TECHNOLOGY VS PRIVACY AT WORK: THE EXTENT AND LIMITATIONS OF ORGANIZATIONAL CONTROL MECHANISMS

Zsófia Ásványi[*]

Received: 17. 6. 2022
Accepted: 1. 11. 2022
DOI https://doi.org/10.30924/mjcmi.27.2.14

Review
UDC 342.721
005.962:005.56

Abstract

Employees' right to privacy and employers' extensive need for work-related information collide. The imbalance of authority between employers and employees and the doctrine of managerial prerogative determines the outcome of these competing interests, and therefore the right to privacy requires statutory protection. The study aims to examine the legislative (hard law) and law enforcement (soft law) achievements of European and Hungarian initiatives on organizational labor control mechanisms and to understand their possible limitations concerning the doctrine of managerial prerogative. The research method was a thematic document and literature review of appropriate legislation and case law records from the European Court of Human Rights, the Hungarian Supreme Court, and the Hungarian National Authority for Data Protection and Freedom of Information. The research results confirmed our hypothesis: current legal instruments seem to limit the control mechanisms of organizations, both in terms of content and process. However, rapid technological innovations make employee privacy a moving target, where the law provides only temporary and limited protection.

Keywords: *employee privacy, work control mechanisms, the doctrine of the managerial prerogative, balance of interests*

1. INTRODUCTION

A sales employee set up a Yahoo Messenger account at his employer's request so he could answer customer inquiries. A few months later, the employer notified him that he was using the company's Internet for personal purposes, violating company rules, according to official monitoring. Because of the violation of internal rules, the employer terminated his contract. In another case, the employer summarily dismissed a supermarket cashier for theft. The employer's covert video surveillance uncovered the theft. University lecturers complained that the dean had introduced camera surveillance in the university's lecture halls. The professors argued that there was no legitimate reason for camera surveillance of lectures because there was no danger to the safety of people or property. Yet, they felt that the surveillance violated their privacy.

In these actual cases, described in more detail later in the text, the employer's right

* Zsófia Ásványi PhD, assistant professor, University of Pécs, Faculty of Business and Economics, Department of Leadership and Organizational Sciences, Hungary, 7622 Pécs, Rákóczi str. 80., Hungary, E-mail: asvanyizs@ktk.pte.hu

to be informed and the employee's right to privacy collided. Several theorists have also pointed out that the "right to be forgotten" (Gidron, Volovelsky, 2018) and the employee's right to privacy constantly collide with the employer's right to be informed due to the nature of the employment relationship (Workman, 2009; Foth et al., 2012; Ogriseg, 2017; Simitis, 1999).

The relationship between the employee's privacy and the employer's right to information is primarily analyzed by data protection experts, mainly from a legal perspective. The issue is rarely explored in management and leadership literature and remains in the legal sphere. Scholars and managers face the dilemma of whether employee privacy should be considered a separate legal issue or an integral part of management practices.

This study takes a multidisciplinary approach. The study explicitly presents a cross-section of data protection law, labor law, and the doctrine of the managerial prerogative. From a scholarly perspective, the article contributes to the development of business ethics by embedding the legal understanding of employee privacy in the doctrine of managerial prerogative.

By compiling and analyzing European and Hungarian legislation related to labor control mechanisms, as well as the case law of the European Court of Human Rights (ECtHR), the decisions of the Hungarian Supreme Court, and the recommendations of the Hungarian National Authority for Data Protection and Freedom of Information, this article contributes to the growth of knowledge in the following areas. First, it sheds light on the reason for the "data hunger" of organizations (van de Waerdt, 2020), which is rooted in the doctrine of managerial prerogative. Second, the study's integrative approach shows how data protection and labor law can contribute to fair labor control mechanisms in organizations. Third, the study highlights such procedures' limitations on managerial prerogative.

As problem-driven research (Reinecke et al., 2016.), this paper is designed to answer the following research questions:

RQ1: What is the underlying reason for the work-related "data hunger" of organizations?

RQ2: How can companies comply with European and Hungarian hard and soft data protection regulations when setting up work control mechanisms to protect and respect employee privacy?

RQ3: To what extent do these legitimate mechanisms of labor control constitute a limitation of the doctrine of the managerial prerogative in the European/Hungarian context to strike a balance between the interests of employers and employees in this way?

The paper tests a conceptual model that examines the impact of the European and Hungarian hard and soft elements of data protection law on employers' labor control mechanisms and, at the same time, on the managerial prerogative doctrine. The conceptual model is shown in Figure 1.

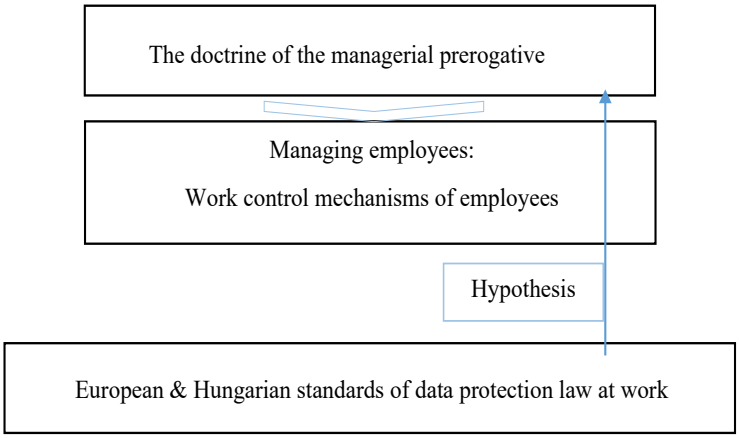

Figure 1. Conceptual model
Source: Author

Based on the research questions and the conceptual model, we have formulated the following hypothesis:

H1: The legally acceptable work control mechanisms create efficient limitations on the doctrine of the managerial prerogative in the European/Hungarian context.

The study did not aim to limit the term "employee" only to those with a contract of employment. Instead, it was intended to encompass all circumstances in which an employment relationship exists, whether based on an employment contract or a freelance activity.

2. METHODS

To test the conceptual model, a qualitative research design was used. To test the research hypothesis, the researcher used a thematic literature and document review approach that included all international, European, and Hungarian legislation and soft law practices related to worker control mechanisms.

In analyzing the relevant soft law, I monitored the decisions of the European Court of Human Rights (ECtHR), affiliated with the Council of Europe. Through a keyword search of the ECtHR's HUDOC database, I found seven relevant cases that I analyzed. The EU's Court of Justice practice resulted in two preliminary rulings relevant to workplace data protection (out of 10,500 until 2020), although none had to do with employee control procedures[1].

had to do with employee control procedures[1]. The soft law analysis for Hungary included the Hungarian Constitutional Court, the Hungarian Supreme Court, and the Hungarian National Authority for Data Protection and Freedom of Information (NAIH). I used the open-access search function of the official websites. In addition to one decision of the Hungarian Constitutional Court and three other court decisions, I found only one (MK 122) and three landmark decisions on the subject from the Supreme Court's colorful and numerous case law database. As an authority specializing in data protection, I found most of the decisions and recommendations in NAIH's practice: twenty out of the 271 posted on its website since 2012.

The analysis did not include areas of data protection at work, such as telecommuting, home office, employee biometrics, electronic documents, or platform work.

2.1. Data Protection Law at work

A considerable body of data protection literature provides an understanding of the evolutionary development of data protection law. As early as the very first study of the right to privacy by Warren & Brandeis in the columns of the Harvard Law Review in 1890 (Warren and Brandeis, 1890) contributed to the foundations of privacy law by outlining the "right to be left alone" (Stalla-Bourdillon, Phillips, Ryan, 2014). Later, Westin's epoch-making work (1967), Schoeman's anthology (1984), and Solove (2008) in the international context, as well as Jóri (2009), Majtényi (2006), and Sólyom (1983) in Hungary, provided offered normative discussions on privacy law.

The first data protection regulations date back to the 1970s and intended to provide citizens with protection from public, computerized (at least partially automated) records. Later, in the 1980s and 1990s, second-generation rules appeared, and not only automated, but also paper-based records were included in the regulation (Jóri, 2009). Thus, the third-generation rules emerged, which, according to Hegedűs (2013), will be followed by the fourth generation of regulation, which, in his view, will be characterized by self-regulation and the emergence of the individual's "right to disconnect." Like many other categorizations, the boundaries of data protection eras should be carefully considered. According to Szőke (2013), it is more important to understand the main achievements of each regulation than to create categories.

The United Nations (UN) and its body, the International Labour Organization (ILO), developed considerable achievements in data protection. In 1990, the UN adopted the Guidelines for the Regulation of Computerized Personal Data Files (Resolution 45/95 (A/RES/45/95). Also in 2013, the UN General Assembly adopted a Resolution on the right to privacy in the digital age (A/RES/68/167), while the ILO itself issued a Code of Practice on the Protection of Workers' Personal Data

[1] In the *Lindqvist case* (2003), the Court ruled that if personal data that clearly identify individuals are posted on the Internet, it means "processing of personal data in part or in full by automated means", but it is not described as „transfer to a third country". In this specific case, a Swedish volunteer uploaded the personal data of other volunteers to the Internet. Related to the Worten case (2013), the Court classified employees' working time data as personal data. It also stated that the employer, as the controller of personal data, must pro-vide immediate access of working time records to the national authorities responsible for monitoring working conditions.

("ILO Code of Practice") in 1997. The code has no binding force. It recommends developing laws, regulations, collective agreements, and company-specific policies regarding collecting, storing, using, and disclosing workers' data.

A particular branch of data protection law has emerged from the Council of Europe. Beyond the protection of "private and family life, home and correspondence" in Article 8 of the European Convention on Human Rights (ECHR, 1963), the Council of Europe Data Protection Convention 108 (1981) was the main data protection document and, until 1995, the only binding source of international law.

The European Union was relatively late in committing to data protection legislation compared to other international organizations and missed the first wave of the regulation (Bankó & Szőke, 2016). When the OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980, revised in 2013) and the Convention 108 of the Council of Europe were adopted in 1980, the prevailing view in the EU was that joining the Convention would solve the problem of harmonizing Community law. Finally, Directive 95/46/ EC on the protection of individuals concerning the processing of personal data and on the free movement of such data was adopted in 1995 (Data Protection Directive, DPD). Most international and Hungarian researchers have recognized the results of the directive (Korff, 2002; Jay & Hamilton, 1999; Jóri, 2009). It established the basic concepts of a global digital society and did not distinguish between public and private data controllers in terms of applicability (beyond the state, the "Big Brother," the data hunger of the corporate sector, the "Little Brother," has also increased). Its scope included both automated and manual data management. However, it was challenging to build the future of privacy law on a directive that rested on the dogmatic foundations of the late 1980s.

Some twenty years ago, when the EU Member States signed the Charter of Fundamental Rights at the Nice Summit in 2000, the freedom to protect personal data was regulated as an independently designated fundamental right (Article 8). The status of data protection law was further strengthened within the EU when the Treaty of Lisbon (2009) made the Charter of Fundamental Rights binding and gave direct protection to personal data protection.

The right to "informational self-determination" was emphasized among the second-generation data protection provisions. This meant that data subjects could decide whether to share their data with other individuals or organizations. Informational self-determination was the focus of numerous publications in Hungary (Szőke, 2013; Balogh, 2011; Majtényi, 2010; Jóri, 2009). The term was part of the German constitutional jurisprudence and was initially called "informationelle Selbstbestimmung." Popular and much quoted is the account of the term by Mayer-Schönberger (1997: 232) when he argues that data protection based on the right to informational self-determination has turned out to be a *"toothless paper tiger,"* a *"toy of the upper middle class."* He insightfully describes the situation where the consent of the data subject (individual) is the primary legal basis for processing personal data. Due to the dominant position of data controllers, this way remained largely a privilege of minorities, who could economically and socially afford to exercise their rights. In contrast, the desired extensive self-determination of one's informational self-image remained a political rhetoric (Mayer-Schönberger, 2001: 232).

EU data protection reform, a forerunner of third-generation regulation, became

urgent in 2012. Global data sharing and collection increased unprecedentedly, making it more common for individuals to make personal data publicly available. Due to the reform, the GDPR Regulation (Regulation EU 2016/679) on "The protection of individuals concerning the processing of personal data and on the free movement of such data" entered into force in all member states on 25 May 2018.

Although the "Key Provisions" subgroup established by Article 29 of the former DPD(95/46/ EC) is no longer used to any significant extent, its work continues to have a significant impact on work-related data processing (Article 29 Data Protection Working Party, 2017; Article 29 Data Protection Working Party, 2014). The elements of international data protection law currently in force are listed in Table 1.

Table 1. International sources of law related to data protection at work

UN & ILO	**Council of Europe**	**European Union**
Guidelines for the Regulation of Computerized Personal Data Files	European Convention of Human Rights (ECHR, 1950)	Treaty on the Functioning of the European Union (TFEU) Article 16.
Resolution no. 68/167 on the right to privacy in the digital age	Revised Data Protection Convention 108 (2015)	Charter of Fundamental Charter Articles 7 & 8.
Code of Practice on the Protection of Workers' Personal Data ("the ILO Code of Practice")	Recommendation 5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (2015)	Article 29 Data Protection Working Party Opinions
		2016/679 GDPR Regulation and its Article 88.

Source: Author

The first reference to the legal protection of personal data in Hungary dates to 1977 (Civil Code of the communist regime - Act IV of 1959 Section 83). It guaranteed that computerized data processing should not violate the rights of individuals and that such data should be disclosed only to the authorized body or person. It also stated the right of the data subject to rectification.

With the regime change in 1989, the protection of personal data and the disclosure of data of public interest were included in the Constitution. In 1992, the Act on the protection of personal data and the disclosure of data of public interest (Act LXIII of 1992, from now on: Avtv.) and the market-based Labor Code (Act XXII of 1992, from now on: Old Mt.) entered into force. At that time, the Data Protection Commissioner oversaw the enforcement of data protection regulations. The year 2012 marked a turning point when both laws were repealed. The Avtv. was replaced by Act CXII of 2011 (Act on the Right to informational self-determination and freedom of information, from now on: Infotv.), and the Act I of 2012 (Labour Code) "retired" the old Mt. after about twenty years. Infotv. abolished the ombudsman

system and established the National Authority for Data Protection and Freedom of Information (from now on: NAIH) as a supervisory body. The Hungarian legal framework for protecting work-related data is shown in Table 2.

Table 2. Legal sources and authorities of data protection at work in Hungary

Before 2011	After 2011
Hungarian Constitution	
Avtv (Act LXIII of 1992)	Infotv (Act CXII of 2011)
Labour Code (Act XXII of 1992)	Labour Code (Act I of 2012)
Data Protection Ombudsman	National Data Protection and Freedom of Information Authority (NAIH)

Source: Author

2.2. Case law

The general aim of this section is to present the data protection cases related to labor control mechanisms that have fallen under the jurisdiction of European and Hungarian law enforcement authorities.

The ECtHR is an essential bastion of data protection. In recent years, it has acted in several cases involving monitoring workers' behaviour in the employment context, which have received a strong international echo. The ECtHR's rulings are analyzed later in the paper, and the main findings are summarised in Table 3 below.

Table 3. ECtHR decisions and their significance related to data protection at work

Case	Year	Significance of judgment
Halford v UK	1997	The employer is not entitled to eavesdrop on the employee's office or private telephone without prior notice.
Copland v UK	2007	E-mails and information resulting from the monitoring of Internet use fall under and are protected by Article 8 of ECHR.
Bărbulescu v Romania	2017	The employer has an accepted and recognized right to inspect the employee and access the employment data stored on the computer. Legal condition: Bărbulescu-test. The employee's privacy cannot be verified even if the employer has expressly prohibited using private assets.
Libert v France	2018	Principle of purpose: all employer monitoring measures must be related to the aim and purpose of the employment relationship. The employer is only entitled to check the employee's data if it is explicitly marked as "private" in the presence of the employee, also taking into account the principle of purpose.
Köpke v Germany	2010	In the case of camera surveillance, the employer must demonstrate a legitimate reason to use the camera.
López Ribalda and Others v Spain	2019	Extension of Bărbulescu-test to video surveillance of employees.
Antović and Mirković v Montenegro	2018	The "private life" concept must be interpreted broadly to include the right to lead a private social life at work.

Source: Author

Table 4 provides a catalog of workplace data management situations, pieces of soft law, and the issuer of the decision I examined related to the employer's control mechanism and measures on employees in Hungary.

Table 4. Hungarian soft law related to data protection at work

Employer's control mechanism	The issuer of soft law	Case number
Camera surveillance	NAIH / Data Protection Ombudsman	NAIH/2019/2466 NAIH/2018/2466/2/K NAIH/2018/3295/H NAIH/2015/3355/H NAIH-1941/2013/H NAIH-4001-6/2012/V 1805/A/2005–3 ABI–97/2010/P
	Supreme Court	EBH 296/2000
	Constitutional Court	36/2005. (X. 5.) CC decision
Supervision of work e-mails	NAIH / Data Protection Ombudsman	NAIH/2019/769 NAIH/2019/51/11 879/A/2005–3
Supervision of work laptop	NAIH	NAIH/2015/1402/H NAIH-421-19/2013/H.
Supervision of work telephone	Supreme Court	SC Mfv.I.10.397/2018.
Monitoring Internet use during working hours		BH2006. 64
Monitoring vehicles used by employees	NAIH / Data Protection Ombudsman	NAIH-42-6/2013/V 1664/A/2006–3
Use of alcohol and drug testing at work	Supreme Court	MK 122. resolution LB Mfv.I. 10.939/1999 EBH 1999/47. BH2006. 64. BH2000. 432. ABI–687/2010/K

Source: Author

3. RESULTS

First, we discuss the potential impact of data protection (hard law) legislation on the work control mechanisms of employees. Data protection legislation of the UN and the ILO operated with guidelines and a code of conduct (with recommendations for the development of national legislation, collective agreements, and company policies), but none with binding legal force. The most influential Council of Europe documents are the ECHR Convention and the Data Protection Convention, both of which are binding under international law (see Table 1), meaning that they must be ratified (implemented into the national legal system) by member states. European data protection legislation within the* framework of the European Union and the Council of Europe has developed in parallel, yet harmoniously, over the past decades. As a result of legal developments, the EU's primary and secondary legislation and the Council of Europe's binding and non-binding legal instruments now provide a horizontal framework for data protection that covers all relevant areas of life, including employment, without specific European labor law provisions. The EU's main piece of legislation, the GDPR Regulation, is directly applicable and affects member states' laws. Its Article 88 allows member states to make fine-tuning or clarifications, but these amendments should not result in a stricter or more permissive regulation than the Regulation itself.

In the current Hungarian legal system, the Labour Code is a sectoral law of the generally applicable Infotv. (Kiss, 2020). In April 2019, when the GDPR Regulation entered into force in the EU member states, the Hungarian Parliament made comprehensive amendments to the sectoral laws (i.e., the Labour Code) based on Article 88 of the GDPR. Accordingly, the basic expectation of data protection measures is lawfulness and compliance with the general principles outlined in the Infotv. and the Labour Code, all of which are in line with international legislation:

1. Principle of purpose: The employer must assign a purpose to all data processing. This means that personal data may only be processed if the establishment, maintenance, or termination of the employment relationship would not be possible without the activity.

2. Principle of necessity and proportionality: the instrument used must be suitable for achieving the purpose, but it may only involve the necessary amount of data processing (limited in time), and the monitoring may only occur in the context of work. The private life of employees may not be monitored.

3. Appropriate legal basis for data processing: There are three possible legal bases for data processing in the workplace, from which the employer must choose one. These are:

   a) the data subject's voluntarily given consent (informational self-determination),

   b) legal authorization and

   c) data processing based on the employer's legitimate interests.

   Article 6 of the GDPR recognizes six possible legal grounds, but the three mentioned above are the most typical in the employment context. I have already

pointed out that the employee's consent can only be considered as a legal basis if the data subject has a natural choice and there are no negative consequences to fear if consent is refused, as the employment relationship is based on solid subordination.

I also refer here to the fact that in the case of a legitimate interest of the employer as a legal basis, the employer must pass an interest balance test (for details, see Data Protection Working Group, 2014). In such a case, the data controller must balance the legitimate interests of himself or an independent third party and his rights and interests arising from the protection of the reasonable privacy or other fundamental rights of the data subject. If the former outweighs the latter, the data management in question cannot be started. Legitimate interests alone can be many and varied, including the economic interests of the employer, efficiency gains, research and development, organizational development, new processes, security measures, abuse prevention systems, statistical data collection, and even ensuring efficient day-to-day operations.

4. Prior information of employees: The central element of the obligation to provide prior and adequate information is Infotv. Section 20 (2) lists the essential circumstances of data management about which the data controller must provide information. If the employer wishes to carry out a control by technical means, this must not be done in secret, but the employees must be informed in advance. Concerning data management in the workplace, it is also of utmost importance who within the employer's organization has access to personal data.

Even in continental Europe, case law (soft law) has a significant impact on shaping legislation and practices in the workplace. The ECtHR handed down the most extensive rulings related to data protection in the workplace, which also dramatically influences national (including Hungarian) law enforcement.

The ECtHR ruled in *Halford v. United Kingdom* case (1997) that both business and private telephone conversations are covered by the right to respect for private and family life under Article 8 (1) of the ECHR. Therefore, the employer is not entitled to tap the employee's office or private telephone without prior notice. In reality, the lawful and ethical monitoring of work phones is challenging, as the device's call log is personal data. While prior consent can be obtained from the employee for monitoring, this is impossible for those being called. Therefore, if the company phone may be used for personal purposes, NAIH (2016) believes it is good practice to have outgoing calls with two dialers: one for official and one for personal calls. The employer can only inspect the details of official calls while tapping employees' phone conversations is prohibited without prior notice (Halford v. UK case).

In *Copland v. United Kingdom* case (2007), the above rule was extended to the use of e-mail and the Internet. The Court argued that the employer may not secretly monitor the employee's telephone, e-mail, or Internet use, i.e., without prior information or relevant and officially published rules of the employer, as they are

all protected by Article 8 of the ECHR. Moreover, according to the definitions of the GDPR, all data appearing on a professional e-mail account, laptop, or phone are considered personal data. When this data is managed, it is officially considered data management. Therefore, the employer should create an internal regulation for using and controlling e-mail accounts and computing devices. This regulation should cover the following essential topics:

1. Whether or not the e-mail account or IT device can be used for private purposes. In Hungary, the employer may be entitled to terminate without notice if an employee violates the prohibition by using the Internet during work for personal matters. (BH2006. 64).

2. If the company e-mail or the IT device, in general, can be used for private purposes, what data may be used or stored on it?

3. What are the rules for backing up?

4. What are the detailed rules for controlling e-mail accounts and other IT tools (NAIH/2019/769)?

If the employer specifies in advance in regulations which websites are automatically blocked in the workplace, this can significantly reduce the chances of controlling Internet use in the first place (Data Protection Working Group, 2014; NAIH, 2016).

When checking the data content of a work laptop, the employee must explicitly identify which data is "private" on it. While checking the laptop, the employer must pay special attention to the fact that employees' private data cannot be processed. The critical element of ECtHR's *Libert v. France* (2018) ruling is that only that act of the employer infringes Article 8 of the ECHR, which supervises data explicitly marked "private" by the employee. The French Court of Cassation, in the main proceedings, distinguished between "private" and "personal" data, and only "private" data falls under and is protected by Article 8. The court argues that "personal" data is less sensitive as it may be related to the job (performance indicators, professional classification). Of course, the sharp distinction between the two data types is not always clear in practice, and the debate between the parties also stemmed from this. It can also be read from the judgment that data marked "private" do not enjoy absolute protection either: if they are stored on a work computer, access to them in the presence of the employee is not prohibited (Sipka & Zaccaria, 2018).

Employers may also encounter requests from workers to use their own devices in the office to perform their duties ("bring your own device" or BYOD procedures). Employers, in these cases, should also put in place internal regulations for securely transferring data between private and employer-owned devices.

The case of *Bărbulescu v. Romania* (2017) was widely reported in the international and Hungarian press, and numerous articles addressed its significance for businesses (Rózsavölgyi, 2018; Kállai, 2017). The foundations of the judgment lie in the fact that it defined the aspects that national courts must consider when assessing whether the procedure for controlling employees and the employer's exercise of disciplinary powers meet normative standards. The applicant (Bărbulescu) complained to the national court that his employer's termination of his contract was based on a violation

of his right to respect his private life and correspondence.

Beyond deciding the case, the Court has made great strides in establishing measures that guarantee proportionality and procedural safeguards for individuals. The so-called "Bărbulescu test" should be followed by national authorities (Bărbulescu Case, 2017: 36-39). The "Bărbulescu test" established the universally applicable measures that ensure proportionality and procedural safeguards for employees in the work arena. During the test, the following questions should be answered to verify the lawfulness of the planned or existing labor control mechanisms:

1. Has the employee been informed about the observation in advance by the employer in a clear form?
2. How far-reaching (in terms of time, space, and the number of people who had access to the results) was the observation, and how much did it interfere with the employee's private life? A distinction must be made here between monitoring the communication process and the content itself.
3. For what legitimate reasons was the observation conducted? Since content monitoring is more invasive than process monitoring, it requires a weightier justification.
4. Would less intrusive methods on the part of the employer have been sufficient?
5. What consequences did the observation have for the employee (assessment of proportionality)?
6. Were there adequate safeguards for the employee (e.g., the possibility of complaining about the monitoring)?

The NAIH recommendation (NAIH/2019/769) in Hungary suggests using the Bărbulescu test in monitoring ICT use in the workplace. Employers must create and disseminate acceptable use and privacy policies that define how the company's network and devices may be used. Second, employers must consider the proportionality of monitoring. As an example of good practice, it is sufficient to check the e-mail address and subject of the letter. In most cases, it is already possible to determine whether the e-mail is intended for private purposes. According to the applicable data protection regulations, the employer is not entitled to review the content of private e-mails stored in the e-mail account, even if the employees were informed in advance about the inspection. Monitoring communication content requires a solid legal justification, as it is a significant intrusion. If this is given, more precise control (checking the content of e-mails) can follow. As a rule, the employee's presence must be guaranteed during the control. However, if this is not possible, the employee must be informed about the employer's plan and allowed to be represented. If this is not possible, the employer may access the e-mail account in the presence of an independent third party.

In the *Köpke v. Germany*[2] case (2010), the ECtHR ruled, in the context of covert video surveillance, that employers who wish to use camera surveillance to monitor the behavior of their employees must show a legitimate reason (such as the protection of property). *López Ribalda and Others v. Spain* (2019) applies the Bărbulescu test to an employer's video surveillance

2 In this case, the applicant was a supermarket cashier, who was dismissed without notice for theft by the employer. The theft was revealed by a covert video surveillance operation carried out by her employer.

procedures, including some of the principles of the Köpke v. Germany decision. The employer should consider the following requirements and factors when implementing video surveillance in the workplace:

1. Prior and explicit notification to the employee of the possibility of video surveillance measures. A compelling need to protect the critical public or private interests may justify a lack of prior notice.

2. Scope of surveillance: reasonable restrictions on time, space, and the number of people who have access to the results should be considered. In addition, video surveillance is prohibited in inherently private places (toilets, changing rooms); privacy protections are high in enclosed work areas (own office) and lower in places accessible to colleagues or the public.

3. Valid reasons must justify surveillance: covert surveillance is generally unacceptable because the slightest suspicion of theft or other employee misconduct may exist. However, reasonable suspicion of serious misconduct and a significant inventory shortage (due to theft) may be sufficient grounds for covert surveillance, mainly if the smooth operation of the business is at risk and there is suspicion of concerted action by multiple employees.

4. The employer must always consider the use of less intrusive methods.

5. The employer must provide adequate safeguards for employees (e.g., inform employee representatives or an independent body about the scope of the surveillance or allow employees to file a complaint about the procedure).

Hungarian case law further elaborates on the possible rules for camera surveillance and lists the situations in which this instrument of control is prohibited in the workplace:

1. If the camera monitors only one worker and their activities.

2. If the observation could violate human dignity (especially in changing rooms, showers, toilets, or medical rooms and the associated waiting room).

3. In rooms designated for work breaks (an exception to this is if there is an object to be protected in the room, such as a food and beverage vending machine).

4. When the purpose of camera surveillance can be achieved by other means less intrusive to privacy (e.g., by security guards).

If no one can legally be at work (outside working hours or on holidays), the entire work area may be monitored, including changing rooms, toilets, and break rooms. The employer may use the electronic surveillance system only to monitor the parts of the building, premises and areas owned or used by the employer or events that have taken place there, excluding public areas. In Hungary, the consent of employees is not required for the use of the camera. Still, they must be informed in writing in advance of which camera has been installed for what purpose, where it is located, and how the data will be managed (see ABI-2962/2010 and NAIH 2016 for more details). In general, using a hidden camera is prohibited but may be exceptionally

justified in criminal proceedings if all the circumstances require it (EBH2000. 296). Finally, the employer must agree in advance with the local works council on the use of technical aids in the surveillance of employees (Labour Code Section 264/1d).

Regarding the spatial extent of video surveillance (step 2 of the Bărbulescu test), an interesting judgment was delivered in Antović and Mirković v. Montenegro (2018) case. The ECtHR found that the privacy rights of two professors under Article 8 of the ECHR had been violated by the university when it installed cameras in lecture halls to protect the security of persons and property. In its reasoning, the Court pointed out that privacy can include *"professional activities or activities taking place in a public context."* The Court noted, "*those university amphitheaters were teachers' workplaces, where they not only taught but also interacted with students, developing relationships and constructing their social identity."*

Technologies that enable companies to keep track of their vehicle fleets are now widely used, especially by companies with large vehicle fleets or companies that operate in the transportation sector. Every employer that uses vehicle telematics collects information about the vehicle and its employee. As the NAIH and the Data Protection Working Group (2014) also point out, this data can include the vehicle's location and the employee, driver behavior, or other information, depending on the technology. Data stored by the navigation system GPS is also considered personal data of the driver, as it allows conclusions to be drawn about the employee. Against this background, using such a system is acceptable if the employer's legitimate interest can be proven and if compliance with other legal obligations is demonstrated. The use of GPS is therefore recommended for logistical purposes, i.e., to determine the position of the vehicle rather than to track the employee, to organize workflows more efficiently for specific activities, or when the value of the vehicle or the vehicle itself explicitly justifies it. In addition, GPS may be lawfully used when the goal is to protect the lives and physical integrity of employees, such as during transportation through a conflict zone. Although employers may have a legitimate interest in pursuing these goals, it is critical to determine whether the processing necessary to achieve these goals is essential and whether its implementation meets the standards of proportionality and subsidiarity. For example, monitoring vehicles outside of working hours are usually unlawful. The most important step a company can take to ensure compliance with the principles when private use of a company car is allowed is to allow employees to temporarily turn off location tracking when exceptional circumstances warrant (e.g., a doctor's appointment). In this way, the employee can act independently to protect specific location data as private (1664/A/2006-3).

A particular employer-initiated monitoring procedure is the monitoring of alcohol or drug use by employees in the workplace. Section 52 (1) of the Hungarian Labour Code explicitly states that the employee is obliged to appear at the place prescribed by the employer, at the right time and in a suitable condition for work, and the employer's obligations also include the creation of safe working conditions (Section 51 of the Labour Code). In this context, the employer may be entitled to conduct an alcohol or drug test on employees. As early as 1999, the Supreme Court ruled that an employer may exclude the consumption of alcohol in the workplace (LB Mfv. I. 10.939/1999). In the event of a violation of this regulation,

termination without notice is also permitted (Mfv. E. 10.741 /2002/1). Resolution 122 also states that an employee's refusal to participate in the test may be capable of giving rise to an adverse legal consequence. An employee who refuses to participate in the test may be excluded from work, and it is, therefore, lawful to withhold their wages for the duration of the ban. However, the control of alcohol consumption must not violate the personal rights of the employee concerned, and the right of control must not be abusive (i.e., it must not be a general practice or a practice lasting several days, and an authorized person must carry it out). To ensure this, it is advisable to carry out a balance of interest test in advance.

Personal data related to drug use are considered particular data. As such, the data processing requires an explicit legal provision or the voluntary, explicit, written consent of the data subject (employee). According to prevailing Hungarian case law, a state of confusion resulting from self-inflicted drug use is considered a state of intoxication due to self-infliction (BH2000. 432). Employee cooperation with employer-initiated drug testing is a must (MK Resolution 122). However, drug testing should only be conducted under the supervision of an appropriately qualified person.

Hard and soft laws cover many aspects of organizational labor control mechanisms. However, employee privacy is a moving target. The proliferation of ICT devices, qualitative and quantitative, and their invasive nature (Stalla-Bourdillon et al. 2014) is so rapid that legal disputes, court decisions, or laws cannot follow. It is becoming increasingly attractive for employers to provide wearable technology to their employees to track and monitor their health, even if the processing of health data is protected. Video surveillance of employees is also a new trend. Because of the ability to access the data collected remotely (via cell phones), the smaller size of cameras, or new video analytics tools (that monitor employee facial expressions), new rules are needed for the same operation. Event data recorders installed in company vehicles record a video when a special traffic event occurs (sudden braking). They can detect employees' behavioral patterns, driving habits, or personal conversations.

4. HYPOTHESIS TESTING AND DISCUSSION

The employment relationship initially reflects a strong subordination between the parties since the employer has a decisive influence on the design of the working conditions. This phenomenon is referred to as the "doctrine of managerial prerogative" (Kiss, 2001; Tsui and Wu, 2005). The term "prerogative" means a "*right or a privilege that belongs to a certain institution, group or person*" (Hawkins, 1988). In the field of labor, the term prerogative refers to the right to run businesses (Strydom, 1999). The need for a prerogative in an enterprise stems from the obvious notion that there must be a mechanism to coordinate the enterprise's core activities and allocate its members' tasks and resources to achieve its goals (Drucker, 1993).

Thus, the managerial prerogative is an exclusive and unique right, power, or privilege of management to shape the company, which relates to both strategy and day-to-day operations and includes, among other things, decisions on expansion and growth, investment, hiring, dismissals, promotions, compensation, disciplinary procedures or the organization of work and monitoring procedures. The list of possible rights of the employer is both long and heterogeneous.

To better understand these decisions, we distinguish between those related to business or economic issues (mergers and acquisitions, use of physical and financial assets necessary for the company, vision, mission, and strategy) and those related to the use of human resources (required number and qualification of employees, employment conditions including work-related monitoring procedures). These two aspects reinforce each other.

Perline (1971) argues that managerial prerogative derives from property ownership. Others, such as Collins (2021), see the source of an employer's managerial prerogative as rooted in his power in the labor market. Comparing the bargaining power of employees with that of employers in the labor market, employers have a clear dominance over employees. According to this view, the subordinate position of the contracting parties in the employment relationship serves as a basis for employers to shape the relationship. Collins' second argument for employer prerogative is that when employees join an organization (i.e., sign the employment contract), they also acknowledge that they are joining the organization's pre-existing architecture.

As noted above, the employer's managerial prerogative extends to all organization activities, including monitoring work processes. The employer's right to direct and assign work and the employee's duty to work result in the employer's extensive right to collect information about its workforce. Throughout the employment relationship, employers need information about employees' skills, abilities, performance levels, motivation, and counterproductive, illegal, or unethical work behaviors (Bhave et al., 2020). Employers conduct background checks and use workplace IT / communication technologies to collect and possess information.

Obviously, because of the doctrine and the imbalance of powers between employers and employees, the means of an employer's right to information are more sophisticated and numerous than those possessed by employees to protect their private lives. "*Privacy ... was a very valuable thing. Everyone wanted a place where they could be alone occasionally. And when they had such a place, it was only common courtesy in anyone else who knew of it to keep his knowledge to himself.*" (Orwell, 1949. p. 173.) Beyond "common courtesy," societies use various tools to protect privacy (including work environment privacy) against the employer's prerogative.

The managerial prerogative is limited primarily, but not exclusively, by international and domestic law. The doctrine of managerial prerogative is the general rule, while employment-related data protection law, which conceptually aims to protect employees from managerial prerogative, is the exception. Other institutions such as good faith, collective bargaining with labor unions (including the right to strike), corporate practices, the labor market, and economic conditions may also limit the prerogative.

The research hypothesis assumes that hard and soft legal elements of workplace privacy are linked to the doctrine of managerial prerogative through legally fair employee control mechanisms.

The thematic analysis of hard and soft law in Europe and Hungary has shown that the hypothesis is temporarily acceptable. It is concluded that all international and Hungarian hard and soft law parts uniformly conclude that employees may be screened only in the context of their

employment-related behavior and that their privacy is always protected once the employer establishes procedures and mechanisms for screening individuals during employment. In addition, data subjects should be fully informed of the monitoring procedure used, but it is not necessary to ask for their consent. In addition, legal monitoring measures and policies must be readily available to employees.

International case law provides organizations with the Bărbulescu test and the principle of proportionality to consider when monitoring the work-related conduct of their employees. A proportionality test should be applied before any monitoring to determine whether all data is necessary, whether the processing outweighs the right to privacy in general, and what steps should be taken to ensure that violations of the right to privacy and the right to confidentiality of communications are minimized.

When processing employees' private data, the employer must always observe the basic principles of data protection, regardless of the technology used (telephone, e-mail, laptop, Internet, camera, and social networks). Analog and electronic communications are treated in the same way.

According to the current GDPR, companies may only collect data for legitimate purposes and process it following established guidelines (e.g., "*being proportionate, necessary, for a real and present interest, in a lawful, articulated and transparent manner*"). When choosing the legal basis for data processing, the employee's consent is inappropriate unless the employee can refuse it without adverse consequences. In some instances, the legal basis may be a legal/contractual authorization or the employer's legitimate interest if the data processing is strictly necessary for a legitimate purpose and complies with the principle of proportionality. If there is no legal obligation to process data if it goes beyond the fulfillment of the employment contract and if the necessity of the data processing results primarily from the employer's interests, the balancing of interests may be the appropriate legal basis.

The hypothesis that the employer's technological tools for monitoring the work of its employees are developing faster than legislation and law enforcement is accepted only temporarily. The ever-changing ICT era offers companies new opportunities to apply the prerogative to its fullest extent. For this reason, other mechanisms that limit the employer's prerogative to monitor work, such as employer branding based on good faith and collective bargaining, are highly valued.

5. CONCLUSIONS

The nature of the employment relationship is complicated because it is psychologically fraught (Kiss, 2020; Sparrow and Cooper, 2003). To be fruitful for both parties, the employment relationship must be built on mutual trust (Palomo Sánchez Case, 2011). Employee trust and commitment quickly diminish when an employer invades employee privacy while exercising its right to obtain work-related information. When the sharp boundary between employees' work and personal lives is removed in this way, it can violate the working relationship's psychological (and ethical) dimensions.

Balancing the interests of employers to exercise the right to control work processes with the interests of employees to protect their privacy remains a challenging issue in professional discussions among scholars.

The digitization of workplaces and the rapid development of technological devices as driving forces must lead to organizational mechanisms to protect workers' privacy. This article highlights the achievements of hard and soft law enacted by international, European, and Hungarian courts and authorities. There are already advanced concepts on how legal and ethical monitoring procedures should also be established to protect the "psychologically charged" and trustful content of the employment relationship. The article's findings can lead to higher data protection compliance and ethical data management in organizations. However, due to the rapid evolution of technologies and the limited pace at which legislation can follow, future research is needed to understand how employer branding practices and collective bargaining can contribute to organizational "self-regulation" in data protection.

REFERENCES

1. Article 29 Data Protection Working Party (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, Brussels
2. Article 29 Data Protection Working Party (2017). *Opinion on Data Processing at Work*, WP 249, Brussels
3. Balogh Zs. Gy. (1998). *Jogi informatika.* Budapest-Pécs: Dialog Campus
4. Balogh Zs. Gy. (2011). Közterületi térfigyelés *és* adatvédelem. *Vezetéstudomány* XLII(5). pp. 26-35.
5. Bankó Z. & Szőke G. (2016). *Issues of the Digital Workplace, Situation in Hungary* Budapest: JurInfo Kiadó
6. Bhave D. P., Teo L. H., Dalal R. S. (2020): Provacy at Work: A Review and a research Agenda for a Contested Terrain. *Journal of Management*. Vol 46(1). pp. 127-164.
7. Collins H.: (2021): Employment Law. Oxford University Press.
8. Council of Europe (1953). European Convention on Huma*n Rights.*
9. Council of Europe (1980). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.
10. Council of Europe (2015). *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. Drucker P. (1993): The New Society: The Anatomy of Industrial Order. Routledge
12. European Commission (2018). *Authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).* COM(2018) 451 final
13. Foth M., Schusterschitz C., Flatscher-Thöni M. (2012). Technology acceptance as an influencing factor of hospital employees' compliance with data-protection standards in Germany. *Journal of Public Health* (20). pp. 253–268
14. Gidron T., Volovelsky U. (2018). The Right to be Forgotten: The Israeli Version. *Computer Law & Security Review* 34(4). pp. 824-829.
15. Hawkins M., J. (1988): The Oxford Paperback Dictionary. Oxford University Press. UK
16. Hegedűs B. (2013). Az adatvédelmi jog általános tanai. In: Tóth András (ed.):

Infokommunikációs jog II. 137-145. Budapest: Patrocínium

17. Jay, R. & Hamilton, A. (1999). *Data Protection. Law and Practice.* London: Sweet & Maxwell
18. Jóri A. (2005). *Adatvédelmi kézikönyv* Budapest: Osiris Kiadó
19. Jóri A. *(*2009). *Az adatvédelmi jog generációi* és *egy második generációs szabályozás részletes elemzése* PhD Diss., University of Pécs Hungary Faculty of Law
20. Kállai P. (2017). *Magán-* és *családi* élet *tiszteletben tartásához való jog Bărbulescu Románia elleni* ügye*.* Fundamentum, 3-4.
21. Karoliny M-né, Ásványi Zs., Bálint B. (2017). Erőforrás-biztosítási rendszerek: toborzás, kiválasztás, beillesztés és leépítés In: Karoliny M-né, Poór J: *Emberi erőforrás menedzsment kézikönyv – Rendszerek* és *alkalmazások.* Budapest: Wolters Kluwer
22. Kerber W., Zolna K. K. (2022): *The German Facebook case: the law and economics of the relationship between competition and data protection law.* European Journal of Law and Economics. Springer. https://doi.org/10.1007/s10657-022-09727-8
23. Kiss Gy. (2001). *Az Európai Unió munkajoga*. Budapest: Osiris Kiadó
24. Kiss, Gy. (2020). *Munkajog.* Budapest: Dialóg Campus Kiadó
25. Korff, D. (2002). *EC Study on Implementation of Data Protection Directive Comparative Summary of National Laws*, Human Rights Centre University of Essex Colchester (UK)
26. Majtényi, L. (2003). Az információs jogok In: Halmai, G. and Tóth G. A. (eds.): *Emberi jogok* Budapest: Osiris Kiadó
27. Majtényi L. (2006). *Az információs szabadságok* Budapest: Complex Kiadó
28. Majtényi L. (2010). *Információs* és *médiajog I*. Budapest: Bíbor Kiadó
29. Mayer-Schönberger, V. (2001). Generational Development of Data Protection in Europe In: Agre P. E. – Rotenberg M. (eds). *Technology and Privacy: The New Landscape*. Massachusetts Cambridge: The MIT Press
30. Mészáros, J. (2017). *Adatvédelem a XXI. században* és *az internet világában,* PhD Diss., University of Szeged Hungary
31. NAIH Tájékoztató (2016). *A Nemzeti Adatvédelmi* és *Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről*
32. OECD (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*
33. OECD (2013). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Revision.*
34. Ogriseg, C. (2017). GDPR and Personal Data Protection in the Employment Context. *Labour Law & Law Issues*. 3(2).
35. Orwell, G. (1949): *1984*. Secker & Warburg. London. UK.
36. Perline M. M. (1971): Organized Labor and Management Prerogatives. *California Management Review 46.*
37. *Reine*cke, J., Arnold, D. G., Palazzo, G. (2016). Qualitative methods in business ethics, corporate responsibility, and sustainability research*.* *Business Ethics Quarterly*. 26 (4). pp. xiii–xxii.
38. Rózsavölgyi B. (2018). Mikor lehet jogszerű a munkáltató ellenőrzése? – az Emberi Jogok Európai Bírósága

Nagykamarája Bărbulescu kontra România ügyben hozott ítéletének iránymutatásai *Munkajog*-HVG Orac 2018(1).

39. Schoeman, F. D. (ed) (1984). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press
40. Simitis, S. (1999). Reconsidering the Premises of Labour Lafw: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data. *European Law Journal*. 5(1). pp. 45-62.
41. Sipka P. & Zaccaria M. L. (2018). A munkáltató ellenőrzési joga a munkavállaló munkahelyi számítógépén tárolt magánadatai fölött. *Munkajog II.* HVG-Orac
42. Solove, D. J. (2008). *Understanding Privacy.* Cambridge, London: Harvard University Press
43. Sólyom L. (1983). *A személyiségi jogok elmélete* Budapest: Közgazdasági és Jogi Könyvkiadó
44. Sparrow P. R. & Cooper C. L. (2003). *The Employment Relationsip: Key Challenges of HR* London & New York: Routledge
45. Stalla-Bourdillon S., Phillips J., Ryan M. D. (2014). *Privacy vs Security ... Are We Done Yet?*. Springer
46. Strydom E (1999): The Origin, Nature and Ambit of the Employer Prerogrative Part I. S. African Mercantile L. J. (40)
47. Szőke G. L. (2013). Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció* és *Jog.* 2013/3 (56.). pp. 107-112.
48. Szőke G. L. (2014). *Adatvédelem* és önszabályozás. *Adatvédelmi irányítási rendszer az adatkezelőnél*, PhD Diss., University of Pécs Hungary Faculty of Law
49. Tsui A. S. & Wu J. B. (2005). T*he new employment relationship versus the mutual investment approach: implications for human resource management* Human Resource Management. 44(2): 115-121.
50. Young (1963): *The Question of Managerial Prerogatives*. Industrial Labor Relations Review 240.
51. van de Waerdt P. J. (2020). Information Asymmetries: Recognizing the Limits of the GDPR on the Data-Driven Market. *Computer Law & Security Review*. 38.
52. Warren, S. D. & Brandeis, L. D (1890). The Right to Privacy. *Harvard Law Review.* 1890/4.
53. Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum
54. Workman M. (2009). A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions. *Information and Organization*. 19. pp. 218–232

European Cases:

55. Antović and Mirković v. Montenegro 2017. Case Nr. 70838/13
56. Bărbulescu v. România 2017. Case Nr. 61496/08.
57. Copland v. UK 2007. Case Nr. 62617/00.
58. Halford v. UK 1997. Case Nr. 20605/92.
59. Köpke v. Germany 2010. Case Nr. 420/07.
60. Libert v. France 2018. Case Nr. 588/13.

61. López Ribalda and Others v. Spain 2019. Case Nrs. 1874/13 & 8567/13
62. Palomo Sanchez v. Spain 2011. Case Nrs. 28955/06, 28957/06, 28959/06 and 28964/06

TEHNOLOGIJA I PRIVATNOST NA RADNOM MJESTU: OPSEG I OGRANIČENJA ORGANIZACIJSKIH KONTROLNIH MEHANIZAMA

Sažetak

Pravo zaposlenika na privatnost i ekstenzivna potreba poslodavaca za informacijama, povezanim s obavljanjem posla, u međusobnom su sukobu. Nesrazmjer autoriteta između poslodavaca i zaposlenika te doktrine menadžerskih povlastica utvrđuje ishod međusobno sukobljenih interesa, zbog čega pravo na privatnost zahtijeva zakonsku zaštitu. Cilj ovog rada je analiza legislativnih („tvrdog“) i provedbenih („mekog“ zakonskog uređenja) postignuća europskih i mađarskih inicijativa za organizacijske mehanizme kontrole rada, kao i razumijevanje njihovih mogućih ograničenja, u odnosu na doktrinu menadžerskih povlastica. Kao istraživačka metoda korišten je tematski pregled dokumenata i literature, koji se odnosi na odgovarajuće zakonodavstvo i sudsku praksu Europskog suda za ljudska prava, mađarskog Vrhovnog suda te mađarske Nacionalne agencije za zaštitu podataka i slobodu informacija. Rezultati istraživanja su potvrdili hipotezu da trenutni pravni instrumenti ograničavaju organizacijske kontrolne mehanizme, kako u sadržajnom, tako i u procesnom smislu. Međutim, brze tehnološke inovacije čine pravo zaposlenika na privatnost „pokretnom metom“, pri čemu sam zakon predstavlja tek privremenu i ograničenu zaštitu.

Ključne riječi: *privatnost zaposlenika, mehanizmi kontrole rada, doktrina menadžerskih povlastica, ravnoteža interesa*