more than 100% of the quality benchmark. In turn, a positive assessment will be granted when the employee's productivity exceeds 120%, and quality is achieved at 100% – during the era of the Eastern Bloc, such an employee would have been called a work pioneer.[1190]

An interesting example of algorithm evaluation can also be found in call centres, as this type of work provides a lot of quantifiable data that demonstrates the efficiency and accuracy of employees. One of the tools used for this type of measurement in such workplaces is the Cogito programme. It is a programme that, on the one hand, provides managers with both live and recorded information about employee productivity and, on the other hand, gives employees real-time feedback on their work based on an analysis of their voice in conversations with customers.[1191] The second feature of the programme is a major innovation. As Roose indicates, it works in such a way that during a conversation, visual information about how the employee is doing is displayed in the bottom right corner of their computer screen – "Talking too fast? The program flashes an icon of a speedometer, indicating that he should slow down. Sound sleepy? The software displays an "energy cue," with a picture of a coffee cup. Not empathetic enough? A heart icon pops up."[1192]

The above examples of employee evaluation using algorithm-based mechanisms, which take place in both digital and more conventional enterprises, confirm Bąba's, to a certain extent, theoretical position that standards are becoming the focal point of algorithmic management of human labour. Mediocrity must be eliminated in order to extract maximum performance from employees so that, as Foucault wrote, "we can get closer to the ideal point where maximum velocity is combined with maximum efficiency"[1193].

[1189] Rozmysłowicz and Krzyżaniak, 2023, p. 154
[1190] Rozmysłowicz and Krzyżaniak, 2023, p. 154
[1191] Brione, 2020, p. 13.
[1192] Roose, 2019.
[1193] Foucault, 2020, p. 230.

The natural consequence of employee evaluation is the application of disciplinary measures if the evaluation does not go according to the employer's expectations. It is no different in the case of algorithmic management.

When it comes to food delivery platforms, disciplinary measures are embodied in the system created for riders to book shifts. On platforms such as Foodora and Deliveroo, the ability to choose specific shifts depends on which of the three categories (so-called “badges”) an employee has been assigned to based on their rating.

For example, at Foodora, the best workers are the first to be allowed to book shifts for the following week, as they have access to the full calendar from Monday; second-category workers are given the opportunity to book on Tuesday; and third-category couriers only on Wednesday. In Deliveroo, the system is similar; however, all riders are allowed to make reservations on Mondays, and their access has been divided according to the time. The best workers have access to the calendar from 11 a.m., the next group from 1 p.m., and the third category from 5 p.m. In practice, such systems result in a significant reduction, and in some cases even exclusion, of the third group of employees from employment, as they will not have access to work shifts that are convenient for them, or such access will be extremely limited.[1194]

It is also common practice for platforms such as Uber to block the accounts of drivers whose ratings, usually coming from customers, are not high enough.[1195] Nevertheless, an extremely interesting case of platforms using disciplinary measures, which clearly illustrates the threat posed by the uncontrolled development of algorithms and digital platforms,[1196] is the blocking of the accounts of Glovo workers who took part in the first Polish strike of platform workers in Białystok.[1197]

Returning to Amazon’s warehouse “POZ1” in Poland, which is practically a textbook example of how algorithmic management operates, it should be noted that the aforementioned employees’ assessments - negative, neutral and positive - have specific consequences for employees. A negative assessment has the most serious consequences, as the employee receives official printouts from the system and is asked to improve, and in some cases, is even recommended by the system for dismissal. A neutral assessment has no consequences, and in the case of a positive assessment, the employee may receive a reward, but in practice, this rarely

[1194] Ivanova, Bronowicka, Kocher and Degner, 2018, p. 15.
[1195] Rosenblat and Stark, 2016, p. 3774; Bakalarz, 2019, p. 15.
[1196] Mirosławski, 2023a, p. 7.
[1197] See more: Szymaniak, 2021.

happens. From the point of view of disciplinary measures, the most important thing is therefore a negative assessment, especially a potential recommendation for dismissal.[1198]

A recommendation for dismissal occurs when an employee has received four negative evaluations within a short period of time, as specified in the workplace policy. However, it is possible to proceed immediately to a recommendation for dismissal if an employee has received six negative evaluations within a year, and a neutral or positive evaluation between negative evaluations is irrelevant.[1199]

The use of AI-equipped cameras in Amazon's vehicles has similar consequences to those mentioned above - recordings obtained through monitoring can be used to make decisions about employees, such as whether to dismiss them. The main factor influencing specific decisions will be the detection by cameras of the dangers the driver has caused.[1200]

When considering disciplinary measures that may be applied by algorithms, Bąba points out that they create a huge asymmetry between the rights of employees and the employer's right to dismiss them, as technological power allows for dismissal at any time and permits an employee to remain in employment only until they are deemed redundant (in the case of loss of productivity as determined by the algorithm).[1201] Furthermore, algorithms only provide apparent validity for the reasons for dismissal, as in reality, algorithms are unable to comprehend them. Algorithms can mathematically calculate that something in the work process can be improved, but this does not mean that the work has been performed improperly so far. Demonstrating that an algorithm works correctly and is not mistaken does not mean anything more than that, given the right data and applying the right rules, that the algorithm has reached mathematically correct conclusions. This is what distinguishes humans from algorithms – the ability to cognitively understand reality, rather than performing simple or more complex mathematical operations.[1202]

Taking the above reflections into account, it should be noted that although many algorithms used in workplace management do not operate completely autonomously, and their potential to completely replace human managers has not yet been fully exploited, a new concept of employee subordination is already on the horizon, namely technological subordination, which replaces hierarchy with centralisation, allowing it to encompass the entire multitude of individuals in the workplace. Its main driving force is the continuous recording of data and

[1198] Rozmysłowicz and Krzyżaniak, 2023, pp. 154-155.
[1199] Rozmysłowicz and Krzyżaniak, 2023, p. 155.
[1200] Palmer, A. 2021.
[1201] Bąba, 2022, p. 99.
[1202] Bąba, 2022, pp. 96-97.

monitoring of employees, which does not require human intervention to function, as an algorithm is sufficient. Thanks to this, all human activity, skills, work methods, diligence and other behaviours can be expressed using signals, i.e. in a way that is understandable to the algorithm, but not necessarily to humans.[1203] This results in the separation of surveillance and control from legal norms and the complete incorporation of these attributes of the employer's authority into the rules of technology used to manage the workplace, along with the workforce.[1204] In other words, technological subordination means the employer's complete domination over the employee.[1205]

3. Employee Monitoring and the Humanisation of Work - Human Interactions in a World of New Technologies

The humanisation of work is an interdisciplinary concept rooted primarily in sociology and management sciences, which has found its way into legal sciences. The idea of humanisation itself can be defined as an endeavour aimed at the physical and mental development of the individual, based on the axiological values of humanism,[1206] such as the individual's right to self-realisation, respect for human dignity, and the individual's right to subjectivity and freedom.[1207] Limiting the scope of humanisation to the notion of work, it should be noted that it is intended to lead to the gradual removal of all obstacles standing in the way of transforming work into an activity that is creative and fosters personal development.[1208] On the other hand, in the field of labour law, it is argued that the humanisation of modern labour relations is reflected in the recognition of employees' rights and interests as the central focus of labour law.[1209] According to Zieliński, labour law is an inherently humanistic branch of law, as it takes an anthropocentric approach to the role of human beings in the world. Its purpose is to protect the interests of workers and to ensure that their dignity and freedom are respected.[1210]

However, the humanisation of work is not a uniform process, and the practices and ideas associated with it stem, in a sense, from working conditions that have arisen as a result of the implementation and functioning of specific economic models at particular times. For example,

[1203] Bąba, 2022, p. 107.
[1204] Bąba, 2022, p. 89.
[1205] Bąba, 2022, p. 108.
[1206] Jędrzycki, 1993, p. 10.
[1207] Walczak-Duraj, 2013, p. 10.
[1208] Kowalewska, 1971, p. 4.
[1209] Wujczyk, 2012, Wstęp.
[1210] Zieliński, 1986, p. 25.

during the First and Second Industrial Revolutions (the late 18th and 19th centuries), when so-called freely competitive capitalism was flourishing, the law was by no means a carrier of the idea of humanising work. Industrial relations at that time were treated strictly as transactional, based on the exchange of goods, to which the worker's labour was also subordinate.[1211] The state's role was to protect citizens from internal and external threats and to seek new markets and sources of capital accumulation, whilst under no circumstances intervening in relations between capital owners (employers) and the wage-earning workforce (employees). Over time, this approach began to change, and the personal aspects of the employment relations, on the one hand due to the development of the workers' movement and, on the other, to the criticism contained in the social teaching of the Catholic Church, began to come to the fore with increasing frequency. The concept of the humanisation of work gained full recognition in the period following the Second World War, though its fate varied from case to case. In the countries of Central and Eastern Europe (including the Visegrad Group countries) belonging to the so-called Eastern Bloc within the Soviet sphere of influence, processes related to the humanisation of work took place under a centrally planned economy, in which state-owned enterprises played a dominant role. At the same time, the rest of the European countries belonging to "Western Europe", including parts of the Northern and Southern Europe, began building so-called welfare states based on the principles of parliamentary democracy and a market economy, in which the state played a significant role as a market actor and regulator aiming to reduce inequalities through appropriate social policies and to safeguard decent working conditions, particularly by adopting proper labour law solutions.[1212] However, by the 1980s, Western countries had begun to reject the welfare state paradigm in favour of a neoliberal model based on competitive individualism and the replacement of the concept of society with that of a collection of individuals. This led to a significant shift away from a labour law model that placed the protection of workers and their welfare at its heart.[1213] In the socialist economy, the concept of the humanisation of labour did not develop uniformly, either; depending on the needs and objectives of a specific plan, as well as the general economic situation, it was sometimes given greater importance and sometimes less.[1214] There was a

[1211] Zieliński, 1986, p. 25.
[1212] Bruun and Hepple, 2009, pp. 34-40.
[1213] Bruun and Hepple, 2009, pp. 45-47.
[1214] For more informaiton on working conditions and the associated humantions of work in the region of Central and Easter Europe during the times of Sovite-type dictatorships, see: Walczak-Duraj, 2013, pp. 12-13; Mirosławski, 2023b, pp. 41-60; Juharová, 2023, pp. 7-22; Konjević, 2023, pp. 23-40; Szabó, C. 2023, pp. 61-75; Patulski, 2021, pp. 119-138; Jovanović and Astrov, 2024, pp. 14-18; Tökés, 1996, pp. 79-101; Pittaway, 2012.

particular discrepancy between practice and the declarative sphere.[1215] Following the turbulent period of the late 1980s and 1990s in European history and the collapse of the Eastern Bloc, eight post-socialist countries (including Poland, the Czech Republic, Slovakia and Hungary) joined the EU in 2004, thereby adopting the new "European social model" and extending their legal systems to include EU law,[1216] under which considerable attention has been devoted to the humanisation of labour relations. Nevertheless, the spread of the principles of liberal democracy, combined with the free and common market across almost the entire old continent, did not bring about Fukuyama's "end of history"[1217] or create ideal working conditions for employees; in fact, given the current state of economic development and the accompanying working conditions, it can be argued that in many cases the opposite has occurred.

Modern employees function within the paradigm of the new economy, in which the traditional organisational hierarchy based on the dichotomous division between labour and capital is gradually disappearing and being replaced by a model of network relations whose structure resembles that of swarms.[1218][1219] The new economy is founded on intangible, unquantifiable values such as information, data (including personal data), identity, loyalty, intellectual capital, ethical competence, belief, reputation, trust, and social and cultural capital. These values are subject to a process of instrumentalisation in order to achieve the highest possible business efficiency.[1220] This, in turn, leads to the dehumanisation of the employee. The example of such dehumanisation is the discourse on "human capital management" that dominates the new economy.[1221] This discourse can be seen as an expression of the ideology of managerialism, which rationalises the unethical techniques applied by managers and, increasingly, by algorithms; it relegates personal and moral issues to outside the sphere of work, treating them as matters of a non-scientific and non-objective nature; it contributes to the creation of power relations between managers and employees; and it also masks the actual social order in which the employee is treated as a corporate asset.[1222]

[1215] For example, the preamble to the Polish Labour Code of 1974 (Dz.U.1974.24.141) stated that "in Polish People's Republic, the ultimate foal of all activity is the human being, and above all the steady growth of their material well-being and cultural level". However, as pointed out in labour law literaturę published in the days of People's Poland, the socio-economic policy launched in 1970s, which placed its main emphasis on costly investments, failed to bring either material or cultural improvements to working people – See: Zieliński, 1986, p. 27.

[1216] Veneziani and Hepple, 2009, pp. 3-4.

[1217] Fukuyama, 1992 (2017).

[1218] Pentland, 2014, p. 42. See also: Zuboff, S. 2019, Chapter 15: The Instrumentarian Collective; Mirosławski, 2023a, p. 4.

[1219] Męcina, 2023, p. 77.

[1220] Walczak-Duraj, 2013, p. 15.

[1221] Liszcz, 2018, p. 28.

[1222] Walczak-Duraj, 2013, p. 16.

Such a radical reduction of the human being to the role they perform within the organisation, that is, their workplace, would not be possible in the modern world without the development of advanced technologies. Ter Haar confirms this view by stating that Industry 4.0 is based on the logic of human beings subservient to technology, rather than technology serving to ensure human well-being and dignity.[1223]

An unshakeable faith in mankind and scientific progress, despite the many laudable goals that underpin it, may lead to the complete stripping of a person of his or her dignity.[1224] This has, in fact, been illustrated repeatedly throughout this dissertation, following an analysis of the infringement of employees' right to privacy due to the traditional and modern forms of monitoring used in the workplaces and new management techniques such as algorithmic management. Therefore, there can be no doubt that, given the ongoing transformation of working conditions driven by technological development, the realisation of the concept of the humanisation of work remains one of the key issues in the field of labour sciences, including labour law.

One of the latest initiatives undertaken in the spirit of making work more humane is the EU's development of an industrial strategy - Industry 5.0. The main aim of this strategy is to look beyond mere efficiency and productivity targets, to place people at the heart of the production process, and to use new technology to ensure prosperity that goes beyond employment and economic growth, whilst respecting our planet's production limits.[1225] However, Industry 5.0 should not be seen as an attempt to carve out a new stage of economic development, but rather as an "overlay" on Industry 4.0, which aims to improve it through the transition to a sustainable, human-centric and resilient European industry.[1226] At present, Industry 5.0 serves more as a tool for shifting the narrative - one that prioritises human well-being and the good of the planet over profit, and subordinates technological development to these goals - rather than real action, for example, through legal measures that would bring these proposed ideas to fruition.[1227] However, in this context, it is necessary to refer to the current model of technological development management in Europe, which is based on the principle of risk, and to the theory of the law of good technology proposed by Ter Haar[1228].

[1223] Ter Haar, 2025, p. 49.
[1224] Barański, 2022c, p. 87; Całus, 2018, p. 252.
[1225] European Comission, Industry 5.0. [Online].
[1226] European Comission, Industry 5.0. [Online].
[1227] Ter Haar, 2025, p. 51.
[1228] Ter Haar, 2025, pp. 47-64.

One of the most recent developments in European law that has a strong impact on the field of employment and the associated development of new technologies, particularly with regard to monitoring and management systems, is the so-called AI Act[1229]. In accordance with Recital 57 of the AI Act,[1230] AI systems used in employment are classified as high-risk and will therefore be subject to stricter regulatory standards, as set out, *inter alia,* in Section 2 "Requirements for high-risk AI systems" in the AI Act.[1231] Nevertheless, the risk-based assessment system has many shortcomings and does not seem to be entirely suited to the realities of the work sphere.[1232] Ter Haar points out that a major problem with risk-based assessment is that it operates on the assumption that every technology is, to a certain extent, harmful (risky); whilst this is understandable from the perspective of labour law and the need to protect workers, it leads to a complete neglect of an alternative approach to technology, namely the development of so-called "good" technology.[1233] Accordingly, the author advocates for replacing the risk-based assessment system with a Value Sensitive Design (VSD) assessment.[1234] VSD assessment stems, in a sense, from the concept of Industry 5.0 and is intended to assess whether a given technology is designed in such a way as to uphold human values such as: welfare, ownership and property, privacy, freedom from bias, universal usability, trust, autonomy, informed consent, accountability, courtesy, identity, calmness and environmental sustainability.[1235] To sum up the topic of Industry 5.0 and the accompanying calls for change, which are, without a doubt, of a humanistic nature, it must be noted that even

---

[1229] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (hereinafter: AI Act).

[1230] Recital 57 of AI Act states that: "AI systems used in employment, workers management and access to self-employment, in particular for the recruitment and selection of persons, for making decisions affecting terms of the work-related relationship, promotion and termination of work-related contractual relationships, for allocating tasks on the basis of individual behaviour, personal traits or characteristics and for monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights. Relevant work-related contractual relationships should, in a meaningful manner, involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Throughout the recruitment process and in the evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. AI systems used to monitor the performance and behaviour of such persons may also undermine their fundamental rights to data protection and privacy."

[1231] See: Article 6 in conjunction with Annex III(4) of the AI Act.

[1232] Adams-Prassl, 2022, pp. 30-50.

[1233] Ter Haar, 2025, p. 53.

[1234] Ter Haar, 2025, p. 55.

[1235] Longo, Padovano and Umbrello, 2020, p. 13.

such strategies that are nominally pro-human can still lead to the exploitation of workers if they are not able to carry out their work freely and in a way that brings them personal fulfilment.[1236]

Another significant factor influencing the humanisation of work in the context of technology and workplace monitoring is the case law of the ECtHR, which has already been described in detail in this thesis. Particular emphasis should be placed on the Court's position, in which it indicated that the concept of privacy is not limited solely to the "inner circle" but also encompasses the possibility of building one's social identity at work through establishing contacts with other people and the outside world.[1237] As Hendrickx points out, the right to privacy plays a significant role in the process of humanising the workplace, particularly in an era of robotisation and widespread use of AI, when the ability to make autonomous decisions and the possibility to develop one's personal identity are becoming increasingly valuable.[1238]

In a world of work where technology is becoming increasingly integrated into every aspect of an employee's activities, great importance is attached to the requirement of transparency, which is intended to protect individuals from unwarranted and incomprehensible interference, for example, by surveillance systems, in the sphere of their privacy and rights. As Heald points out, transparency must be regarded as an instrument enabling the achievement of a specific objective, which, in the context of this thesis, is respect for employees' dignity and privacy.[1239] However, the principle of transparency is not theoretically homogeneous, and two approaches can be distinguished within it – contextual and universal.[1240]

The contextual approach is a mainstream regulatory approach; it forms the basis for, amongst other things, the GDPR and the AI Act, as well as the information obligations regarding monitoring set out in the labour codes of the Visegrad Group countries. It can be described as what Pasquale calls "qualified transparency" – a system of targeted disclosures, the content and level of detail of which depend on who the information is intended for.[1241] In practice, this means that the employer or the provider of the system in question should explain to employees the rationale behind the use of a particular technology, as well as how it affects working conditions and employees' rights. The problem, however, is that the information provided may not lead to a genuine understanding of how the system works.[1242] This stems from a certain information asymmetry (a lack of adequate knowledge) between employees and employers, and

[1236] Ter Haar, 2025, p. 59; Kowalewska, S. 1971, p. 4; Laruffa, 2022, p. 143.
[1237] ECtHR judgment in the case *Niemietz v. Germany* from 16 December 1992 (Application no. 13710/88), 29.
[1238] Hendrickx, 2019b.
[1239] Heald, 2006, pp. 58-73.
[1240] Molè, 2022, pp. 92-94.
[1241] Pasquale, 2015, p. 142; see also: Kaminski, 2019, p. 210.
[1242] Molè, 2022, p. 93.

even between employers and technology developers. Furthermore, understanding how a particular technology works is not made any easier by the phenomena known as "inadvertent" and "strategic" opacity, within which the key information enabling understanding is lost among the mass of other data disclosed by entities subject to transparency requirements.[1243] The contextual approach, therefore, boils down to transparency expressed within specific contexts, and nothing more.

On the other hand, the universalist approach stands in contrast to the contextual approach, as it seeks to remove the requirement for transparency from specific contexts by making technological systems universally understandable, and to move away from the unilateral imposition of a particular interpretation of these solutions by employers or providers, in favour of a collective analysis by the workplace community of how a given technology works, how it might potentially affect the rights and interests of the parties to the employment relationship, and whether and in what form it should be introduced.[1244] Consequently, this approach involves revealing the entire operational architecture of the technology, i.e. what constitutes the so-called "system functionality" – the system's requirements specification, decision trees, pre-defined models, criteria and classification structures, and how these elements affect employees.[1245] This approach could serve as a significant trigger for trade unions to redefine their role in light of the changes taking place in the world of work,[1246] since, as De Stefano points out, trade union activity and collective bargaining have been, and in the future shall be even more so, key factors in redressing inequalities between the parties to an employment relationship enhanced by the use of new technologies.[1247]

The humanistic perspective on surveillance and the relationship between employees and new technologies has also been significantly enriched by Sewell's intellectually incisive insights in the book "Surveillance: A Key Idea for Business and Society". In his work, the author, using arguments based on management theories and philosophical and sociological analysis, draws attention to the paradoxes of modern workplace surveillance. The first major paradox of workplace monitoring is the belief that surveillance is good because it is not directed "at me". Sewell points out, however, that even if we are not the target of monitoring today, we certainly will be in the future, as progressively raised performance targets will sooner or later result in us

[1243] Stohl, Stohl and Leonardi, 2016, p. 132; Varošanec, 2022, p. 4.
[1244] Molè, 2022, p. 93.
[1245] Wachter, Mittelstadt and Floridi, 2017, p. 78.
[1246] Męcina, 2023, p. 77.
[1247] De Stefano, 2018, pp. 21-24.

becoming an "inefficient resource".[1248] The second major paradox is the one-sided nature of performance monitoring. Just as managers have expectations of their subordinates, so too do employees have expectations of their managers. The paradox, however, lies in the fact that, in practice, subordinates are unable to assess their superiors because they do not have access to the detailed information on the basis of which they themselves are evaluated. [1249]

The third and final major paradox of monitoring is that the response to the frequent failure to achieve the intended outcomes of workplace monitoring is to introduce even more and even more detailed monitoring. Sewell compares this situation to an ideological trap - "it's like complaining that the Soviet Union collapsed because it wasn't communist enough or that, after years of neoliberal economic policy, so-called free markets are failing because they aren't free enough."[1250]

In light of the above, Sewell concludes that the only way to break the vicious circle of modern monitoring is to radically redefine, or rather, return to the concept of privacy as a space in which decisions are made collectively regarding what we wish to reveal about ourselves and what we wish to keep to ourselves. It is probably impossible to eliminate monitoring entirely, but we must strive to shift the paradigm from one where the minority monitors the majority to one of mutual surveillance, the aim of which is to support each other. Sewell's idea can be summed up in the rallying cry which, as the author himself suggests, he hopes to hear in the future: "The coercive surveillance of managers is dead; long live the caring surveillance of our true peers!"[1251][1252]

Moving slowly towards a conclusion of this section of the thesis, I shall take a broader view on the humanisation of work, drawing on the ideas of the eminent 19th-century economist and theorist of economic nationalism, Friedrich List, whose thinking, given the global challenges faced by national states, may constitute a significant intellectual framework for economic development in the Central and Eastern European region. In the seventeenth chapter, entitled "Industrial Power and Individual Social and Political National Productive Forces", of his opus magnum "The National System of Political Economy", List draws attention to the complex process of national development brought about by a well-structured and planned state industrial and trade policy.[1253] In doing so, he draws attention not only to development in the economic

[1248] Sewell, 2021, p. 144.
[1249] Sewell, 2021, pp. 144-145.
[1250] Sewell, 2021, pp. 145-146.
[1251] Sewell, 2021, p. 155.
[1252] Sewell, 2021, pp. 152-155.
[1253] List, 1841(2026), pp. 289-302.

sense, but also to the spiritual development of the individual, as the nation's productive forces grow, its level of education, freedom and humanism also increases. This, in turn, should translate into ever-improving working conditions in which the individual is at the centre. This argument is based on List's concept of political economy, since labour law is largely dependent on the state's economic policy, and the full and genuine humanisation of work is only possible in a state that shapes its economy responsibly and consciously, basing it on domestic capital and development of national industry, as this approach gives it full influence over the situation of working people through legal means (enforcing existing law against foreign or international entities in a dependent economy is far less effective).

The nature of the modern world brings to the fore the role of the state and the law, which is to shape reality and social relations through legal regulations. Consequently, it is the state's responsibility to steer the development of labour law in such a way as to protect the dignity of working people to the greatest possible extent. However, if the state fails to meet this challenge, it is likely that change will come from the social forces themselves, compelled to act by the threat posed by unregulated technological development, just as was the case with the Luddites. This conclusion takes on all the more significance as the first signs of the so-called neo-Luddites are already visible on the horizon.[1254]

[1254] Merchant, 2023, pp. 463-468.

Conclusion - *De lege ferenda* remarks

The trajectory of the development of workplace monitoring demonstrates a profound evolution in its forms, methodologies, objectives and implications. Beginning with the monitoring practices within task-oriented systems of labour in societies such as the society of the Middle Kingdom of Egypt, through the medieval labour surveillance aimed at preserving hierarchical social relations, then following Robert Owen's morally evaluative frameworks of "Silent Monitor", to the efficiency-focused scientific management of Frederic Winslow Taylor and modern algorithmic surveillance, it is evident that monitoring has consistently reflected broader societal values and particularly power dynamics.

As the thesis illustrates, the interplay between technology, organisational control, development of the industry and employee autonomy is resulting in an ongoing shift in the boundaries of workplace monitoring. Early practices prioritised collective productivity and moral oversight, while later systems based on scientific methods emphasised efficiency and data-driven decision-making. However, it is crucial to realise that in the realm of contemporary monitoring, we are witnessing a cyclical return to a kind of moral sphere surveillance. Modern means of employee monitoring, such as psychological tests, tracking of workers' non-work related behaviours and social media monitoring, increasingly focus on assessing workers' personal traits, emotions and characters, echoing past approaches which sought to regulate moral and behavioural norms.

The return to moral scrutiny, currently facilitated by advanced technology, raises various critical questions about privacy, ethical boundaries and the preservation of employee autonomy. While monitoring systems bring new opportunities to improve organisational efficiency in the workplace, at the same time they carry a significant risk of excessive intrusion into the personal sphere, undermining the privacy, independence and, most importantly, the dignity of the individual, which was demonstrated particularly in Chapter IV, in the section devoted to technological subordination.

Workplace monitoring cannot be perceived only as a technological phenomenon but rather as a socio-political construct shaped by historical context, economic systems and the hierarchical relations of power. In order to comprehensively understand the complexity of the modern workplace and new monitoring methods, particularly focusing on the Visegrad Group countries, it was essential to adopt, in this thesis, a critical, ethically aware, axiologically grounded and historically contextualised approach, which allows for an understanding of employee autonomy, whilst also taking into account the complex dynamics of the continuous loop of monitoring practices.

Therefore, in light of the above-presented approach and complete analysis conducted in this thesis, the first research question, “Are the regulations underpinning current workplace monitoring models in the V4 countries capable of ensuring respect for employees’ dignity, particularly in the context of modern forms of workplace monitoring?” should be answered in a nuanced manner. The regulations underpinning the current workplace monitoring models in the Visegrad Group countries are capable, to a certain extent, of securing the basic right of employees and limiting the most excessive forms of interference from the side of the employer. The framework of protection is based mainly on general requirements, such as legality, proportionality, purpose limitation, information obligation, transparency, and the obligation to respect employees’ privacy and dignity. Nevertheless, the level of protection is only partially sufficient, especially when viewing them in the context of modern forms of monitoring, which increasingly rely on highly specialised digital and algorithmic tools able to deeply interfere with the employee’s private sphere (to a certain extent even the intimate one as argued in Subchapter 4 of Chapter III). The main shortcomings of the V4 models include the usage of vague legal terms, unclear catalogues of monitoring forms and the specific grounds for conducting it, the omission of the issue of advanced monitoring technologies and limited employee participation in shaping monitoring systems. Therefore, the currently existing regulations provide the minimum necessary level of protection, but are not entirely comprehensive in terms of the changes taking place in the sphere of employment. However, given the concept of the dignity of working people, a situation in which such dignity is respected, but only to a certain extent, is not acceptable.

These conclusions lead to the formulation of certain *de lege ferenda* observations, the aim of which is to improve monitoring models in the Visegrad Group countries so that they can serve the parties to the employment relationship as effectively as possible and take into account the dignity of the employee, and in particular, its fundamental aspect, namely, privacy. Nevertheless, these observations can be divided into two groups. The first group comprises *de lege ferenda* comments in the narrow sense, i.e. those that focus primarily on legal changes and improvements to existing regulations forming the individual models of workplace monitoring in the Visegrad Group countries. The second group, in turn, is characterised by proposals of a more idealistic nature, requiring not only legal changes but, above all, social and systemic ones.

With regard to the first group of comments, it is apparent that within the workplace monitoring models, there are several semantic ambiguities which adversely affect legal certainty and the proper application of monitoring measures by employers. This is particularly evident in the example of the notion of "serious reasons/causes" arising from the employer's nature of activity, the existence of which permits interference with an employee's privacy through the use of monitoring measures by the employer. The ambiguities arising from the broad term of "serious reasons/causes," analysed in detail in the thesis, call for the establishment, within the Slovak and Czech Labour Code, of an exhaustive list of grounds that would authorise employers to apply forms of monitoring aimed at employees in the workplaces. Nevertheless, such a list should not be overly casuistic, so as to allow for a proper case-by-case analysis of each individual situation. Consequently, the concept of "serious reasons/causes" should rather be clarified in relation to specific areas of workplace operation and organisation by indicating that the serious reasons/causes may relate to the need to ensure compliance with occupational health and safety rules, the protection of the health and lives of employees and third parties present in the workplace, the protection of employer's and employee's property, the monitoring of productivity, etc. This approach could also be used to resolve uncertainties arising under Section 316 (1) of the Czech Labour Code concerning the concept of "appropriateness" of the manner in which an employer is entitled to carry out "a general check" to ensure that an employee does not, without the employer's consent, use the resource entrusted to him/her for the performance of the work for private purposes. For this purpose, paragraph 1 of Section 316 of CLC should be repealed, and the requirement to verify whether an employee is complying with the rules on the use of means of production should be included in a newly created catalogue specifying the serious cause justifying the use of monitoring. This would help to overcome concerns regarding the forms of monitoring that employers might use for the purpose of "general check," which are currently subsumed solely under the concept of "appropriateness," and, above all, to move beyond the erroneous conviction that such a type of control does not constitute an invasion of the employee's privacy.

Under the Czech model of monitoring, there is one further element that is not found in the other V4 countries. This concerns, specifically, the extensive scope for the use of covert monitoring, as explicitly provided for in Section 316 (2) of the Czech Labour Code. This provision must be viewed critically in every respect, as, firstly, it runs counter to the information obligation laid down in Section 316 (3) of the CLC, and secondly, to the principle of transparency in data processing, which is one of the key principles set out in the GDPR. If covert surveillance were to be permitted under national law, it would have to be restricted solely to exceptional cases, which would generally boil down to the detection of criminal and unlawful behaviour on the part of employees, and be subject to adequate safeguards, which was one of the ECtHR's conclusions in its judgment in the case of *López Ribalda and Others v. Spain.* However, such restrictions do not apply under the current provisions governing workplace monitoring in the Czech Republic.

However, among the Visegrad Group countries, Hungary's regulation on workplace monitoring should be regarded as the most general in terms of its conceptual scope. Its, on the one hand, brevity and, on the other, vagueness, necessitate a thorough analysis of legal doctrine, jurisprudence and, above all, the guidelines issued by the Hungarian Data Protection Authority, which have been referred to repeatedly in the thesis. Given the practical implications of workplace monitoring, this creates an unfavourable and rather complicated situation for the parties to the employment relationship, who, when turning to the provisions of the Hungarian Labour Code, are virtually unable to ascertain what rules the monitoring should comply with. Understanding how to apply workplace monitoring in Hungary is further complicated by the fact that the current regulations contain definitions that constitute a logical fallacy of the "*ignotum per ignotum*"[1255] type. An example of this type of error is the definition of "data related to the employment relationship." Under paragraph 3 of Section 11/A of the Hungarian Labour Code, an employer is entitled to inspect a computing device entrusted to an employee for work purposes, inter alia, to verify that the employee has not used it for private purposes without the employer's consent. Only data relating to the employment relationship is to be subject to such inspection. From the perspective of this provision, it is desirable to define "data related to the employment relationship." However, the Hungarian legislator's only attempt to define this concept is found in Section 11/A (4) of the HLC, which states that data required for an employer's inspection of how an employee uses the equipment entrusted to them should be considered data relating to the employment relationship. This definitional issue becomes even more significant in light of Section 11/A (5) of the HLC, according to which the employer's inspection also applies to cases where an employee, by agreement with the employer, uses personal computing devices to carry out the tasks assigned to them under their employment contract. In this regard, it would be reasonable to propose, firstly, that the term "data related to the employment relationship" be clarified by replacing it with a term more closely matching 'data concerning the performance of tasks assigned within the framework of the employment relationship," which would significantly improve the clarity of what exactly is meant by this data. Secondly, the legal fiction applied in Section 11/A(4) of the HLC, which provides that all data necessary for the employer to carry out an inspection constitutes data relating to the

[1255] Defining the unknown through the unknown.

employment relationship, is too far-reaching and, from the perspective of the employee's privacy and, above all, the proportionality of data processing, is unjustified. There is no doubt that an employer must have the right to monitor how their property is used (unless the employee is using their own personal equipment to fulfil the employment relationship) and how the employee carries out their duties. On the other hand, however, an employee's private data stored on equipment entrusted to him/her - even if they have not been permitted to use it for private purposes - cannot be regarded as data related to the employment relationship. In view of the above and the fact that, when an employee uses his/her own computing equipment, the employer is also entitled to inspect it, a requirement should be added to Title 5/A of the Hungarian Labour Code, which covers data processing in the workplace, to specify in written form (as in Section 11/A (1) of the HLC) the manner in which such an inspection may be carried out and to provide this information to the employee prior to the inspection; furthermore, where an employee uses their own equipment for work-related tasks, the employer should be required to introduce an appropriate internal workplace policy in which the use of personal equipment is precisely regulated, primarily by requiring a clear separation between private data and data required for the performance of work.[1256] An internal policy on the use of private equipment for work purposes is also highly desirable from a workplace cybersecurity perspective.

Regarding the second research question, "Is there a model of workplace monitoring in the Visegrad region that strikes the desired balance between employees' privacy and employers' interests, and could serve as a benchmark for the other V4 countries?" it should be stated that among the workplace monitoring models currently in force in the Visegrad Group countries, the Polish model stands out positively and could, in a sense, serve as a role model or at least influential inspiration for the other countries of V4.

A key feature of this approach is its comprehensive and detailed approach to workplace monitoring, which is reflected, first and foremost, in the fact that the use of specific forms of workplace monitoring is conditional upon the existence of specific grounds set out in Articles 22^2 and 22^3 of the Polish Labour Code, which significantly impacts the implementation of the principle of purpose and proportionality in data processing.

Secondly, with regard to the form of surveillance, which is video monitoring, only the Polish legislation explicitly specifies which areas must be excluded from its scope. Such an approach should definitely be adopted in other monitoring models, as at present the areas of

[1256] A practical solution in this context could be to use an external hard drive to store work-related files, or to create two separate user profiles - one for work and the other for personal use, to which the employer would under no circumstances have access.

individual exemptions in V4 countries can only be inferred from legal doctrine, case law and the guidelines of national data protection authorities, which significantly reduces the standard of regulation. Moreover, another positive feature of the Polish model that is absent in the other Visegrad Group countries is the stipulation of a maximum retention period of three months for data collected using video monitoring. However, it should be noted that it would also be appropriate to specify a maximum retention period for the other forms of monitoring, which would comply with the principles of data minimisation and storage limitation set out in Article 5(1)(c) and (e) of the GDPR. Whilst Guidelines No. 3/2019 issued by the EDPB states that the preferred maximum data retention period is 72 hours, and that exceeding this period requires additional justification,[1257] it should be noted that the EDPB identifies the protection of the employer's property and the securing of evidence relating to the infringement of such property as the primary purpose of video surveillance. Under the Polish workplace monitoring model, the purpose of video surveillance may be not only to protect the employer's property, but also to ensure the safety of employees, control production, and ensure the confidentiality of information whose disclosure might damage the employer's interests. Therefore, for example, with regard to the latter premise, for the purposes of internal proceedings at the employer's, a period of three months may be adequate.

Nevertheless, particular attention should be paid to Article 22^2 (6) of the Polish Labour Code, which could serve as a starting point for a new approach to the issue of workplace monitoring. The provision specifies how the objectives, the scope and the manner of use of monitoring shall be established. The approach adopted by the Polish legislator in this regard paves the way for the parties to the employment relationship to determine these matters, to a certain extent, autonomously by bringing together the position of employees and employer, as the regulation stipulates that they should be specified in a collective labour agreement or in the work regulations, or in an announcement if the employer is not covered by a collective labour agreement or is not obliged to adopt work regulations. Of the methods outlined for setting objectives, scope and manner of monitoring, collective agreements ensure the greatest equality between the parties and the greatest involvement of the employee side in the process of regulating monitoring, as they are concluded through legally regulated negotiations between the employer side and the trade union organisations at the workplace or inter-workplace level, within which a common position should be reached.[1258] Not without significance for the

[1257] The European Data Protection Board, 2020, p. 28.
[1258] The collective bargaining process is regulated by Article 9 of the Act of 5 November 2025 on collective labour agreements and collective agreements, Dz.U.2025.1661.

employees' ability to participate in establishing the rules for monitoring is also the work regulation, the introduction of which is mandatory if the employer employs at least 50 employees, provided that its scope has not already been regulated by a collective agreement.[1259] The process of drawing up the work regulations involves consultation with the trade union at the workplace.[1260] However, unlike in the case of collective agreements, the trade union's powers in this context are merely advisory in nature; consequently, its position is in no way binding on the employer.[1261] Moreover, in situations where it is not possible to agree on the content of the work regulations with the trade union within the timeframe agreed by the parties, or where there is no trade union at the workplace, the work regulations are unilaterally determined by the employer.[1262]

Although Polish legislation is, in this context, significantly limited compared to the legislation of other Visegrad Group countries, theoretically, it affords the greatest opportunity for influence to employees who will be subject to monitoring regarding the manner in which it is applied. Among the other countries analysed in the thesis, only the Hungarian and Slovak labour codes provide for the possibility for representation of employees to express their views on the details of a workplace monitoring system that is about to be introduced.[1263] Nevertheless, these procedures are advisory and do not impose any additional rights or obligations on the parties. In view of the above, the postulate raised, inter alia, in Slovak legal doctrine - namely, that consultations of an advisory nature should be replaced by a requirement for an agreement to be reached between the employer and the employees' representatives, which cannot be superseded by a decision of the employer[1264] - should be supported.

Despite its many merits, the Polish model, as has been pointed out, has its limitations; consequently, it must be acknowledged that, in fact, like the rest of the models present within the legal system of Visegrad Group countries, it also does not lead to a fair and resilient balance between parties of the employment relationship.

On the other hand, it should be noted that given the technological transformation and connected to it, changing organisation for work and evolving nature of employee subordination, achieving such a fair balance on the basis of any workplace monitoring model founded on strictly defined statutory principles, but in practice applying mostly to the individual

[1259] Art. 104 §1[1] of the Polish Labour Code.
[1260] Art. 104[2] §1 of the Polish Labour Code.
[1261] Nałęcz, 2021, p. 375-376.
[1262] Art. 104[2] §2 of the Polish Labour Code.
[1263] See: Section 264 (2) (d) of the Hungarian Labour Code and Section 13 (4) of the Slovak Labour Code.
[1264] Škvarková, 2017, p. 212.

relationship between an employer and a single employee, will be extremely challenging, if not unattainable.

In this regard, with reference to the second group of proposals, which are of a more idealistic nature, it shall be pointed out that the most reliable solution would be to regulate matters relating to the conduct of monitoring within collective labour agreements, as these constitute a source of labour law whose content is most strongly influenced by the parties to such agreements, thus demonstrating their social autonomy. Furthermore, collective labour agreements allow for the best possible reflection of the organisational characteristics of a given workplace or even an entire branch of industry, thereby enabling the appropriate adaptation of monitoring rules to suit the specific conditions. They may also be a significant factor in shifting the approach to monitoring, particularly in the V4 countries, from viewing it as a phenomenon affecting the individual employee, towards an approach that focuses on its collective dimension, which impacts the entire workplace environment and also brings about significant changes in the world of work. Collective agreements will also enable employees to exercise *ex ante* control over the monitoring system and contribute to the desired transparency and explainability of individual forms.

Given how low the rates of unionisation among employees and collective agreement coverage are in the Visegrad states, as supported by the data presented earlier in this thesis the above proposal serves as a starting point for a broader examination of the issue of workplace monitoring and for concluding that the development of a human-centred, solidaristic model, resilient to technological changes, which largely concern monitoring, that would enable employee participation and their protection, yet, on the other hand, providing employers with the necessary leeway in organising the workplace and safeguarding them against errors arising from insufficient clarity of regulations, should begin with efforts by national legislators to increase unionisation and coverage of collective agreements. Definitely a step in the right direction is the position set out in the Directive (EU) 2022/2041 of the European Parliament and of the Council of 19 October 2022 on adequate minimum wages in the European Union, according to which any Member State where the collective bargaining coverage rate is below 80% should adopt measures aimed at promoting collective bargaining.[1265]

However, a detailed analysis of how to achieve a high level of unionisation and collective agreement coverage in the Visegrad Group countries is beyond the scope of this thesis;

[1265] See: Recital 25 and Article 4 (2) of the Directive (EU) 2022/2041 of the European Parliament and of the Council of 19 October 2022 on adequate minimum wages in the European Union.

nevertheless, it may serve as a starting point for further research into workplace monitoring from the perspective of collective labour law in the V4 countries.

Bibliography

Literature:

1. Abraha, H. H. (2022) ‘A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workpalce’, *International Data Privacy Law*, 12(4), pp. 276-296.
2. Abraha, H. H. (2022) ‘A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace, *International Data Privacy Law*, Vol. 12, No. 4, p. 276-296.
3. Adamczyk, S. (2025) ‘Poland’ in: Müller, T. (ed.) *Collective Bargaining and minimum wage regimes in the European Union – The Transpostion of the EU Directive on Adequate Minimum Wages in the EU27*, Brussels: ETUI, pp. 91-94.
4. Adams-Prassl, J. (2022) ‘Regulating algorithms at work: Lessons for a ‘European approach to artificial intelligence’’, *European Labour Law Journal*, 13/1, pp. 30-50.
5. Agre, P. E. (1994) ‘Surveillance and Capture: Two Models of Privacy’, *Information Society*, 10(2), pp. 737-760.
6. Albin, E. (2025) ‘Privacy as Professional Identity’, *Comparative Labour Law & Policy Journal*, 45(3), pp. 521-552.
7. Aloisi, A. and De Stefano, V. (2022) *Your Boss is an Algorithm – Artificial Intelligence, Platform Work and Labour.* London: Hart Publishing.
8. Arabadjieva, K. and Franklin, P. (2023) ‘Home-Based Telework, Gender and the Public- Private Divide’ in Countouris, N., et al. (eds.), The Future of Remote Work. Brussels: ETUI, pp. 61–81.
9. Ásványi, Z. (2022) ‘Technology vs privacy at work: The extent and limitations of organizational control mechanisms’, *Management: Journal of Contemporary Management Issues*, 27(2), pp. 261-282.
10. Bąba, M. (2022) ‘Podporządkowanie technologiczne w zatrudnieniu’, *Państwo i Prawo*, Vol. 2, pp. 88 – 109.
11. Baiocco, S., Fernandez-Macías, E., Rani, U., Pesole, A. (2022) *The Algorithmic Management of work and its implications in different contexts*. Brussels: ILO and European Commission.
12. Bakalarz, T. (2019) ‘Zatrudnienie za Pośrednictwem Platformy Internetowej jako Przejaw “Uberyzacji” Pracy’, *Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji,* Vol. CXVII, pp. 9-19.
13. Ball, K.: *Workplace Surveillance: An Overview*. “Labour History”, 2010, Vol 51, Issue 1 [online]. Available at: https://www.researchgate.net/publication/45229880_Workplace_Surveillance_An_Overview (Accessed 01.02.2025).
14. Balogh, G., Z., Hagedorn, F., Kiss, A., Polyák, G., Rátai, B., Szőke, G., L. (2012) ‘Comparative report on the regulation of workplace privacy in Hungary and Germany’, in Szőke, G., L. (ed.) *Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary*. Budapest: HVG-ORAC, pp. 25-161.
15. Balogh, Z. G., Polyák, G., Rátai, B., Szőke G., L. (2012) ‘Munkahelyi adatvédelem a gyakorlatban’, *Infokommunikáció és jog,* 9(3), pp. 95-104.
16. Bankó, Z. (2008) *AZ ATIPIKUS MUNKAJOGVISZONYOK - A munkajogviszony általánostól eltérő formái az Európai Unióban és Magyarországon*. Pécs: Pécsi Tudományegyetem.
17. Bankó, Z. and Szőke, G. L. (2016) *Issues of the Digital Workplace – The Situation in Hungary*. Hungary: Jurinfo Books.

18. Baran, K. W. (2016) 'Functions of Labour Law' in Baran K. W. (ed.) *Outline of Polish Labour Law System*. Warsaw: Wolters Kluwer, pp. 33-39.
19. Barancová, H. (2016) *Nové Technológie v Pracovnom Práve a Ochrana Zamestnanca (Možnosti a Riziká).* Prague: Leges.
20. Barancová, H. (2017) *Zákonník práce – Komentár.* 1st edn. Bratislava: C. H. BECK.
21. Barancová, H. (2019) '§3 Funkcie pracovneho prava' in Barancová, H., Olšovská, A., Hamuľák, J., Dolobáč, M. *Slovenské pracovné parvo*. Bratislava: Sprint 2 s.r.o., pp. 41-42.
22. Barancová, H. (2019) 'II Predmet pracovneho prava' in Barancová, H., Olšovská, A., Hamuľák, J., Dolobáč, M. *Slovenské pracovné parvo*. Bratislava: Sprint 2 s.r.o., pp. 33-37.
23. Barancová, H. (2019) 'VIII. Pripustne zasahy zamestnavatel'a do prava na sukromny zivot zamestnancov' in Barancová, H., Olšovská, A., Hamuľák, J., Dolobáč, M. (eds.) *Slovenské pracovné parvo*. Bratislava: Sprint 2 s.r.o., pp. 147-149.
24. Barancová, H. (2020) 'Ochranná funkcia pracovného práva a aktuálne problémy vzťahu zamestnanca a zamestnávateľa', *Societas Et Iurisprudentia*, 8(1) pp. 47-60.
25. 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,* 2018/2, pp. 44-52.
26. Barański, M. (2020) 'Ukryty monitoring w miejscu pracy', *Monitor Prawa Pracy,* 2020/3, pp. 26-32.
27. Barański, M. (2021) 'Artificial intelligence in the workplace through the prism of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms' in: Martín, L. M., Załucki, M. (eds.) *Artificial Intelligence and Human Rights*. Madrid: Dykinson, pp. 340-353.
28. Barański, M. (2022a) 'Ochrona danych osobowych pracowników w orzecznictwie Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości', *Państwo i Prawo*, 1/2022, pp. 46-65.
29. Barański, M. (2022b) 'Employment Flexibility in Times of Crisis', *Studia Iuridica*, Vol. 95, pp. 9-29.
30. Barański, M. (2022c) 'Initial Remarks on Artificial Intelligence and Axiological Foundations of Labour Law', *Studia z Zakresu Pracy i Polityki Społecznej*, 29(2), pp. 85-93.
31. Barański, M. (2022d) 'Poland: Employment Relationship from the Perspective of Individual, Collective Labor Law and EU Law' in Jakab, N. (ed.) *Fundamentals of Labor Law in Central Europe*. Miskolc-Budapest: CEA Publishing, pp. 163-182.
32. Barański, M. and Gredka-Ligarska, I. (2025) 'Autonomous subordination and technological subordination as new concepts of subordinate work – in search of a new regulatory model', *Praca i Zabezpieczenie Społeczne,* LXVI(3), pp. 20-29.
33. Barański, M. and Mirosławski, T. (2023) 'Geolocation Monitoring of an Employee from the Perspective of Article 8 of the ECHR', *Acta Universitatis Sapientiae*, 12(2), pp. 1-17.
34. Barański, M. and Mirosławski, T. (2025) 'The Principle of Proportionality in the Jurisprudence of the European Court of Human Rights in Cases Concerning Workplace Monitoring', *Review of European and Comparative Law*, 63(4), pp. 177-204.
35. Barański, M. and Mirosławski, T. (2026) Monitoring the psychological or emotional state of a worker - de lege lata and de lege ferenda remarks under EU law', *Prawo i Więź,* forthcoming, pp. 1-20.

36. Barański, M., Giermak, M. (2017) ‘Protection of employees’ geolocation data in EU law’ in: Jankowska, M., Pawełczyk, M., Augustyn, S., Kulawiak, M. (eds.) *Earth Observation & Navigation. Law and Technology*. Warsaw: Ius Publicum, Instytut Praw Gospodarczego, Fundacja Instytut Własności Intelektualnej, pp. 197-208.
37. Beierová, S. (2017) ‘Kauza Bărbulescu Proti Rumunsku a Jej Vplyv Na Rozhodovanie Súdov v Slovenskej Republike’ in Barancová, H., Olšovská, A. (eds.) *Pracovné Právo v Digitálnej Dobe*. Prague: Leges, pp. 252-270.
38. Benák, J.,Vyhnánek, L. and Zahumenský, D. (2019) ‘Human Dignity in the Czech Republic’ in: Becchi, P. and Mathis, K. (eds.) *Handbook of Human Dignity in Europe.* Cham: Springer, pp. 197-210.
39. Bennett, J. (2010) ‘Compulsory Service in Late Medieval England’, *Past & Present*, 2010/209, pp. 7-51.
40. Beňová, S. and Ladiverová, E. (2020) ‘Monitorovanie zamestnancov z pohľadu GDPR’, *Comenius Časopis*, 2020/3, pp. 78-87.
41. Bibby, A. (2016) *You’re being followed – Electronic Monitoring and surveillance in the workplace.* UNI Global Union.
42. Bodie, M.T., Cherry, M.A., McCormic, M.L., Tang, J. (2016) ‘The Law and Policy of People Analytics’, *University of Colorado Law Review,* 2016/6, pp. 1-79.
43. Borrelli, I., Santoro, P. E., Gualano, M. R., Perrotta, A., Daniele, A., Amantea, C. and Moscato, U. (2022) ‘Alcohol Consumption in the Workplace: A Comparison between European Union Countries’ Policies’, *International Journal of Environmental Research and Public Health*, 19(24), pp. 1-19.
44. Božovič, M. (1995)(1787) *Jeremy Bentham: The Panopticon Writings.* New York and London: Verso.
45. Brione, P. (2020) *My boss is the algorithm: An ethical look at algorithms in the workplace.* London: ACAS, p. 1-28.
46. Bronowicka, J., Ivanova, M., Klicki, W., King, S., Kocher, E., Kubisa, J., Zielińska, J. (2020) *Game That You Can’t Win’? Workplace Surveillance in Germany and Poland*. Frankfurt (Oder): European University Viadrina.
47. Brown, P., Lauder, H., Ashton, D. (2011) *The Global Auction: The Broken Promises of Education, Jobs, and Incomes*. Oxford: Oxford University Press.
48. Bruun, N. and Hepple, B. 2009, Economic Policy and Labour Law, in: Hepple, B. and Veneziani, B. (eds.), The transformation of labour law in Europe, Oxford: Hart, Bloomsbury, pp. 31-57.
49. Bury, B. (2006) ‘Podporządkowanie pracownika pracodawcy’, *Państwo i Prawo*, Vol. 9, pp. 57-68.
50. Całus, K. (2018) ‘Transhumanizm – wizja nowego człowieka’, *Studia z Historii Filozofii*, 9(4), pp. 237-255.
51. Carmona, S., Ezzamel, M., Gutierrez, F. (1997) ‘Control and Cost Accounting Practices in the Royal Tobacco Factory of Seville’, *Accounting, Organizations and Society,* 22(5), pp. 411-446.
52. Casale, G. (2011) ‘The Employment Relationship: A General Introduction’ in Casale, G. (ed.) *The Employment Relationship – A Comparative Overview*. Geneva: ILO, pp. 1-33.
53. Cate, F. H. (1997) *Privacy in the Information Age*. Washington: The Brookings Institution.
54. Chatziathanasiou, M. 2010, ‘Addressing new aspects of surveillance in late mediaeval England, 1350-1550’, *Mos Historicus: A Critical Review of European History*, 2(1), pp. 30-56.

55. Chikritzhs, T. and Livingston, M. (2021) ‘Alcohol and the Risk of Injury’, *Nutrients*, 13(8), pp. 1-15.
56. Chountalas, P. and Karagiorgos, A. (2015) ‘Bring Your Own Device philosophy from the user’s perspective: An empirical investigation’, *Proceedings of the 2nd HOBA International Conference,* 2015/1, pp. 1-12.
57. Clark, G. (1994) ‘Factory Discipline’, *The Journal of Economic History*, 1994, 54(1), pp. 128-163.
58. Collins, H. (2025) ‘Privacy and the Right to (Dis)connect’, *Comparative Labour Law & Policy Journal*, 45(3), pp. 467-486.
59. Coser, L. A. (1977) *Masters of sociological thought : ideas in historical and social context*. New York: Harcourt Brace Jovanovich.
60. Crawford, K. (2021) *Atlas of AI.* New Haven and London: Yale University Press.
61. Cséffán, J. (2024) *A Munka Törvénykönyve és magyarázata*. Szeged: Szegedi Rendezvényszervező Kft.
62. Ćwiertniak, B. M. (2016) ‘Employment Relationship’ in Baran K. W. (ed.) *Outline of Polish Labour Law System*. Warsaw: Wolters Kluwer, pp. 121-139.
63. Czerniak-Swędzioł, J. (2025) ‘Bossware jako nowoczesne narzędzie monitorowania pracownika z perspektywy polskiego prawa pracy’, in Gersdorf M. and Maniewska E. (eds.) *Prawo Pracy Wobec Nowych Technologii*. Warsaw: Wolters Kluwer, pp.154-163.
64. Czichy, K. (2009) ‘Obowiązek trzeźwości i skutki jego naruszenia’, *Praca i Zabezpieczenie Społeczne*, 2009/8, pp. 29-35
65. Czubik, A. (2013) *Prawo do prywatności – Wpływ Amerykańskich Koncepcji i Rozwiązań Prawnych na Prawo Międzynarodowe*.Cracow: Instytut Multimedialny.
66. Dąbrowska, O. (2019) ‘Kryteria dopuszczalności stosowania monitoring w miejscu pracy oraz zwiazane z tym obowiązki pracodawcy w świetle reform ochorny danych osobowoych’, *Prawo Mediów Elektronicznych*, 1/2019, pp. 12-19.
67. De Hert, P. and Lammerant, H. (2013) *Protection of Personal Data in Work-related Relations*. Brussels: Directorate General for Internal Policies - Policy Department C: Citizens’ Rights and Constitutional Affairs.
68. De Stefano, V. (2018) ‘“Negotiating the algorithm”: Automation, artificial intelligence and labour protection*’*, *Employment Policy Department – Employment Working Paper*, 2018/246.
69. De Stefano, V. (2019) ‘‘Negotiating the Algorithm’: Automation, Artificial Intelligence and Labour Protection’, *Comparative Labor Law & Policy Journal*, 41(1), pp. 15-46.
70. Deleuze, G. (1992) ‘Postscript on the Societies of Control’, *The MIT Press*, Vol. 59, pp. 3 – 7.
71. Deli, G. and Kukoreli, I. (2019) ‘Human Dignity in Hungary’ in: Becchi, P. and Mathis, K. (eds.). *Handbook of Human Dignity in Europe.* Cham: Springer, pp. 393-414.
72. Dixon, A., Kiazim, O., Creed, S., Bowden, O. (2021) ‘Facial recognition technology in employment: what you need to know’, *RAIL: The Journal of Robotics, Artificial Intelligence & Law*, 4(2), pp. 121-130.
73. Dolobáč, M. (2022) ‘Slovakia: Traditions and New Challenges of Labor Law’ in Jakab, N. (ed.) *Fundamentals of Labor Law in Central Europe*. Miskolc-Budapest: CEA Publishing, pp. 37-56.
74. Donkin, R. (2010) *The History of Work*. London: Palgrave Macmillan.

75. Dörre-Kolasa, D. (2016) ‘Rights and Obligations of the Parties to an Employment Relationship’ in Baran K. W. (ed.) *Outline of Polish Labour Law System*. Warsaw: Wolters Kluwer, pp. 256-279.
76. Dörre-Kolasa, D. (2023) ‘Przetwarzanie Danych Osobowych Pracowników w Ramach Tak Zwanych Innych Form Monitoringu’, *Acta Universitatis Wratislaviensis – Przegląd Prawa i Administracji* CXXXII(4147), pp. 63-79.
77. Duraj, T. (2015) ‘Ewolucja pracowniczego podporządkowania jako cechy konstrukcyjnej stosunku pracy w świetle przepisów prawa pracy’, *Studia Iuridica Lublinensia,* XXIV(3), pp. 159–179.
78. Edwards, L., Martin, L. and Henderson, T. (2018) *Employee Surveillance: The Road to Surveillance is Paved with Good Intentions*. SSRN.
79. Edwards, L., Martin, L., and Henderson, T. (2018) *Employee Surveillance: The Road to Surveillance is Paved with Good Intentions*. SSRN.
80. European Committee of Social Rights (2013) *Activity Report 2012*. Council of Europe.
81. European Committee of Social Rights (2017) *Activity Report 2016*. Council of Europe.
82. European Committee of Social Rights. *Activity Report 2012*. Council of Europe, 2013.
83. European Committee of Social Rights. *Activity Report 2016*. Council of Europe, 2017.
84. European social partners autonomous framework agreement on digitalisation of 2020.
85. European Social Partners, *Framework Agreement on Digitalisation*, 2020.
86. European Union Agency for Fundamental Rights (2022) *Bias in algorithms – artificial intelligence and discrimination.* Luxembourg.
87. Ezzamel, M. (2004) ‘Work organization in the Middle Kingdom, ancient Egypt’, *Organization*, 11(4), pp. 497-537.
88. Fabbrini, F. (2010) ‘The European Multilevel System for the Protection of Fundamental Rights: A ‘Neo-Federalist’ Perspective’, *Jean Monnet Working Paper 15/10*, pp. 7-60.
89. Fajgielski, P. (2025) *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* in *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* 3rd edn. Warsaw: Wolters Kluwer/LEX.
90. Fikfak, V. and Izvorova, L. (2022) ‘Language and Persuasion: Human Dignity at the European Court of Human Rights’, *Human Rights Law Review*, 22(3) pp. 1-24.
91. Filípek, M. (2020/2021), *Ochrana soukromí a osobních údajů zaměstnanců v pracovněprávních vztazích*. Brno: Právnická Fakulta Masarykovy Univerzity.
92. Ford, M. (2000) ‘Article 8 and the Right to Privacy at the Workplace’ in Ewing, K. D. (ed) *Human Rights at Work*. London: Institute of Employment Rights, pp. 25-42.
93. Ford, M. (2002) ‘Two Conceptions of Worker Privacy’, *Industrial Law Journal,* 31(2), pp. 135-155.
94. Foucault, M. (1975) *Discipline and Punish – The Birth of the Prison*. New York: Vintage Books.
95. Foucault, M. (2020) *Nadzorować i karać. Narodziny więzienia*. Warsaw: Aletheia.
96. Fukuyama, F. (1992) (2017), *Koniec Historii i Ostatni Człowiek*. Cracow: Znak.
97. Gajar, P. K., Gosh, A. and Rai, S. (2013) ‘Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies’, *Journal of Global Research in Computer Science*, 4(4), p. 62-70.
98. Galvin, P., Bierman, A., Schieman, S. (2024) ‘Private Eyes, They See Your Every Move: Workplace Surveillance and Worker Well-Being’, *Social Currents*, 11(4), pp. 327-345.

99. Garlicki, L. (2016) ‘Art. 30’ in: Garlicki, L. and Zubik, M. (eds.) *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, *T. II*, 2nd edn. Warsaw: Wolters Kluwer/LEX.
100. Gekiere, W., Baeten, R. and Palm, W. (2010) ‘Free movement of services in the EU and health care’ in Mossialos, E., Permanand, G., Baeten, R., Hervey, T. K. (eds.) *Health Systems Governance in Europe - The Role of European Union Law and Policy*, 1st ed. Cambridge: Cambridge University Press, pp. 461-508.
101. Genin, É. (2016) ‘Proposal for a Theoretical Framework for the Analysis of Time Porosity’, *International Journal of Comparative Labour Law and Industrial Relations*, 32(3) pp. 280-300.
102. Gerber, Ch. and Krzywdziński, M. (2019), ‘Brave New Digital Work? New Forms of Performance Control in Crowdwork’, in Vallas, S.P. and Kovalainen, A. (eds.) *Work and Labor in the Digital Age*, Bingley: Emerald Publishing, pp. 121-143.
103. Global Commission on the Future of Work (2019) *Work for a Brighter Future*. Geneva: ILO.
104. Góral, Z. (2016) ‘Principles of labour law’ in Baran, K. W. (ed.) *Outline of Polish Labour Law System*, pp. 45-73.
105. Greguš, J. (2017) ‘O Monitorovanie Zamestnancov v Cestnej Doprave’ in Barancová, H., Olšovská, A. (eds.) *Pracovné Právo v Digitálnej Dobe*. Prague: Leges, pp. 227-251.
106. Greguš, J. (2018) ‘*Monitorovanie zamestnancov GPS systémom v cestnej doprave*’ in Švec, M., Bulla, M. (eds.), *Práca 4.0, digitálna spoločnosť a pracovné parvo*. Bratislava: Friedrich Ebert Stiftung, pp. 26-35.
107. Grzybowski, K. (2020) ‘Autonomia informacyjna jednostki a zgoda na przetwarzanie przez pracodawcę danych osobowych’, *Przegląd Sejmowy*, No. 6(161), pp. 47 – 67.
108. Grzybowski, S. (1957) *Ochrona Dóbr Osobistych Według Przepisów Ogólnych Prawa Cywilnego*, Warsaw: Wydawnictwo Prawnicze.
109. Gyulavári, T. (2014a) ‘A bridge too far? The Hungarian regulation of economically dependent work’, *Hungarian Labour Law E-Journal*, 2014/1, pp. 82-103.
110. Gyulavári, T. (2014b) *A szürke állomány - Gazdaságilag függő munkavégzés a munkaviszony és az önfoglalkoztatás határán*. Budapest: Pázmány Press.
111. Gyulavári, T. (2019), *Munkajog*, 5th edn. Budapest: ELTE Eötvös Kiadó.
112. Gyulavári, T. (2023) ‘Privacy at Work in Hungary’ in Hendrickx, F., Mangan, D., Gramano, E., *Privacy@work – A European and Comparative Perspective*. Alphen aan den Rijn: Kluwer Law International B. V., pp. 289-302.
113. Gyulavári, T. (2024) ‘The first platform work judgment in Central and Eastern Europe’, *European Labour Law Journal*, 15(4), pp. 931-938.
114. Hadady-Lukács A. (2024), ‘“Mutasd a táskád, megmondom ki vagy!” A munkavállaló csomagjának munkáltató általi ellenőrzése’, *Kúriai Döntések Bírósági Határozatok*, Vol. 72, 2024/8, pp. 1459-1465.
115. Hamuľák, J. and Minčič, V. (2017) ‘Nové Poznatky a Prístupy v Oblasti Monitorovania Zamestnancov’ in: Barancová, H., Olšovská, A. (eds.) *Pracovné právo v digitálnej dobe*. Praha: Leges, pp. 65-77.
116. Harris, M. D. (1907) *The Coventry Leet Book or Mayor's Register.* London and Bungay: Early English Text Society, Original Series No. 134.
117. Hatch, M. J., Cunliffe, A. L. (2013) *Organization Theory: Modern, Symbolic, and Postmodern Perspectives.* Oxford: Oxford Univeristy Press.
118. Havrilla, G. and Sanák, R. (2017) ‘Legal rules for employers for monitoring employees in Slovakia (sk)’, *European Employment Law Cases*, 2017/2, pp. 90-91.

119. Heald, D. (2006) 'Transparency as an Intrumental Values', in Heald, D. and Hood, C. (eds.) *Transparency: The Key to Better Governance?*. Oxford-New York: Oxford University Press, pp. 58-73.
120. Hendrickx, F. (2019a) 'Privacy 4.0 at work: regulating employment, technology and automation', *Comparative Labor Law & Policy Journal*, 41(1), pp. 147-172.
121. Hendrickx, F. (2022) *Protection of workers' personal data: General principles* - *ILO Working Paper 62.* Geneva: ILO.
122. Hendrickx, F. (2023) 'Privacy@work: A Systemic Introduction' in Hendrickx, F., Mangan, D., Gramano, E., (eds.) *Privacy@work – A European and Comparative Perspective*. Alphen aan den Rijn: Kluwer Law International B. V., pp. 1-56.
123. Hendrickx, Frank. "Privacy 4.0 at Work: Regulating Employment, Technology and Automation." *Comparative Labor Law & Policy Journal* 41, iss. 1 (2019): 147-172.
124. Hijmans, Hielke (2021) 'Data Protection and Surveillance: The Perspective of EU Law' in Valsamis, M. and Vavoula, N. (eds.) *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives*. Oxford: Hart Publishing, pp. 235-253.
125. Horňák, P. (2017) 'Ochrana zamestnancov vo vzťahu k monitorovaniu internetovej prevádzky zo strany zamestnávateľa' in Barancová, H., Olšovská, A. (eds.) *Pracovné právo v digitálnej dobe*. Prague: Leges, pp. 193-202.
126. Hoskin, K. W., Macve R. H. (1986) 'Accounting and the Examination: A Genealogy of Disciplinary Power', *Accounting, Organizations and Society,* 11(2), pp. 105-136.
127. Husovec, M. (2017) 'Courts, privacy and data protection in Slovakia: A hesistant guardian? in: Brkan, M. and Psychogiopoulou, E. (eds.), *Courts, Privacy and Data Protection in the Digital Environment*, Cheltenham – Northampton: Edward Elgar Publishing, p. 181.
128. Husovec, M. (2017) 'Courts, privacy and data protection in Slovakia: A hesitant guardian?' in: Brkan, M. and Psychogiopoulou, E. (eds.) *Courts, Privacy and Data Protection in the Digital Environment*. Cheltenham – Northampton: Edward Elgar Publishing, pp. 180-196.
129. Ienca, M., Malgieri, G. (2022) 'Mental data protection and the GDPR', *Journal of Law and the Biosciences*, 9(1), pp. 1-19.
130. Ingram, J. K. (1880) *Work and the Workman: An Address to the Trades' Union Congress in Dublin, September, 1880*. London: Longmans & Co. Dublin: E. Ponsonby.
131. Instytut Analiz Rynku Pracy (2020) *Czwarta rewolucja przemysłowa i jej wpływ na rynek pracy – raport tematyczny*. Warsaw.
132. Ivanova, M., Bronowicka, J., Kocher, E. and Degner, A. (2018) *The App as a Boss? Control and Autonomy in Applicaiton–Based Management*. Frankfurt (Oder): Viadrina.
133. Jakab, N. (2022) 'Hungary: Contracts in Labor Law' in Jakab, N. (ed), *Fundamentals of Labor Law in Central Europe*. Miskolc-Budapest: CEA Publishing, pp. 205-226.
134. Jarrahi, M. H., Newlands, G., Lee, M. K., Wolf, Ch. T., Kinder, E., Sutherland. W. (2021) 'Algorithmic management in a work context', *Big Data & Society*, 8 (2), pp. 1-14.
135. Jaskulska, J. (2023) 'Employee sobriety control – new legislation in light of past problems. Is the direction of changes reasonable?', *Praca i Zabezpieczenie Społeczne*, 2023/2, pp. 39-46.
136. Jędrzycki, W. (1993) *Humanizacja pracy – założenia modelowe i praktyka społeczna.* Warsaw: IFiS PAN.
137. Jończyk, J. (1965) *Spory ze stosunku pracy*. Warsaw: PWN.

138. Jończyk, J. (1995) *Prawo Pracy*, 3rd edn. Warsaw: PWN.
139. Jovanović, B. and Astrov, V. (2024) *Labour developments, living standards and well-being in Eastern Europe before the transition*. Vienna: The Vienna Institute for International Economic Studies.
140. Juharová, J. (2023) 'The Gender Equality of Workers in Slovakia During Socialism', *Revista Română de Istoria Dreptului / Romanian Journal of Legal History*, 3(1), pp. 7-22.
141. Kadish, G. E. (1996) 'Observations on Time and Work-Discipline in Ancient Egypt' in Der Manuelian, P. (ed.) *Studies in Honor of William Kelley Simpson,* Vol. II. Boston: Museum of Fine Arts, pp. 439-449.
142. Kahn-Freund, O. (1983) *Labour and the Law.* Davies, P. and Freedland, M. (eds.), 3rd ed. London: Stevens & Sons.
143. Kajtár, E. (2015) 'Európai ügyek a Facebook sötét oldaláról – A munkavállalók közösségi oldalakon tanúsított kötelezettségszegő magatartása' in Horváth, I. (ed.) *Tisztelgés: ünnepi tanulmányok Dr. Hágelmayer Istvánné születésnapjára*. Budapest: ELTE Eötvös Kiadó, pp. 199-213.
144. Kajtár, E. (2016) *Dignity at Work: Employees' Personality Rights in the 21st Century*. Pécs: University of Pécs, Faculty of Law.
145. Kalus S. (2018) 'Art. 23' in Fras, M. and Habdas, M. (eds.) *Kodeks cywilny. Komentarz. Tom I. Część ogólna (art. 1-125)*. Warsaw: Wolters Kluwer/LEX.
146. Kaminski, M. E. (2019) 'The Right to Explanation, Explained', *Berkeley Technology Law Journal*, 34(1), pp. 189-218.
147. Kanigel, R. (2000) *The One Best Way: Frederick Winslow Taylor and the Enigma of Efficiency*. London: Abacus.
148. Kant, I. (1785)(1889)(2011) *Kant's Critique of Practical Reason and Other Works on the Theory of Ethics*. 4th edn. London: Kongmans, Green and Co., 1889, digitalised by Liberty Fund, Inc. in 2011.
149. Kardkovács, K. (2014) *A Munka Törvénykönyvének magyarázata.* Budapest: HVG-ORAC.
150. Kártyás, G., Répáczki, R., Takács G. 2016, *A munkajog digitalizálása - A munkajog hozzáalkalmazása a digitális munkakörnyezethez és a változó munkavállalói kompetenciákhoz*. Budapest: Közösen a Jövő Munkahelyeiért Alapítvány.
151. Kellogg, K.C., Valentine, M.A., Christin, A. (2020) 'Algorithms at Work: The New Contested Terrain of Control', *Academy of Management Annals*, 14(1), p. 366-410.
152. Kokott, J. and Sobotta, C. (2013) 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law*, 3(4), pp. 222-228.
153. Kołakowski, L. (1976)(2000) *Główne Nurty Marksizmu - Część I Powstanie.* Warsaw: Wydawnictwo Zysk i S-ka.
154. Koltay, A. (2022) 'Social Media and Freedom of Speech in Employment: Limitations on Employees' Right to Self Expression' in Gyulavári, T. and Menegatti, E. (eds.) *Decent Work in the Digital Age: European and Comparative Perspectives*. Oxford: Hart, pp. 331-345.
155. Koltay, A. (2023) 'The Protection of Privacy in the Hungarian Legal System, with Special Regard to the Freedom of Expression' 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. 77-109.
156. Konjević, T. (2023) 'Legislative and Social Emancipation of Working Women in Croatia Under the Influence of Socialist Ideologies', *Revista Română de Istoria Dreptului / Romanian Journal of Legal History,* 3(1), pp. 23-40.

157. Kopff, A. (1972) ‘Koncepcja praw do intymności i do prywatności życia osobistego. Zagadnienia konstrukcyjne’, *Studia Cywilistyczne*, t. XX, pp. 3-44.
158. Kovanič, M. (2020) ‘Individual Experiences of Surveillance: Attitudes Towards Camera Surveillance in Slovakia’, *Sociologický Časopis / Czech Sociological Review*, 56(3), pp. 343-361.
159. Kowalewska, S. (1971), *Humanizacja pracy*. Warsaw: Wydawnictwo Związkowe CRZZ.
160. Križan, V. (2016) ‘Ochrana súkromia zamestnanca v ére internetu’ in: Barancova., H., Olšovska., A. (eds.) *Súčasný stav a nové úlohy pracovného práva*. Praha: Leges, pp. 260-273.
161. Kuba, M. (2014), ‘Monitoring w miejscu pracy – refleksje na tle aktualnego stanu prawnego’, *Krytyka Prawa. Niezależne Studia Nad Prawem*, 6(1), pp. 559-570.
162. Kuba, M. (2014), Prawne formy kontroli pracownika w miejscu pracy. Warsaw: Wolters Kluwer/LEX.
163. Kuba, M. (2019) ‘Monitoring Poczty Elektoronicznej Pracownika – Refleksje na Tle Nowych Regulacji Prawnych’, *Praca i Zabezpieczenie Społeczne,* 2019/11, pp. 29-35.
164. Kuba, M. (2025), ‘Art. 22(1c)) Przesłanki wprowadzenia i sposób przeprowadzenia kontroli trzeźwości pracowników’, in Baran, K. W. (ed.) *Kodeks pracy. Komentarz. Tom I. Art. 1-93*. Warsaw: Wolters Kluwer/LEX.
165. Kun, A. (2021) ‘Non-standard forms of work in Hungary – Selected Issues’ in Mihes, C. (ed) *Non-standard forms of employment in selected countires in Central and Eastern Europe – A critical glance into regualtion and implementation*. Geneva: International Labour Organization, pp. 47-68.
166. Kuźnicka, D. (2018) ‘Monitorowanie Pracownika w Miejscu Pracy a Ochrona Prywatności’, *Przegląd Prawniczy Uniwersytetu Warszawskiego*, 2018/1, pp. 53-79.
167. Lafferty, M. (2014) ‘Article 8: The Right to Respect for Private and Family Life, Home and Correspondence’ in Harris, D., O’Boyle, M., Bates, E. P., and Buckley, C. M., (eds.) *Harris, O’Boyle & Warbrick: Law of the European Convention on Human Rights*. Oxford: Oxford University Press, pp. 522-591.
168. Ľalík, T. (2019) ‘Human Dignity in Slovakia’ in: Becchi, P. and Mathis, K. (eds.) *Handbook of Human Dignity in Europe.* Cham: Springer, pp. 799-815.
169. Landes*,* D. S. (1969) *The Unbound Prometheus: Technological Change and Industrial Development in Western Europe from 1750 to the Present.* Cambridge: Cambridge University Press.
170. Laruffa, F. (2022) ‘Re-thinking Work and Welfare for the Social-Ecological Transformation’, *Sociologica*, 16(1), pp. 123-151.
171. Lis-Staranowicz, D. and Dobrowolski, M. (2022) '(Im)permanence of Polish Constitutionalism: in Search of an Optimal Vision of the State’ in: Csink, L. and Trócsányi, L. (eds.) *Comparative Constitutionalism in Central Europe: Analysis on Certain Central and Eastern European Countries.* Miskolc-Budapest: CEA Publishing, pp. 89-108.
172. List, F. (1841)(2026) *Narodowy System Ekonomii Politycznej*. Warsaw: Prześwity.
173. Liszcz, T. (2018) *Aksjologiczne Podstawy Prawa Pracy*. Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej.
174. Lock, T. (2019) ‘Commentary on Article 8 CFR’ in Kellerbauer, M., Klamert, M., Tomkin, J., (eds.) *Commentary on the EU Treaties and the Charter of Fundamental Rights.* Oxford: Oxford University Press, pp. 2121-2127.
175. Longfellow, E. (2006) ‘Public, Private, and the Household in Early Seventeenth-Century England’, *Journal of British Studies*, 45(2), pp. 313-334.

176. Longo, F., Padovano, A. and Umbrello, S. (2020) 'Value-Oriented and Ethical Technology Engineering in Industry 5.0: A Human-Centric Perspective for the Design of the Factory of the Future', *Applied Sciences,* 10(12), pp. 1-25.
177. Lőrincz G. (2025) 'Commentary on Section 11/A' in Petrovics Z. (ed.) *A Munka Törvénykönyvének magyarázata*. Budapest: ORAC Kiadó.
178. Lubasz, D., Chomiczewski, W., Czerniawski, M., Drobek, P., Góral, U., Kuba, M., Makowski, P., Witkowska-Nowakowska, K. (2018) 'Art. 4' in Bielak-Jomaa, E. and Lubasz, D. (eds.) *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Warsaw: Wolters Kluwer/LEX.
179. Łuczak, J. (2018) 'Art. 12' in Bielak-Jomaa, E. and Lubasz, D. (eds.) *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Warsaw: Wolters Kluwer/LEX.
180. Lukács A. (2023) '"Csak még egy pohárkával!" – A munkavállalók alkohol és kábítószer fogyasztásának szabályozása és ellenőrzése', *Kúriai Döntések Bírósági Határozatok*, Vol. 71, 2023/11, pp. 2092-2099.
181. Lukács, A. (2017) 'Privacy at Work: the Regulation of Camera Surveillance in Hungarian Labour Law', *Acta Universitatis George Bacovia. Juridica*, 6(1), pp. 77-118.
182. Lukács, A. (2021) *Employees' Right to Privacy and Right to Data Protection on Social Network Sites.* Szeged: Iurisperitus Publishers.
183. Lupton, D. (2016) *The Quantified Self.* 1st edn. Cambridge: Polity.
184. Maciejewska, M. and Figurski, A. (2014) 'Wybrane metody kontroli pracownika w świetle obowiązujących przepisów prawnych', *Zeszyt Naukowy.pl/Wyższa Szkoła Zarządzania i Bankowości w Krakowie*, 2014/32, pp. 1-13.
185. Majchrzak (2015) 'Zakres najważniejszych obowiązków pracownika w świetle przepisów Kodeksu Pracy', *Prawo Kanoniczne,* 58(1), pp. 151-167.
186. Markantonatou, M. (2007) 'The ideal-typical transition from Fordist to post-Fordism: A neopositivist problem setting', *European Research Studies*, X(1-2), pp. 119-129.
187. Marx, K. (1867)(1992) *Capital: A Critique of Political Economy Vol. I*. London: Penguin.
188. Matuszak, M. (2023) 'Funkcja ochronna prawa pracy a penalizacja naruszeń praw pracowników', *Studia Prawnicze KUL*, Vol. 1(93), pp. 99-112.
189. McCartney, D. R. (1994) 'Electronic surveillance and the resulting loss of privacy in the workplace', *UMKC Law Review*, 62(4), pp. 859-891.
190. McGill, L. D. (1990) 'Psychological tests in the workplace: Should your company use them?', *Employment Relations Today*, 17(3), pp. 227-232.
191. Męcina, J. (2023), *Od cyfryzacji I robotyzacji do sztucznej inteligencji – wyzwania dla gospodarki I rynku pracy*. Warsaw: Wydawnictwo Naukowe Scholar.
192. Mélypataki, G., Rácz, Z. (2018) 'A személyiségi jogok védelmének ütközése a munkajogban' in: Auer, Ádám et al. (eds) *Ünnepi kötet a 65 éves Kiss György tiszteletére – Liber Amicorum in honorem Georgii Kiss aetatis suae LXV*. Budapest: Dialóg Campus Kiadó, pp. 677-684.
193. Merchant, B. (2023) *Blood in the Machine – The Origins of the Rebellion Against Big Tech*. New York-Boston-London: Little, Brown and Company.
194. Mesarčík, M., Poruban, A. (2023) 'Privacy at Work in Slovakia' in Hendrickx, F., Mangan, D., Gramano, E. (eds.) *Privacy@work – A European and Comparative Perspective*, Alphen aan den Rijn: Kluwer Law International B. V., pp. 455-468.
195. Miller, S. and Weckert, J. (2000) 'Privacy, the Workplace and the Internet', *Journal of Business Ethics*, 28(3), pp. 255-265.

196. Miłosz, M. and Świątek-Rudoman, J. (2019) 'Nowe ramy prawne stosowania przez pracodawcę monitoringu wizyjnego w zakładzie pracy', *Praca i Zabezpieczenie Społeczne*, 2019/4, pp. 31-39.
197. Mirosławski, T. (2023a) 'Platform work as a manifestation of a new form of employment in the era of the fourth industrial revolution', *Z Problematyki Prawa Pracy i Polityki Socjalnej*, 21(4), pp. 1-16.
198. Mirosławski, T. (2023b) 'The Principle of Gender Equality in Employment: Historical Development During the Period of Soviet-type Dictatorship in Poland', *Revista Română de Istoria Dreptului / Romanian Journal of Legal History*, 3(1), pp. 41-60.
199. Mirosławski, T. (2025) 'Between Casuistry and Vagueness – A Comparative Legal Analysis of Employer Surveillance of Employee Tasks under Polish and Czech Legislation', *Central European Academy Law Review*, *2*(1), pp. 191-216.
200. Mitrus, L. (2014) '*Godność jako podstawa aksjologiczna praw pracowniczych'* in Skąpski, M. and Ślebzak, K. (eds.) *Aksjologiczne podstawy prawa pracy i ubezpieczeń społecznych*. Poznań: Ars boni et aequi - Przedsiębiorstwo Wydawnicze - Michał Rozwadowski, pp. 133-142.
201. Molè, M. (2026), *Monitored at Work – The Legitimate Exercise of the Employer's Monitoring Power in the Age of Artificial Intelligence and the Internet of Things*. Alphen aan den Rijn: Kluwer Law International B. V.
202. Molè, M. 2022, 'The Internet of Things and Artificial Intelligence as Workplace Supervisors: Explaining and Understanding the New Surveillance to Employees Beyond Art. 8 ECHR', *Italian Labour Law e-Journal*, 15(2), pp. 87-103.
203. Molè, M. and Mangan, D. (2023) ''Just more surveillance': The ECtHR and workplace monitoring', *European Labour Law Journal*, 14(4), pp. 694 – 700.
204. Moore, P. V., Akhtar, P., Upchurch. M. (2018) 'Digitalisation of Work and Resistance' in Moore, P. V., Upchurch, M., Whittaker, X. (eds.) *Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism*. London: Palgrave Macmillan Cham, pp. 17-44.
205. Morávek, J. (2012) 'Sledování zaměstnanců v kontextu novely zákoníku práce', *Právní rozhledy*, 2012/5, pp. 175-185.
206. Morávek, J. (2013) *Ochrana osobních údajů v pracovněprávních vztazích.* Prague: Wolters Kluwer/ASPI.
207. Morávek, J. (2017) 'Kontrola a sledování zaměstnanců - výklad § 316 ZPr', *Právní rozhledy,* 25(17), pp. 573-585.
208. Morávek, J. (2020) 'Kamerové systémy z hlediska inspekce práce a Úřadu pro ochranu osobních údajů' in Morávek, J. (ed.) *Důkazní Prostředky A Jejich Přípustnost Zejména Se Zaměřením Na Kamerové Sledování.* Prague: Eva Rozkotová Publishing, pp. 6-43.
209. Moreham, N. A. (2008) 'The right to respect for private life in the European Convention on Human Rights: a Re-examination', *European Human Rights Law Review*, 2008/I, pp. 44-79.
210. Morris, G.S. (2001) 'Fundamental Rights: Exclusion by Agreement', *Industrial Law Journal*, 30(1), pp. 49-71.
211. Mrozek, J.J. (2014) 'Godność Osoby Ludzkiej Jako Źródło Praw Człowieka i Obywatela', *Civitas et Lex*, 2014/1, p. 41-47
212. Munn, L. (2024) 'Expansive and Invasive: Mapping the "Bossware" Used to Monitor Workers', *Surveillance & Society,* 2024/2, pp. 104-119.
213. Musiała, A. (2009) 'Podporządowanie pracownika w stosunku pracy – Glosa do wyroku z dnia 7 marca 2006 r., I PK 146/05', *Gdańskie Studia Prawnicze – Przegląd Orzecznictwa,* 2009.1, pp. 127-133.

214. Musiała, A. (2019) *Polskie Prawo Pracy a Społeczna Nauka Kościoła – Studium Prawno Społeczne.* Poznań: Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza w Poznaniu.
215. Nádas, G., Rab, H., Sipka, P., Zaccaria, M. L., (2018) *Az egyenlő foglalkoztatás követelménye a változó munkajogi elvárásokat tükröző HR tendenciák keretei között*. Budapest: HVG-ORAC.
216. Nałęcz, M. (2021), Rozdział IV. Regulamin Pracy in: Muszalski, W. and Walczak, K. (eds.) *Kodeks Pracy – Komentarz,* 13th edn. Warsaw: C.H.Beck, pp. 365-377.
217. Olšovská, A., Švec, M. 2017, 'Use of Psychological Examinations of Employees and Job Applicants in Personnel Management' in Mura, L. (ed.) *Issues of Human Resource Management*. London: InTech, pp. 23-41.
218. Oręziak, B. (2023) 'The Right to Privacy in the Digital Age: A Perspective from the Republic of Poland' 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. 311-343.
219. Otto, M. (2016), *The Right to Privacy in Employment – A Comparative Analysis*. Oxford and Portland: Hart Publishing.
220. Otto, M. (2019) 'Prawo do prywatności pracowników w orzecznictwie Europejskiego Trybunału Praw Człowieka'*, Monitor Prawa Pracy,* 2019/8, pp. 50-56.
221. Otto, M. (2022) 'Dyskryminacja Algorytmiczna w Zatrudnieniu. Zarys Problemu', *Studia z Zakresu Prawa Pracy i Polityki Społecznej,* 29(2), pp. 145-160.
222. Otto, M. (2023) 'Privacy at Work in Poland', in Hendrickx, F., Mangan, D., and Gramano, E. (eds.) *Privacy@Work: A European and Comparative Perspective*. Alphen aan den Rijn: Kluwer Law International B. V., pp. 393-412.
223. Pasquale, F. (2015) *The Black Box Society – The Secret Algorithms That Control Money and Information*. Cambridge-London: Harvard University Press.
224. Patulski, A. (2021) 'Praca w Państwie Prerogatywnym w Wersji Socjalistycznej', *Rocznik Administracji i Prawa*, II/XXI, pp. 119-138
225. Pentland, A. (2014) *Social Physics – How Social Networks Can Make Us Smarter*. New York: Penguin Books.
226. Petrik, F. (2014) 'Személyiségi jogok' in: Wellmann G. (ed.) *Polgári jog: Bevezető és záró rendelkezések. Az ember mint jogalany. Öröklési jog,* 2nd edn. Budapest: HVG-ORAC, pp. 173 – 174.
227. Petrovics, Z. (2021) 'Break out of the Box: A Proposal on How to Interpret Termination without Notice on the Grounds of Objective Impossibility in Hungarian Labour Law', *Hungarian Labour Law E-Journal*, 2021/1, pp. 46-61.
228. Pichrt, J and Stádník, J. (2019) '§ 106, Práva a povinnosti zaměstnance' in Bělina, M. and Drápal, L. *Zákoník práce. Komentář*, 3rd edn. Prague: C. H. Beck, pp. 590 – 599.
229. Pisarczyk, Ł. (2010) 'Przeobrażenia Prawa Pracy a Jego Funkcja Ochronna', *Studia Prawnicze: Rozprawy i Materiały*, 2010/1, pp. 15-45.
230. Pisarczyk, Ł. (2025) 'Art. 11(2)' in Baran, K. W. (ed.) *Kodeks pracy. Komentarz. Tom I. Art. 1-93*, Warsaw: Wolters Kluwer/LEX.
231. Pittaway, M. (2012) *The Workers' State – Industrial Labor and the Making of Socialist Hungary 1944 – 1958*. Pittsburgh: University of Pittsburgh Press.
232. Pók, L. (2012) 'Lájkolni szabad? Munkavállalói véleménynyilvánítás az új Munka Törvénykönyve tükrében'*, Infokommunikáció és jog*, 2012/4 (51), pp. 160–165.
233. Pope John Paul II, (1981)(2021) *Laborem Exercens*. Wroclaw: Wydawnictwo Wrocławskiej Księgarni Archidiecezjalnej.
234. Pope Leo XIII (1891) *Rerum Novarum*. Warsaw: Capital sp. z.o.o.
235. Pope Pius XI (1931) *Quadragesimo Anno*. Warsaw: Capital sp. z.o.o.

236. Potyková, A. (2018/2019) *Ochrana osobních údajů v pracovněprávních vztazích*. Brno: Masaryk University.
237. Prusinowski, P. (2025) ‘Art. 304’ in Baran, K. W. (ed.) *Kodeks pracy. Komentarz. Tom II. Art. 94–304(5),* Warsaw: Wolters Kluwer/LEX.
238. Pryciak, M. (2010) ‘Prawo do prywatności’, *Studia Erasmiana Wratislaviensia*, Vol. IV, pp. 211-229.
239. Puci, M. (2016) ‘Elektronizácia pracoviska’, in Žuľová, J. (ed.) *Ochrana Súkromia Zamestnanca*. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach - Právnická Fakulta, pp. 79-99.
240. Rácz, I. (2015) ‘A közösségi média használatának árnyoldalai a munkaviszonyban’ in Deres, P., Grad-Gyenge, A. (eds.) *Acta Iuvenum Caroliensia VII*. Budapest: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, pp. 279-305.
241. Rawls, J. (1971)(1999), A Theory of Justice. Cambridge (Massachusetts): Harvard University Press, Belknap Press.
242. Razzolini, O. (2010) ‘The Need to Go Beyond the Contract: “Economic” and “Bureaucratic” Dependence in Personal Work Relations’, *Comparative Labor & Policy Journal,* 31(2), pp. 267–301.
243. Richards, N. M. (2013) ‘The Dangers of Surveillance’, *Harvard Law Review*, Vol. 126, pp. 1934-1965.
244. Robertson, K. (2006) *The Laborer’s Two Bodies*. New York: Palgrave Macmillan.
245. Rosenblat, A. and Stark, L. (2016) ‘Algorithmic Labor and Information Asymmetries: A Case Study of Uber’s Drivers’, *International Journal of Communication*, Vol. 10, pp. 3758–3784.
246. Rothschild, E. 1973, *Paradise Lost: The Decline of the Auto-Industrial Age*. New York: Random House.
247. 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*, 16(2), pp. 149-164.
248. Rushing, W. A. (1966) ‘Organizational Rules and Surveillance: Propositions in Comparative Organizational Analysis’, *Administrative Science Quarterly*, 10(4), pp. 423-443.
249. Rustad, Michael. L., and Paulsson, Sandra. R. (2005) ‘Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe’, *University of Pennsylvania Journal of Business Law*, 7(4), p. 829–904.
250. Sarzyński, K. (2016) ‘Bring Your Own Device (BYOD) – szansa czy zagrożenie dla przedsiębiorstwa?’, *Organizacja i Zarządzanie: Kwartalnik Naukowy*, 2016/4, pp. 66-80.
251. Schronk, R. (2017) ‘The Concept of ‘Employee’: The Position in Slovakia’ in: Waas, B. and Heerma van Voss, G. (eds.) *Restatement of Labour Law in Europe: The Concept of Employee*. Oxford: Hart Publishing, pp. 619-640.
252. 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.
253. Sewell, G. (2021) *Surveillance: A Key Idea for Business and Society.* London and New York: Routledge.
254. Sewell, G., Barker, J. R. (2006) ‘Coercion versus Care: Using Irony to Make Sense of Organizational Surveillance’, *The Academy of Management Review*, 31(4), pp. 934-961.

255. Šimečková, E. (2021) 'Legislation on Employer Monitoring of Employees at the Workplace in the Czech Republic', *Studia Prawno-Ekonomiczne*, 105(2021), pp. 91–105.
256. Simitis, S. (1998) 'From the General Rules on Data Protection to a Specific Regulation of the Use of Employee Data: Policies and Constraints of the European Union', *Comparative Labor Law and Policy Journal,* 19(3), pp. 351-371.
257. Simitis, S. (1998) 'From the General Rules on Data Protection to a Specific Regulation of the Use of Employee Data: Policies and Constraints of the European Union', *Comparative Labor Law and Policy Journal,* 19(3), pp. 351-372.
258. Sinzheimer, H. (1927) 'Fundamental Questions of Labour Law (*Das Wesen des Arbeitsrechts*)' in Hermes, G. (ed.) *Grundfragen des Arbeitsrechts*. Berlin: Berlag d. Allg (translated by Robert Knegt).
259. Sipka, P. and Zaccaria M. L. (2019) 'Kísérlet a magyar munkaviszony fogalom újragondolására az NMSZ 198. zámú ajánlásának fényében', *Miszkolci Jogi Szemle,* 14(1), pp. 49-67.
260. Siskovičová, K. (2015) *Ochrana Súkromia a Osobných Údajov Zamestnanca*. Trnava: Trnavská Univerzita v Trnave.
261. Skąpski, M. (2006) *Ochronna funkcja prawa pracy w gospodarce rynkowej*. Cracow: Zakamycze/Wolters Kluwer-LEX.
262. Škvarková, M. (2017) 'Kamerový Systém na Pracovisku vs. Právo Zamestnanca na Súkromie' in Barancová, H., Olšovská, A. (eds.) *Pracovné právo v digitálnej dobe*. Prague: Leges, pp. 203-215.
263. Šmejkal, V. (2019) 'High Tech Monitoring Versus Privacy in the Workplace in the Law and Case Law of the Czech Republic', *Białostockie Studia Prawnicze,* 24(2), pp.53-89.
264. Šmigová, K. (2023) 'The Right to Privacy in the Digital Age from the Viewpoint of the Slovak Legal Order', 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. 165-197.
265. Smith, A. (1977) (1776) *An Inquiry into the Nature and Causes of the Wealth of Nations*, Cannan E. (ed.). Chicago: University of Chicago Press.
266. Smolski, M. (2015) 'Kontrola Osobista Pracowników – Wczorajsze Orzeczenie w Dzisiejszej Rzeczywistości (Uwagi w Świetle Wyroku Sądu Najwyższego z Dnia 13 Kwietnia 1972 Roku)', *Zeszyty Naukowe Uniwersytetu Szczecińskiego,* 2015/9, pp. 75-94.
267. Sobczyk, A. (2021), *Zakład pracy jako zakład administracyjny*. Cracow: Wydawnictwo UJ.
268. Stefański, K. (2021) 'Employee geolocation versus the GDPR', *Praca i Zabezpiecznie Społeczne*, 2021/4, pp. 14-17.
269. Štefko, M. (2012) 'Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochraně lidských práv a základních svobod', J*urisprudence*, 2012/7-8, pp. 17-21.
270. Štefko, M. (2016) 'Social Media in the Workplace in the Czech Republic, Poland and Slovakia', *The Lawyer Quarterly*, 6(1), pp. 11-17.
271. Štefko, M. (2017) 'Social Media in the Workplace (Bărbulescu v. Romania, ECHR, 61496/08)' in Bellomo, S., Gundt, N., Łaga, M., Boto, J. M. M. (eds.), *Labour Law and Social Rights in Europe: The Jurisprudence of International Courts – Selected Judgements*. Gdańsk: Gdańsk University Press, pp. 145-156.
272. Štefko, M. (2022) 'Czech Republic: Critical Legal Analysis on Dogmatic and Current Issues of Labor Law', in Jakab, N. (ed.) *Fundamentals of Labor Law in Central Europe.* Miskolc-Budapest: CEA Publishing, pp. 135-162.

273. Štefko, M. (2023) ‘Privacy at Work in the Czech Republic’ in Hendrickx, F., Mangan, D., Gramano, E., (eds.) *Privacy@work – A European and Comparative Perspective*. Alphen aan den Rijn: Kluwer Law International B. V., pp. 137-156.
274. Štefko, M. and Pichrt, J. (2015) *Labour Law in the Czech Republic*, 2nd edn. Alphen aan den Rijn: Wolters Kluwer.
275. Štěpánková, K. (2025) ‘Workplace Surveillance of Employees from the Czech Perspective’, *Central European Academy Law Review*, 2(1), pp. 319-336.
276. Stohl, C., Stohl, M. and Leonardi, P. M. (2016) ‘Managing Opacity: Information Visibility and the Paradox of Transparency in the Digital Age’, *International Journal of Communication*, Vol. 10, pp. 123-137.
277. Supiot, A. (1999) ‘The transformation of work and the future of labour law in Europe: A multidisciplinary perspective’, *International Labour Review,* 138(1), pp. 31-46.
278. Surdykowska, B. (2023) ‘O lęku przed nadciągającym chipowaniem pracowników – uwagi na tle powstającego ustawodawstwa w USA’, *Z Problematyki Prawa Pracy i Polityki Socjalnej, 2023,* 21(4), pp. 1-15.
279. Surdykowska, B. (2023) ‘O lęku przed nadciągającym chipowaniem pracowników – uwagi na tle powstającego ustawodawstwa w USA’, *Z Problematyki Prawa Pracy i Polityki Socjalnej*, 4(21), pp. 1-15.
280. Surdykowska, B. (2025) ‘Jak długo nasze ciała pozostaną nasze? Kilka uwag o udoskonalaniu człowieka w kontekście wykonywania pracy’ in: Gersdorf, M. and Maniewska, E. (eds.) *Prawo Pracy Wobec Nowych Technologii*. Warsaw: Wolters Kluwer, pp. 303-325.
281. Sut, P. (1994) ‘Ochrona Sfery Intymności w Prawie Polskim – Uwagi De Lege Lata i De Lege Ferenda’, *Ruch Prawniczy, Ekonomiczny i Socjologiczny,* 56(4), pp. 102-104.
282. Švec, M. and Valentová, T. (2021) *Prevencia negatívneho zásahu do súkromia zamestnanca*. Bratislava: Wolters Kluwer.
283. Švec, M., Toman, J., Olšovská, A., Žuľová, J., Tonhauser, P., Hamuľák, M., Drobný, M., Dušeková Schuszteková, S., Horecký, J., Dolobáč, M. (2023), *Zákonník práce – komentár*. Wolters Kluwer/ASPI.
284. Swan, M. (2013) ‘The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery’, *Big Data*, 1(2), pp. 85-99.
285. Sygit-Kowalkowska, E. and Ziółkowski, M. (2019) ‘Workplace Stress and Alcohol Consumption. Research State-of-art. Review and Further Development’, *Alcoholism and Drug Addiction*, 32(2), pp. 109-130.
286. Szabó, C. (2023) ‘Historical Development of Gender Equality During the Soviet-type Dictatorship in Romania’, *Revista Română de Istoria Dreptului / Romanian Journal of Legal History,* 3(1), pp. 61-75.
287. Szabó, D. M. and Székely, I. (2005) ‘A privacy védelme a munkahelyen’ in Szabó, D. M. and Székely, I. (eds.) *Szabad Adatok, Védett Adatok*. Budapest: BME GTK ITM, pp. 115-148.
288. Szádeczky, T. (2012) ‘The Role of the Technology - Auditing and Certification in the Field of Data Security’ in Rátai, B., Szádeczky, T. and Szőke, G. L. (eds.) *Privacy Management System for the Purpose of Managing Personal Data Protection Challenges Regarding Monitoring of Employees – Implementing and Audit of the Codes of Conduct – v. 1.0*, pp. 27-53.
289. Szpunar, A. (1979), Ochrona Dóbr Osobistych. Warszawa: PWN.
290. Szubert, W. (1971) ‘Funkcje Prawa Pracy’, *Państwo i Prawo*, 1971/3-4, pp. 567-583.
291. Szubert, W. (1972) *Zarys Prawa Pracy*. Warsaw: PWN.
292. Tatár, I. (2021) ‘A munkahelyi alkohol-ellenőrzés egyes kérdései’, Munkajog, 2021/4, pp. 68-79.

293. Taylor, F. W. (1911)(1919) *The Principles of Scientific Management.* New York and London: Harper & Brothers Publishers.
294. Ter Haar, B.P. (2025) 'The law of good technology' in Gersdorf, M. and Maniewska, E. (eds.) *Prawo Pracy Wobec Nowych Technologii*. Warsaw: Wolters Kluwer, pp. 47-64.
295. Thompson E. P. (1967) 'Time, Work-Discipline, and Industrial Capitalism', *Past & Present,* 38(1), pp. 56-97.
296. Tökés, R. (1996) 'Political Transition and Social Transformation in Hungary', *Revista CIDOB d'Afers Internacionals,* 34/35, pp. 79-101.
297. Tóth, G.A. (2003) 'Az Emberi Méltósághoz Való Jog És Az Élethez Való Jog' in Halmai, G. and Tóth, G.A. (eds.) *Emberi Jogok*. Budapest: Osiris Kiadó, pp. 255-361.
298. Tóth, I. (1956) 'A munkajogviszony elhatárolása a megbízási jogviszonytól', *JOGTUDOMÁNYI KÖZLÖNY Az Állam- és Jogtudományi Intézet folyóirata*, 1956/XI, pp. 219-230.
299. Trykhlib, K. (2020) 'The Principle of Proportionality in the Jurisprudence of the European Court of Human Rights' in Duić, D., Petrašević, T. (eds.) *EU and Comparative Law Issues and Challenges Series*, 2020/4. Osijek: Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek, pp. 128-154.
300. Trzyniec, K. (2017) 'Monitorowanie stanów emocjonalnych pracownika za pomocą interfejsów mózg – komputer', *Bezpieczeństwo Pracy,* 2017/12, pp. 23-25.
301. Van Oort, M. (2018) 'The Emotional Labour of Surveillance: Digital Control in Fast Fashion Retail', *Critical Sociology,* 45(7-8), pp. 1-13.
302. Varga, D. (2019) 'Az adatvédelem és a munkáltatói ellenőrzés kérdései a XXI. századi munkaviszonyok tükrében (The Questions of the Data Protection and the Employer's Right to Control in View of the 21st Century's Employment Relationships)', *Miskolci Jogtudó,* 2019/1, pp. 81-89.
303. Varošanec, I. (2022) 'On the Path to the Future: Mapping the Notion of Transparency in the EU Regulatory Framework for AI', *University of Groningen Faculty of Law Research Paper Series*, 2022/18, pp. 1-25.
304. Veneziani, B. and Hepple, B. (2009) 'Introduction' in Hepple, B. and Veneziani, B. (eds.) *The transformation of labour law in Europe*. Oxford: Hart, Bloomsbury, pp. 1-29.
305. Wachter, S., Mittelstadt, B. and Floridi, L. (2017) 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law*, 7(2), pp. 76-99.
306. Walczak-Duraj, D. (2013) 'Czy konieczny nowy paradygmat w humanizowaniu pracy i stosunków pracy?', *Humanizacja Pracy*, 273(3), pp. 9-26.
307. Wank, R. (2004) 'Diversifying Employment Patterns – the Scope of Labor Law and the Notion of Employees', *JILPT Comparative Labor Law Seminar (9-10 March 2004)*, pp.137-143.
308. Warren, S. D. and Brandeis, L. D. (1890) 'The Right to Privacy', *Harvard Law Review*, 4(5), pp. 193-220.
309. Warren, S., Brandeis, L. (1890) 'The Right to Privacy', *Harvard Law Review*, IV(5), pp. 193-220.
310. Wąż, P. (2008) 'Kontrola osobista pracownika', *Atest,* 2008/1, p. 4-6.
311. Weiss, M. (2011) 'Re-Inventing Labour Law?', in: Davidov, G. and Langille, B. (eds.) *The Idea of Labour Law*. Oxford: Oxford University Press.
312. Westin, A. (1967)(2018) *Privacy and Freedom*. New York: Ig Publishing.

313. Wilejczyk, M. (2009) ‘Wolność Ducha Jako Podłoże Zjawisk Prawnych - Heglowskie Określenie Prawa’, *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, 2008/78, pp. 11-21.
314. Wood, A.J. (2021) *Algorithmic Management Consequences for Work Organisation and Working Conditions*. Seville: European Commission.
315. Wujczyk, M. (2012) *Prawo pracownika do ochrony prywatności*. Warsaw: Wolters Kluwer/LEX.
316. Wujczyk, M. (2012), *Prawo pracownika do ochrony prywatności*. Warsaw: Wolters Kluwer/LEX.
317. Wyka, T. (2025) ‘Art. 207’ in: Baran, K. W. (ed.) *Kodeks pracy. Komentarz. Tom II. Art. 94–304(5)*, Warsaw: Wolters Kluwer/LEX.
318. Zannoni, D. (2018) ‘GPS Surveillance for the Perspective of the European Convention on Human Rights’, *European Criminal Law Review*, Vol. 8, pp. 294-312.
319. Zieliński, T. (1986) *Prawo Pracy – Zarys systemu – Część I. Ogólna*. Warsaw-Cracow: PWN.
320. Ziółkowska, K. (2013) ‘Dopuszczalność kontroli osobistej pracownika a obowiązek dbałości o dobro zakładu pracy’, *Studia Prawnoustrojowe,* 2013/20, pp. 131-142.
321. Zofcinova, V. (2015) ‘Redefining of Dependent Work and Its Socio-Legal Dimension in Slovak Republic’, *European Scientific Journal*, 2015/1, pp. 45-53.
322. Żołyński, J. (2023) *Kontrola trzeźwości pracowników. Art. 22(1c)–22(1g) Kodeksu pracy. Komentarz.* Warsaw: Wolters Kluwer.
323. Zuboff, S. (2019) *The Age of Surveillance Capitalism – The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs; Mirosławski, T. 2023a, p. 4.
324. Žuľová, J. and Švec, M. (2018), *GDPR a ochrana záujmov zamestnanca*, Bratislava: Friedrich Ebert Stiftung.
325. Žuľová, J. et al. (2018) *Spracúvanie osobných údajov zamestnanca podľa GDPR (Analýza GDPR na pracovisku)*. Košice: Pavol Jozef Šafárika University in Košice.
326. Žůrek, J. (2017), *Praktický průvodce GDPR*. Olomouc: ANAG.

Legislation

International and European law:

1. Charter of Fundamental Rights of the European Union of 18 December 2000, 200/C 364/01.
2. Consolidated Version of the Treaty on European Union of 26 October 2012, C 326/13.
3. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981.
4. Directive (EU) 2022/2041 of the European Parliament and of the Council of 19 October 2022 on adequate minimum wages in the European Union.
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Offcial Journal L 281.
6. European Convention on Human Rights, as amended by Protocols Nos. 11, 14 and 15, ETS No. 005.
7. European Social Charter (revised) of 3 May 1996, ETS No. 163.
8. International Covenant on Economic, Social and Cultural Rights of 16 December 1966.
9. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data adopted on 18 May 2018 (Convention 108+).

10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
11. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
12. Treaty of Peace of Versailles of 28 June 1919.
13. Universal Declaration of Human Rights of 10 December 1948.

International and European official documents without legal force:

1. Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014.
2. Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, Adopted on 16 May 2011.
3. Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, 2017.
4. Article 29 Data Protection Working Party, Working document on the surveillance of electronic communications in the workplace, 29 May 2002, 5401/01/EN/Final WP 55.
5. Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 223.
6. Council of the European Union, 2008, Report of the Mission for Flexicurity, 17047/1/08 REV 1.
7. European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*, COM(2012) 9 final, 2012.
8. European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, 2010.
9. Explanations relating to the Charter of Fundamental Rights (2007/C 303/02).
10. Explanatory Memorandum to Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment.
11. Opinion 2/2017 on data processing at work, 8 June 2017, 17/EN WP 249.
12. Opinion 8/2001 on the processing of personal data in the employment context, 13 September 2001, 5062/01/EN/Final WP 48.
13. Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the Processing of Personal Data in the Context of Employment, 1 April 2015.
14. Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes, 18 January 1989.
15. The ILO Code of Practice on the protection of workers' personal data. Geneva: International Labour Office, 1997.

National law:

1. Act on Laboratory Medicine of 15 September 2022, Dz.U.2023.2125.
2. Constitution of the Republic of Poland of 2nd April 1997 no. 78 item 483.
3. Constitution of the Slovak Republic of 1 September 1992, 460/1992 Zb.
4. Czech Act 65/2017 on the Protection of Health from the Harmful Effects of Addictive Substances (Zákon č. 65/2017 Sb. - Zákon o ochraně zdraví před škodlivými účinky návykových látek).
5. Czech Act of 3 February 2012, the Civil Code, 89/2012 Sb.
6. Czech Charter of Fundamental Rights and Freedoms of 16 December 1992 (Const. act No. 2/1993 Coll. as amended by constitutional act No. 162/1998 Coll.)
7. Czech LABOUR CODE (full translation) No. 262/2006 Coll., as amended "Zákoník práce".
8. Fundamental Law of Hungary of 25 April 2011.
9. Hungarian Act CXXXIII of 2005 on the rules for the protection of persons and property and the activity of private detectives (2005 évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól).
10. Hungarian Act I of 2012 on the Labor Code (version before the amendment of 2019 Act XXXIV on the amendments necessary for the implementation of the European Union reform on data protection).
11. Hungarian Act I of 2012 on the Labor Code.
12. Hungarian Act LIII of 2018 on the protection of privacy.
13. Hungarian Act on information self-determination right and information freedom (2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról).
14. Hungarian Act V of 213 on the Civil Code.
15. Hungarian Act XCIII on Occupational Safety (1993. évi XCIII. törvény a munkavédelemről).
16. Hungarian Act XCIII on Occupational Safety (1993. évi XCIII. törvény a munkavédelemről).
17. Hungarian Act XXII of 1992 on the Labour Code.
18. Hungarian Act XXXIV of 2019 on the amendments necessary for the implementation of the European Union reform on data protection (hereinafter: Enforcing Act).
19. Polish Act of 1 December 2022 on the amendment of the Labour Code and certain other acts, Dz.U.2023.240.
20. Polish Act of 10th May 2018 item 1781 on personal data protection.
21. Polish Act of 26 June 1974 Dz.U.2023.1465 Labour Code.
22. Polish Act of 5 November 2025 on collective labour agreements and collective agreements, Dz.U.2025.1661.
23. Polish Act on the Protection of Persons and Property of 22 August 1997 (Ustawa o Ochronie Osób i Mienia, Dz.U.2025.532).
24. Polish Act on Upbringing in Sobriety and Counteracting Alcoholism of 26 October 1982, Dz.U.2023.165.
25. Polish Act on Upbringing in Sobriety and Counteracting Alcoholism of 26 October 1982, Dz.U.2023.2151.
26. Polish Civil Code (Dz. U. 1964 Nr 16 poz. 93).
27. Polish Regulation of the Minister of Health and the Minister of Internal Affairs and Administration of 28 December 2018 on testing for alcohol content in the body, Dz.U.2018.2472.

28. Regulation of the Minister of Health of 16 February 2023 on testing for the presence of alcohol or substances similar to alcohol in the organism of an employee, Dz.U.2023 poz.317 (Rozporządzenie Ministra Zdrowia z dnia 16 lutego 2023 r. w sprawie badań na obecność alkoholu lub środków działających podobnie do alkoholu w organizmie pracownika, Dz.U.2023 poz.317 (Regulation of the Minister of Health of 16 February 2023 on testing for the presence of alcohol or substances similar to alcohol in the organism of an employee, Dz.U.2023 poz.317).
29. Slovak Act of 2 February 2006 on Occupational Health and Safety, 124/2006 Z. z.
30. Slovak Civil Code (Občiansky zákonník, 40/1964 Zb.).
31. Slovak Labour Code, Act 311/2001 Coll.
32. Slovak Persona Data Act, Act 18/2018 Coll.
33. The Statute of Laborers from 1351.

National official documents without legal force:

1. 7001/2005. (MK 170.) FMM-PM együttes irányelv a munkavégzés alapjául szolgáló szerződések minősítése során figyelembe veendő szempontokról (2005).
2. Justification for the government's draft act amending the Labour Code and other acts, print number 2335 (Uzasadnienie rządowego projektu ustawy o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw, druk nr 23335).
3. T/4479. számú törvényjavaslat az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról (2019).
4. T/4786. számú törvényjavaslat a Munka Törvénykönyvéről.

Jurisprudence

ECtHR:

1. Grand Chamber of the ECtHR judgement in Bărbulescu v. Romania from 5 September 2017, 61496/08.
2. ECtHR judgment in S. and Marper v. the United Kingdom from 4 December 2008, 30562/04 and 30566/04.
3. ECtHR judgment in case Gorzelik and Others v. Poland from 17 February 2004, 44158/98.
4. ECtHR judgment in Antović and Mirković v Montenegro from 28 November 2017, 70838/13.
5. ECtHR judgment in *Florindo de Almeida Vasconcelos Gramaxo v. Portugal* from 13 December 2022, 26968/16.
6. ECtHR judgment in case of Dudgeon v. the United Kingdom from 22 October 1981, (7525/76).
7. ECtHR judgment in Tyrer v. the United Kingdom from 25 April 1978, 5856/72.
8. ECtHR judgment in Niemietz v. Germany from 16 December 1992, 13710/88.
9. ECtHR judgment in Halford v. the United Kingdom from 25 June 1997, 20605/92.
10. ECtHR judgment of 25 September 2001, *P. G. and J. H. v the United Kingdom*, Application No.44787/98;
11. ECtHR judgment Lopez Ribalda and Others v Spain from 17 October 2019, 1874/13 and 8567/13.
12. ECtHR decision in Madsen v. Denmark from 7 December 2002, 58341/00.
13. ECtHR decision in Madsen v. Denmark from 7 December 2002 (Application No. 58341/00); ECtHR decision in Wretlund v. Sweden from 9 March 2004, 46210/99.

14. ECtHR judgment in Odièvre v. France from 13 February 2003, 42326/98.
15. ECtHR judgment in Perry v the United Kingdom from 17 July 2003, 63737/00.
16. ECtHR judgment in Copland v. the United Kingdom from 3 April 2007, 62617/00.
17. ECtHR judgment in Evans v. the United Kingdom from 10 April 2007, 6339/05.
18. ECtHR judgment in *Peev v. Bulgaria* from 26 October 2007, 64209/01.
19. ECtHR decision in Köpke v Germany from 5 October 2010, 420/07.
20. ECtHR judgment in Von Hannover v Germany (no. 2) 7 February 2012, 40660/08.
21. ECtHR judgement in Michaud v. France from 6 March 2013, 12323/11.
22. ECtHR judgment in Fernández Martínez v Spain from 12 June 2014, 56030/07.
23. ECtHR judgement in Bărbulescu v. Romania from 12 January 2016, 61496/08.
24. ECtHR judgment in Denisov v Ukraine from 25 September 2018, 76639/11.
25. ECtHR judgment in Herbai v. Hungary from 5 February 2020, 11608/15.

CJEU:

1. CJEU: Case C-101/01, 2003.
2. CJEU: Case F-46/09, 2011.
3. CJEU: Joint Cases C-465/00, C-138/01 and C-139/01, 2003.
4. CJEU:(C-275/06), 2008.

National Supreme Courts:

1. Judgement of the Czech Supreme Court of 07 August 2014, 21 Cdo 747/2013.
2. Judgement of the Czech Supreme Court of 16 August 2012, 21 Cdo 1771/2011.
3. Judgement of the Czech Supreme Court of 17 October 2012, 21 Cdo 2596/2011.
4. Judgment of the Czech Supreme Court of 19 December 2016, 21 Cdo 4733/2015.
5. Judgment of the Czech Supreme Court of 20 March 2017, 21 Cdo 1043/206.
6. Judgment of the Czech Supreme Court of 21 January 2014, 21 Cdo 1496/2013.
7. Judgment of the Czech Supreme Court of 7 May 2003, 21 Cdo 2172/2002.
8. Judgment of the Polish Supreme Court of 11 March 1986, I CR 4/86.
9. Judgment of the Polish Supreme Court of 13 April 1972, I PR 153/72.
10. Judgment of the Polish Supreme Court of 13 April 2016, II PK 81/15.
11. Judgment of the Polish Supreme Court of 16 January 1976, II CR 692/75.
12. Judgment of the Polish Supreme Court of 18 January 1984, I CR 400/83.
13. Judgment of the Polish Supreme Court of 22 September 2020, I PK 126/19.
14. Judgment of the Polish Supreme Court of 23 July 1987, I PRN 36/87, OSNC 1989/2, Item 32.
15. Judgment of the Polish Supreme Court of 25 November 2005, I UK 68/05.
16. Judgment of the Polish Supreme Court of 26 October 2001, V CKN 195/01.
17. Judgment of the Polish Supreme Court of 4 December 2018, I PK 194/17, OSNP 2019/6, item 73.
18. Judgment of the Polish Supreme Court of 5 April 2002, II CKN 953/00.
19. Judgment of the Polish Supreme Court of 7 March 2006, I UK 127/05.
20. Judgment of the Polish Supreme Court of 7 September 1999, I PKN 277/99.
21. Judgment of the Polish Supreme Court of 9 July 2009, II PK 311/08.
22. Judgment of the Slovak Supreme Court of 18 February 2010, 3 Cdo 137/2008.
23. Judgments of the Polish Supreme Court of 7 March 2006, I PK 146/05.
24. Resolution of the Polish Supreme Court of 14 December 1978, V PZP 7/78, OSNC 1979/2, Item 21.
25. Ruling of the Polish Supreme Court of 12 May 2025, I PSK 132/24.

26. Ruling of the Slovak Supreme Court of 12 September 2016, n. 3Cdo/233/2015.
27. The Hungarian Supreme Court decision (Kúria/Curia), BH2006.64.
28. The Hungarian Supreme Court decision (Kúria/Curia), EBH2000. 296.
29. The Hungarian Supreme Court decision (Kúria/Curia), Mfv. 10.397/2018/2., BH 2020. 48.
30. The Hungarian Supreme Court judgement (Kúria/Curia), Mfv. 10.469/2013/4.
31. The Hungarian Supreme Court judgment (Kúria/Curia), Mfv.X.10.281/2019/4.
32. The Hungarian Supreme Court judgment (Kúria/Curia), Mfv.I.10.427/2016/4.
33. The Hungarian Supreme Court judgment (Kúria/Curia), Mfv.VIII.10.091/2023/7.
34. The Hungarian Supreme Court judgment of (Kúria/Curia), BH 2001.2.61.
35. The Hungarian Supreme Court resolution (Kúria/Curia), MK no. 122.

Constitutional Courts and Tribunals:

1. Decision of Hungarian Constitutional Court (Alkotmánybíróság), 36/2005.(X.5.).
2. Decision of the Hungarian Constitutional Court, 1115/B/1995. AB.
3. Decision of the Hungarian Constitutional Court, 35/2002. (VII. 19.).
4. Decision of the Slovak Constitutional Court of 26 March 2015, II. ÚS 191/2015.
5. Decision of the Slovak Constitutional Court of 28 October 2014, PL. ÚS 24/2014.
6. Judgment of the Constitutional Tribunal of 18 June 2018, SK 19/17.
7. Judgment of the Czech Constitutional Court of 1 March 2000, II. ÚS 517/99.
8. Judgment of the Czech Constitutional Court of 12 October 1994, PL. ÚS 4/94.
9. Judgment of the Czech Constitutional Court of 20 May 2002, IV. ÚS 315/01.
10. Judgment of the Czech Constitutional Court of 22 March 2011, Pl. ÚS 24/10.
11. Judgment of the Czech Constitutional Court of 27 February 2019, IV. ÚS 774/18.
12. Judgment of the Czech Constitutional Court of 8 June 2010, Pl.ÚS 3/09.
13. Judgment of the Czech Supreme Court of 16 August 2012, 21 CDO 1771/2011.
14. Judgment of the Hungarian Constitutional Court, 11/2014. (IV. 4.) AB.
15. Judgment of the Hungarian Constitutional Court, 15/1991. (IV. 13.) AB.
16. Judgment of the Hungarian Constitutional Court, 30/1992. (V. 26.) AB.
17. Judgment of the Hungarian Constitutional Court, 30/2015. (X. 15.) AB.
18. Judgment of the Hungarian Constitutional Court, 3046/2016. (III. 22.) AB.
19. Judgment of the Hungarian Constitutional Court, 32/2013. (XI. 22.).
20. Judgment of the Hungarian Constitutional Court, 46/1995. (VI. 30.) AB.
21. Judgment of the Hungarian Constitutional Court,15/1991. (IV.13.).
22. Judgment of the Polish Constitutional Tribunal 11 October 2016, SK 28/15.
23. Judgment of the Polish Constitutional Tribunal 26 April 2018, K 6/15.
24. Judgment of the Polish Constitutional Tribunal of 12 November 2002, SK 40/01.
25. Judgment of the Polish Constitutional Tribunal of 14 October 2015, Kp. 1/15.
26. Judgment of the Polish Constitutional Tribunal of 19 May 1998, U 5/97.
27. Judgment of the Polish Constitutional Tribunal of 20 January 2015, K 39/12.
28. Judgment of the Polish Constitutional Tribunal of 24 June 1997, K 21/96.
29. Judgment of the Polish Constitutional Tribunal of 24 June 1998, U 4/97.
30. Judgment of the Polish Constitutional Tribunal of 25 May 2016, Kp 5/15.
31. Judgment of the Polish Constitutional Tribunal of 26 April 2018, K 6/15.
32. Judgment of the Polish Constitutional Tribunal of 30 October 2006, File ref. P 10/06.
33. Judgment of the Polish Constitutional Tribunal of 5 March 2013, U 2/11.
34. Judgment of the Slovak Constitutional Court of 13 May 1997, II. ÚS 19/97.
35. Judgment of the Slovak Constitutional Court of 29 November 1995, I. ÚS 33/95.

36. Judgment of the Slovak Constitutional Court of 4 December 2007, PL. ÚS. 12/01.
37. Judgment of the Slovak Constitutional Court of 4 February 2009, I. ÚS 117/07.
38. Judgment of the Slovak Constitutional Court of 6 November 2014, II. ÚS 424/2012.
39. Judicial decision of the Constitutional Court of the Slovak Republic, I. ÚS 117/07 of 4 February 2009.
40. Judicial decision of the Constitutional Court of the Slovak Republic, I. ÚS 274/05 of 14 June 2006.
41. Resolution of the Czech Constitutional Court of 31 March 2009, I. ÚS. 452/09.

Other domestic courts:

1. Judgement of the Czech Supreme Administrative Court of 23 August 2013, 5 As 158/2012-49.
2. Judgement of the Polish Supreme Administrative Court of 13 February 2014, I OSK 2436/12.
3. Judgement of the Regional Court in Bratislava of 29 October 2012, n. 6Co/203/2012.
4. Judgment of the Court of Appeal in Lublin of 8 April 2020, III Apa 4/20, LEX nr 2978529.
5. Judgment of the Municipal Court in Prague, 6A 42/2013 - 48.
6. Judgment of the Regional Court in Bratislava from 16 January 2013, n. 4CoPr/1/2012 and n. 4CoPr/2/2012.

Decisions, guidelines and other documents issued by national and European data protection authorities and labour inspectorates:

1. A Nemzeti Adatvédelmi és Információszabadság Hatóság (2013), *Ajánlása a munkahelyen alkalmazott elektronikus megfigyelorendszer alapveto követelményeirol*.
2. A Nemzeti Adatvédelmi és Információszabadság Hatóság (2016) *Tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről*.
3. A Nemzeti Adatvédelmi és Információszabadság Hatóság, Decision NAIH/2017/439/H.
4. Az Adatvédelmi Biztos (1998) *Az Adatvédelmi Biztos Beszámolója*.
5. Bureau of the Inspector General for Personal Data Protection from Poland, Office for Personal Data Protection from the Czech Republic, Croatian Personal Data Protection Agency, Commission for Personal Data Protection from the Republic of Bulgaria (2012) *Privacy protection in the workplace. Guide for employees*.
6. European Data Protection Supervisor (2010), *The EDPS Video-Surveillance Guidelines*.
7. Nemzeti Adatvédelmi és Információszabadság Hatóság, Decision in case NAIH-2732-2/2023.
8. Státní Úřad Inspekce Práce (2019) *Ochrana Osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele*. Opava: SUIP.
9. The European Data Protection Board (2020) *Guidelines 3/2019 on processing of personal data through video devices, Version 2.0.*
10. Úřad pro ochranu osobních údajů (2009) *Stanovisko č. 2/2009 - Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*.
11. Úřad pro ochranu osobních údajů (2024) *Metodika k Návrhu a Provozování Kamerových Systémů z Hlediska Zpracování a Ochrany Osobních Údajů.*
12. Urząd Ochrony Danych Osobowych (2018a) *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców. Poradnik RODO.*

13. Urząd Ochrony Danych Osobowych (2018b) *Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego*.
14. Urząd Ochrony Danych Osobowych, Opinia 138/1076.

Internet sources:

1. Balousová, M. (2017) *Je alkohol na pracovišti vždy důvodem k výpovědi?* [Online]. Available at: https://www.epravo.cz/top/clanky/je-alkohol-na-pracovisti-vzdy-duvodem-k-testimony-105684.html (Accessed 3 May 2026).
2. Belltechlogix, *The Importance of Creating a Bring-Your-Own-Device Strategy* [Online]. Available at: https://belltechlogix.com/bring-your-own-device-strategy/ (Accessed: 3 May 2026).
3. Cambridge dictionary, *"monitoring"* [Online]. Available at: https://dictionary.cambridge.org/dictionary/english/monitor?q=monitoring (Accessed: 3 May 2026).
4. Cambridge dictionary, *"surveillance"* [Online]. Available at: https://dictionary.cambridge.org/dictionary/english/surveillance (Accessed: 3 May 2026).
5. Council of Europe, *Chart of signatures and ratifications of Treaty 108* [Online]. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 (Accessed 2 May 2026).
6. Dobosi, K. (2025) *Alkoholfogyasztás ellenőrzése a munkahelyen* [Online]. Available at: https://ado.hu/munkaugyek/alkoholfogyasztas-ellenorzese-a-munkahelyen/ (Accessed: 4 May 2026).
7. Drzewicka, E. (2013) *Obowiązki pracodawcy w zakresei ochorny danych osobowych pracownika* [Online]. Available at: https://www.prawo.pl/biznes/obowiazki-pracodawcy-w-zakresie-ochrony-danych-osobowych,194562.html (Accessed 3 May 2026).
8. European Commission, *Industry 5.0* [Online]. Available at: https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en?prefLang=da (Accessed: 5 May 2026).
9. European Data Protection Board, *Legacy: Art. 29 Working Party* [Online]. Available at: https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en (Accessed: 2 May 2026).
10. European Union Drugs Agency (2022) *Workpalces and drugs: health and social responses* [Online]. Available at: https://www.euda.europa.eu/publications/mini-guides/workplaces-and-drugs-health-and-social-responses_en (Accessed: 3 May 2026).
11. Fr. Popiełuszko, J. (1983) *Homily from 24 April 1983* [Online]. Available at: https://biogramy.ipn.gov.pl/bio/wszystkie-biogramy/ksiadz-jerzy-popieluszk/kazania/108728,24-kwietnia-1983.html (Accessed: 5 May 2026).
12. Hendrickx, F. (2019b) *Privacy 4.0 at work: regulating employment, technology and automation* [Online]. Available at: https://legalblogs.wolterskluwer.com/global-workplace-law-and-policy/privacy-40-at-work-regulating-employment-technology-and-automation/ (Accessed: 5 May 2026).
13. Jouza, L. (2022) Ochrana osobnosti zaměstnance v pracovněprávních vztazích [Online]. Available at: https://web.archive.org/web/20240227130801/https://advokatnidenik.cz/2022/05/21/ochrana-osobnosti-zamestnance-v-pracovnepravnich-vztazich/ (https://advokatnidenik.cz/2022/05/21/ochrana-osobnosti-zamestnance-v-pracovnepravnich-vztazich/) (Accessed: 3 May 2026/27 March 2024).

14. Kaplan, E. (2015) *The Spy Who Fired Me – The Human Cost of Workplace Monitoring,* [Online]. Available at: https://harpers.org/archive/2015/03/the-spy-who-fired-me/ (Accessed: 5 May 2026).
15. Kessler, S. (2022) *Robots are replacing managers, too* [Online]. Available at: https://qz.com/1039981/robots-are-replacing-managers-too (Accessed: 5 May 2026).
16. Kolářová, K. (2017) *Většina stížností na nepřiměřené sledování v práci je oprávněná* [Online]. Available at: https://www.lidovky.cz/ceska-pozice/vetsina-stiznosti-na-neprimerene-sledovani-v-praci-je-opravnena.A171207_131049_pozice-tema_lube (Accessed: 3 May 2026).
17. Kyselková, K. (2013) *Kontrola věcí a prohlídky zaměstnanců prováděné zaměstnavatelem* [Online]. Available at: https://www.epravo.cz/top/clanky/kontrola-veci-a-prohlidky-zamestnancu-provadene-zamestnavatelem-90023.html (Accessed: 3 May 2026).
18. Leśniak, G. J. (2021) *Sąd stanął po stronie wolności słowa urzędnika państwowego* [Online]. Available at: https://www.prawo.pl/kadry/pracownik-zwolniony-za-wpisy-w-mediach-spolecznosciowych-jaki,508257.html (Accessed: 2 May 2026).
19. Metelka, J. (2024) *GPS na pranýři aneb sledování zaměstnanců* [Online]. Available at: *https://www.pravniprostor.cz/clanky/obcanske-pravo/gps-na-pranyri-aneb-sledovani-zamestnancu* (Accessed: 3 May 2026).
20. Michalski, B. (2022) *Dyscyplinarka dla pracownika Poczty Polskiej za wpisy pochwalające wojnę. Co na to eksperci?* [Online]. Available at: https://www.gazetaprawna.pl/praca/artykuly/8386055,poczta-polska-zwolnienie-dyscyplinarne-media-spolecznosciowe-wpis-wojna-w-ukrainie.html (Accessed: 2 May 2026).
21. Német, T. (2019) *Pert nyert az ügyész, akit három Facebook-posztja miatt rúgtak ki* [Online]. Available at: https://index.hu/belfold/2019/05/10/facebook_per_ugyesz_ugyeszseg_kirugas_itelet/?token=ec537fc4771e0f1a5fac51a7cefc3b19 (Accessed: 2 May 2026).
22. OECD Data Explorer, *Collective Bargaining Coverage* [Online]. Available at: https://data-explorer.oecd.org/vis?lc=en&df[ds]=dsDisseminateFinalDMZ&df[id]=DSD_TUD_CBC%40DF_CBC&df[ag]=OECD.ELS.SAE&dq=..&pd=2000%2C&to[TIME_PERIOD]=false&vw=tb (Accessed: 3 May 2026).
23. OECD Data Explorer, *Trade Union Density* [Online]. Available at: https://data-explorer.oecd.org/vis?tm=trade%20union&pg=0&snb=81&df[ds]=dsDisseminateFinalDMZ&df[id]=DSD_TUD_CBC%40DF_TUD&df[ag]=OECD.ELS.SAE&df[vs]=1.0&dq=..&ly[cl]=TIME_PERIOD&ly[rs]=REF_AREA&to[TIME_PERIOD]=false&lom=LASTNPERIODS&lo=10&vw=tb (Accessed: 3 May 2026).
24. OECD/AIAS ICTWSS Database, Trade Union Density Data [Online]. Available at: https://www.oecd.org/en/data/datasets/oecdaias-ictwss-database.html (Accessed: 4 May 2026).
25. Office for Personal Data Protection of the Slovak Republic, Frequently Asked Questions [Online]. Available at: https://dataprotection.gov.sk/en/legislation/guidelines-faq/frequently-asked-questions-faq/# (Accessed: 3 May 2026).
26. Palmer, A. (2021) *Amazon is using AI-equipped camers in delivery vans and some drivers are concerned about privacy* [Online]. Available at: https://www.cnbc.com/2021/02/03/amazon-using-ai-equipped-cameras-in-delivery-vans.html (Accessed: 5 May 2026).

27. Poczta Polska (2022), *Oświadczenie* [Online]. Available at: https://media.poczta-polska.pl/releases/oswiadczenie-2022-03-17 (Accessed: 2 May 2026).
28. Predotova, K. and Llave, O. V. (2021) *Workers want to telework but long working hours, isolation and inadequate equipment must be tackled* [Online]. Available at: https://www.eurofound.europa.eu/en/publications/all/workers-want-telework-long-working-hours-isolation-and-inadequate-equipment (Accessed: 4 May 2026).
29. Roose, K. (2019) *A Machine May Not Take Your Job, but One Could Become Your Boss* [Online]. Available at: https://www.nytimes.com/2019/06/23/technology/artificial-intelligence-ai-workplace.html (Accessed: 5 May 2026).
30. Rzeczpospolita (2024) *"Małpki" pod lupą* [Online]. Available at: https://www.rp.pl/przemysl-spozywczy/art40999491-malpki-pod-lupa (Accessed 3 May 2026).
31. Słownik języka polskiego, *"monitoring"* [Online]. Available at: https://sjp.pwn.pl/szukaj/monitoring.html (Accessed: 3 May 2026).
32. Słownik języka polskiego, *"nadzór"* [Online]. Available at: https://sjp.pwn.pl/szukaj/nadzór%20.html (Accessed: 3 May 2026).
33. Szymaniak, M. (2021) *Glovo jednym stuknięciem stłumiło strajk kurierów w Polsce. Praca jak z Black Mirror* [Online]. Available at: https://spidersweb.pl/plus/2021/05/kurierzy-glovo-strajk-protest-aplikacja-black-mirror (Accessed: 5 May 2026).
34. Vobořil, J. (2012) Nejvyšší Soud k možnostem utajeného sledování zaměstnanců [Online]. Available at: https://zpravodaj.genderstudies.cz/cz/clanek/nejvyssi-soud-k-moznostem-utajeneho-sledovani-zamestnancu (Accessed: 3 May 2026).
35. Vych, J. (2015) Navrhovaná změna v oblasti ochrany soukromí zaměstnanců [Online]. Available at: https://www.epravo.cz/top/clanky/navrhovana-zmena-v-oblasti-ochrany-soukromi-zamestnancu-98803.html (Accessed: 3 May 2026).
36. Website of the Kronos producer: https://www.ukg.com (Accessed: 5 May 2026).
37. WHO indicators on pure alcohol consumption, litres per capita, age 15+ [Online]. Available at: https://gateway.euro.who.int/en/indicators/hfa_426-3050-pure-alcohol-consumption-litres-per-capita-age-15plus/#id=19443 (Accessed: 3 May 2026).
38. Wikipedia, *"employee monitoring"* [Online]. Available at: https://en.wikipedia.org/wiki/Employee_monitoring (Accessed: 3 May 2026).
39. Zemanová Šimonová, H. (2016) Právní Prostředky Ochrany Osobnosti Zaměstnance [Online]. Available at: http://www.bulletin-advokacie.cz/pravni-prostredky-ochrany-osobnosti-zamestnance (Accessed: 3 May 2026).

Statement

In accordance with the provisions of the Regulation on the Use of Artificial Intelligence of University of Miskolc and the Guidelines for the Use of Artificial Intelligence of the Deák Ferenc Doctoral School of Law, I, undersigned Tomasz Mirosławski (name), declare that I have used / ~~have not used~~ artificial intelligence in my doctoral dissertation and thesis booklets.

In the case of the use of artificial intelligence (hereinafter: AI), I declare the following:
1. The name of the AI tool used: DeepL Translator – Machine Translator; Grammarly: AI Writing Assistance and ChatGPT 5.5 – Large Language Model
2. The URL and the version number of the AI tool used: ,
, https://chatgpt.com.
3. The exact date of production of the generated content (year, month, day): I have been using these tools from approximately 2024 to 2026.
4. The purpose and extent of use (describing in detail which part of the dissertation and to what extent the use of AI affects, and for which sub-task the AI was used): These tools were used solely for the purpose of translating documents, legal texts and literature in foreign languages, as well as sections of my doctoral thesis. For translation, I primarily used the DeepL translator, supplemented by the full-document translation feature in ChatGPT. I used Grammarly to correct spelling mistakes and to carry out a final check of the thesis for such errors. The indicated AI tools were not used to generate the substantive content of the thesis.

I acknowledge that according to the Guidelines for the Use of Artificial Intelligence of the Deák Ferenc Doctoral School of Law, *„The use of AI is prohibited for the formulation of theses, research results, conclusions, inferences and analyses. Any thesis or paper prepared in this way is not admissible."*

Miskolc, 2026.08.24

....

signature