UDC: 349.2:621.397.4
DOI: 10.5937/PDSC26040G

Slađana Gligorić, PhD, Assistant Professor
Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad
email: sladjana.gligoric@pravni-fakultet.info,
ORCID ID: 0000-0003-4535-8041

DIGITAL MONITORING AT WORK AND WORK RELATIONS: KEY LABOUR LAW ASPECTS

Abstract: Digital transformation of work within the Fourth Industrial Revolution, as well as the ever-wider use of artificial intelligence systems and various AI tools, have led to significant changes in work organization and employment relations. Remote work and working from home have intensified, which has simultaneously contributed to increased use of digital employee surveillance. Although the use of digital monitoring is often justified from the employer's perspective as a legitimate and useful measure aimed at improving work organization, increasing productivity and efficiency, and strengthening safety and occupational health systems, its implications from the employees' viewpoint are considerably more complex and problematic. Continuous digital workplace surveillance has significant negative psychosocial effects, including increased stress, a persistent sense of being monitored, and deteriorating employee mental health. It also leads to reduced self-confidence, motivation, and perceived autonomy, while compromising privacy. Furthermore, there is a risk of discrimination against vulnerable groups, such as persons with disabilities and older workers. At the same time, constant monitoring may discourage employee solidarity and trade union organizing. In this article, using normative and comparative legal methods, we will analyze the forms, objectives, advantages, and risks of digital workplace surveillance, with a review of the legal and ethical implications. Special attention is paid to the balance between legitimate employer interests and employees' right to privacy. It is concluded that transparent and proportionate application of digital surveillance is crucial

for preserving employment relationships and protecting employees' fundamental rights at work, and that when video surveillance is used a certain balance must be established between the employer's interests (protection of property, security measures) and the employees' rights (dignity, protection of personal data), observing the principle of data minimisation, by which only data that are necessary and indispensable are collected.

Key words: *digital surveillance, video surveillance, privacy, work and labour relations*

INTRODUCTION

The rise of digital monitoring was further accelerated in many countries with the onset of the COVID-19 pandemic, as employers worldwide adopted remote working practices. New methods of collecting and processing data introduce additional risks for workers, particularly in the context of digitalization and automation, the use of artificial intelligence, and the expansion of work beyond the employer's premises — including remote work, home-based work, and platform-based work. As remote work becomes more prevalent, workers are increasingly accepting monitoring as a trade-off for flexibility (Abraha, 2025, p. 8).

The adoption of new technologies has accelerated the flow of information and eliminated traditional temporal and spatial boundaries in communication. As a result, many tasks are now performed through the internet, email, mobile phones, and social platforms. This development prompts critical questions regarding the limits of employer control within managerial and disciplinary authority: should these boundaries be confined to working hours and the physical workplace, or can they be interpreted more broadly? Remote work, especially working from home, has opened new questions regarding the monitoring of employees' work, since direct employer supervision is absent. Indirect control is increasingly carried out through digital tools that record time spent working and availability; employees submit work reports; presence on the employer's server is tracked through system logs; but sometimes continuous video surveillance via the computer camera is required. Altogether, this raises issues of respecting privacy and the legality of such practices. Modern employment relations, on the other hand, are characterized by greater freedom and autonomy of employees in organizing work, due to the development of digitalization, although the employer's fundamental duty remains to provide

work, delegate tasks, and supervise their execution. Nevertheless, it should be borne in mind that, despite the generally greater autonomy of employees in performing work obligations, certain employer powers have been strengthened thanks, among other things, to the development of technologies that enable more intensive monitoring of employees' work. This is, for example, the case with video surveillance or systems that provide the employer with virtually unlimited 'remote control' (Global Positioning System /GPS/, Radio Frequency IDs /RFID/, Global Information Systems /GIS/, etc.) (Kovačević, 2014, p. 338). The criteria for analyzing the admissibility of supervisory measures implemented by the employer over employees' work are usually found in the literature primarily in light of the principles of conscientiousness and fairness, and in light of the obligation to refrain from unjustified and excessive restrictions on employees' human rights and freedoms in the workplace (Kovačević, 2014a, p. 339).

The issue of digital surveillance in working environments must also be viewed through the prism of the protection of civil rights and freedoms, as part of a tendency toward the 'constitutionalization' of labour law, where the relationship of guaranteed civil rights is considered at the level of the employee–employer relationship. This is theoretically justified as setting new boundaries of legal subordination in employment, or as compensation for new risks accompanying greater flexibility in working conditions, particularly the risk of job insecurity (Kovačević, 2013, p. 1583). Therefore, modern labour law has the key task of reconciling employers' freedom in organizing work, based on the principle of entrepreneurship, with the need to ensure the protection of workers' economic and social rights. Globalization, digitalization, and new forms of work (platform work, the 'gig economy') further complicate this balance, as employers seek deregulation for competitiveness, while workers demand expanded protection in new forms of performing work obligations.

Electronic Workplace Surveillance – General Issues of Conceptual Definition and Normative Regulation

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 (International Labour Organisation [ILO], 1997, 1). Surveillance is conducted to collect data and information, and may utilize digital and automated systems or involve

human participation. Although the terms monitoring and surveillance are different concepts, we will look at them as synonyms.The difference is that surveillance includes physical monitoring of employees' performance, very often without prior notice. The common classification of the most widespread surveillance systems includes video surveillance, monitoring of communication channels, and GPS systems for tracking geolocations. Within the category of monitoring of communication, this encompasses computer surveillance (such as monitoring emails and access to Internet pages) as well as monitoring of telephone communications. The most common monitoring and surveillance practices can be categorized as *performance* monitoring[1], *behaviour* monitoring, *personal characteristics* monitoring[2] (Abraha, 2025a, p. 8). With the development of artificial intelligence systems, namely algorithmic management systems and numerous AI tools, their use in work and employment relations is increasing (through systems for recruitment, systems for delivering work tasks, systems for monitoring and evaluation), which are considered high-risk systems according to the EU Artificial Intelligence Act (AI Act) (Regulation (EU) 2024/1689). Therefore such high-risk AI systems would have to comply with a range of requirements, particularly on risk management, testing, technical robustness, data training and data governance, transparency, human oversight, and cybersecurity, before being placed on the market or put into service (Regulation (EU) 2024/1689), in order to maintain basic labour law rights, expecially right to protect privacy, protect personal data and discriminatory practices. The AI Act mandates that employers inform and consult workers or their representatives about the planned deployment of high-risk AI systems in the workplace, and it bans the use of emotion recognition AI systems in the workplace (Abraha, 2025b, p. 28).

The Code of Practice on the Protection of Workers' Personal Data (1997) of the International Labour Organization is one of the first comprehensive international documents to provide guidelines on the collection, processing, and monitoring of employee data, with the aim of

[1] Including monitoring of emails, telephone calls and internet usage to more sophisticated biometric technologies, predictive analytics and AI. Employment monitoring systems can track workers' computer activities, including mouse movement and the number of keystrokes, take screenshots etc. (Abraha, 2025c, 8).

[2] Some of the most invasive worker monitoring tools can be deployed remotely and secretly monitor workers' every move and activity across devices, including secretly activating webcams (to track eye movements, body language, and facial expression to assess attentiveness and infer stress) and microphones (Abraha, 2025d, 9).

safeguarding their privacy and dignity. Although not legally binding, it serves as a reference in the drafting of laws, collective agreements, and enterprise-level policies. It's worth mentioning that the International Labour Conference just adopted Convention No. 193 in June 2026, establishing the first international labour standard dedicated to the platform economy and the first international standard developed specifically to address the impact of digitalization on the world of work. It seeks to ensure that all platform workers, regardless of their employment status, can benefit from fundamental rights and appropriate protections, while recognizing the opportunities created by digital labour platforms (ILO, 2026). Also, it is worth mentioning the Protocol amending Convention 108 of the Council of Europe, as the enhanced version of the first binding international convention on data protection Convention 108 from 1981 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1985), which introduces stricter rules on privacy, transparency, and accountability in the digital age and Convention on the Protection of Human Rights and Fundamental Freedoms with Protocols.

Furthermore, the key regulations that indirectly govern the issue of digital surveillance in the EU are the General Data Protection Regulation (Regulation (EU) 2016/679, 2018) and the Charter of Fundamental Rights of the European Union - specifically, Article 7 (the right to respect for private and family life) and Article 8 (the right to the protection of personal data) (Charter of Fundamental Rights of the European Union, 2012/C 326/02) elevate the right to protection of private life and personal data to constitutional status. Directive 2002/14/EC also prescribes the right to information and consultation on decisions likely to lead to substantial changes in work organisation or in contractual relations (Directive 2002/14/EC, Art. 4). The EU General Data Protection Regulation (GDPR) establishes broad principles for the protection of personal data, taking a general approach without specifically focusing on employment relations. Within its framework, employees are often regarded as consumers, while specific issues of workplace data protection are left to the Member States to regulate through national legislation and collective bargaining. Also there are regulations in labour laws, industrial relations, emerging digital regulations (e.g. AI Act, Platform Work Directive) and other sector-specific laws offering indirect protections, creating a fragmented system with divergent substantive safeguards (Abraha, 2025d, p. 46). Therefore, a key shortcoming is the absence of clear rules regulating their use; persistent challenges remain regarding the efficacy of these laws in protecting individuals—particularly workers—within the increasingly digitalised

workplace. Workers are especially susceptible to harm due to entrenched power asymmetries and heightened risks of data exploitation, yet many existing legal frameworks provide insufficient or inconsistent protection, and some jurisdictions explicitly exclude workers from coverage (Abraha, 2025e, p. 1).

The case law of the European Court of Human Rights (ECHR) is of invaluable importance in shaping the boundaries and criteria that national courts must follow when assessing whether an adequate system of privacy protection exists in the workplace. It is essential that the employee is transparently informed of any potential digital surveillance (principle of transparency), that the purpose and scope of surveillance are clearly justified (principle of proportionality-restriction of rights only to the extent necessary), and that there is a defined temporal and spatial framework for such limitations. Furthermore, it is crucial to determine whether there were legitimate reasons justifying the monitoring of an employee's communications and other grounds for accessing their content, which requires a stronger justification; whether less restrictive alternatives existed from the perspective of respecting the employee's privacy; what the consequences of surveillance were for the employee; whether the surveillance was conducted in accordance with its originally defined purpose; and whether adequate privacy safeguards were in place, particularly in monitoring content (Mojsilović, 2023, p. 330). The criteria developed by the European Court of Human Rights (ECHR) should serve as key guidelines for assessing the scope and justification of workplace surveillance in defining the boundaries between the employer's legitimate interests and employees' right to privacy.

In the Republic of Serbia, the normative framework that indirectly regulates digital surveillance is primarily prescribed in the Law on Personal Data Protection (Law on Personal Data Protection, 2018), which governs data processing, including employee monitoring. Employers are required to have a legal basis for such processing and to ensure the proportionality of measures. In addition, the Law on Electronic Communications (Law on Electronic Communications, 2023) guarantees the confidentiality of electronic communications, regulates interception, and prescribes obligations for data retention. The issue of surveillance is not explicitly regulated by the Labour Law. Special guarantees of protection may be achieved through provisions safeguarding the employee's personal integrity and dignity, as well as through rules on protection of personal data (Labour Law, 2005).

Limits of Permissible (and Impermissible) Digital Surveillance of Employees at Work

Electronic monitoring has been a regular feature in many factory shop floors and offices for decades. Monitoring can be distinguished in terms of its purposes, invasiveness, synchronicity (which may allow for frequent, continuous and instantaneous recording), and the transparency of its use and deployment (Jeske, 2022). It rapidly increases its presence due to the boom of digitalization and automation at work.[3] The ability to monitor and exert control over employees in a variety of different ways increases managerial prerogative (Lockwood, 2018a, 205) and can lead to abuse of employer prerogatives. Digital surveillance in the workplace can be introduced in two ways. If employees are not consulted, they tend to reject the measures, view them as excessive, and become demotivated, which lowers productivity. Alternatively, involving employees in designing the measures, explaining their purpose, and guiding them through the process fosters acceptance and cooperation. By this alternative means, the collective entitlement of employees to information and participation is safeguarded, creating a durable sense of satisfaction among workers. Therefore, employee reactions to electronic monitoring are often influenced by the motives behind the implementation of the monitoring systems, the use of these systems and the extent to which employee needs are met and their voices heard (by the organizations and managers who are directly responsible for systems implementation) (Jeske, 2022a). Excessive monitoring can negatively affect performance, result in a lack of trust, demotivate staff and is not conducive to the creation of a positive work environment (Lockwood 2018b, 219). Extensive evidence indicates that privacy-invasive workplace practices, particularly pervasive surveillance, can cause psychological harm and contribute to stress-related illnesses (Lockwood, 2018c, 20). Through constant surveillance, union activism may be diminished, since employers are able to predict collective actions based on data from other employees without direct observation of each worker.[4] Algorithmic bias in hiring and

[3]Digital surveillance is very whidspread, research in the USA has revealed that surveillance in the workplace is common practice with it being deployed by nearly eighty per cent of employers. In the UK context, it is estimated that sixty per cent of employers engage in monitoring of employees (Lockwood, 2018c, 205).

[4] Therefore, in order to protect workers, the National Labour Relations Act (NLRA) in USA protects workers' rights to organise and engage in collective activities, prohibiting employers from using surveillance tools to interfere with unionization efforts, while also

management systems perpetuates systemic discrimination, for example Amazon's abandoned AI recruitment tool, which penalised resumes containing the word 'women', exemplifies how historical biases embedded in training data disadvantage protected groups. Marginalised groups face compounded harms in low-wage sectors like warehousing, where invasive monitoring disproportionately affects women and people of colour. These technologies risk entrenching inequality by creating opaque barriers to employment opportunities (Lockwood, 2018d, p. 19). Accordingly, work in digital spaces raises the matter of ensuring the protection of employees' mental health and overall welfare, in light of technostress stemming from the persistent use of digital technologies.

The digitalization of work reinforces control mechanisms through digital surveillance and algorithmic management, whereby AI systems assume employer-like functions in recruitment, task delegation, and performance evaluation, and can directly influence decisions on hiring, promotion, or even contract termination. Algorithmic management, based on automated data processing, poses significant risks to privacy, equality, and labour and social rights. These risks are particularly acute for vulnerable groups such as women, people with disabilities, and the elderly, especially when public digital data is aggregated to produce predictive conclusions about workers' future behaviour. Therefore, Article 22 of the GDPR grants the data subject the right not to be subjected to a decision based solely on automated data processing, including profiling, if such a decision produces legal effects or significantly affects them. Exceptions exist when such processing is necessary for a contract, is based on law, or relies on the explicit consent of the data subject (Regulation (EU) 2016/679 (General Data Protection Regulation), 2018, Art. 22, par. 1-2). Furthermore, the employment relationship embodies inherent conflicts of interest between the employer and the employee, and the aim of labour law is to bring these interests into balance as much as possible. This balance may be reflected, for example, in the employer's interest in restricting unauthorized disclosure of business information and protecting trade secrets to preserve operations and competitiveness, and *vice versa* in the employee's interest in having workplace privacy respected, which the employer is to some extent obliged to ensure, in accordance with the legal standard of 'reasonable expectation of workplace privacy,' which is not precisely defined (Reljanović & Knežević Bojović, 2025). To reconcile conflicting interests, the balancing

mandating transparency in reporting surveillance costs related to labour disputes (Lockwood, 2018e, 31).

test is applied, designed to determine which (legitimate) interest, in the specific case, should be given priority and to what extent. In essence, this balances the employee's expectation of privacy against the employer's legitimate interests (Kovač Orlandić, 2018, 73), thereby preventing abuse of managerial powers and avoiding unethical practices.Therefore, the employer is obliged to respect the standard of transparency and objective justification when undertaking actions that restrict employees' workplace privacy. Transparency, in the broadest sense, means that the employer must inform employees in advance, clearly and unequivocally, about any potential privacy limitations. Transparency does not only concern the possibility of restricting the right to privacy, but must also ensure that employees are aware of the legitimate reasons (purpose) justifying such restriction, the methods (means) of restriction, duration, and the consequences of such measures (Kovač Orlandić, 2018a, 69). Therefore, employees must be informed about the measures implemented by the employer, and these measures must have objective justification, which is reflected in the protection of the employer's interests (property, persons, and the like), in accordance with the principle of proportionality. Restrictions on employee privacy and personal data protection must be consistent with the principle of data minimization, requiring that such measures be undertaken to the minimal extent necessary.[5] Accordingly, employers are obliged to inform employees about all aspects of privacy (or lack thereof) in the workplace, including situations where work is performed remotely or at the employee's home. Furthermore, invasive measures applied by the employer must be reduced to a minimum, and any restrictive measures must be proportionate, minimally invasive, and objectively necessary (Reljanović &Knežević Bojović, 2025a, 42).

Electronic surveillance may be carried out at any time and in any location, whether physical or virtual, with the workplace and working hours serving as the dividing line between the professional and private spheres, thereby defining the permissible scope of employer oversight. Work tools provided by the employer are subject to the employer's control, with the establishment of a clear policy on the use of official electronic work tools (in accordance with the principle of transparency). Thus, where an employee uses an official phone for private communication during rest periods, employer surveillance of such calls would be unlawful, as the employee's

[5]For example, installing video surveillance in employer restrooms or changing rooms would constitute invasive and excessive control without objective justification, whereas justification would exist if video surveillance were installed in warehouses (for the protection of property).

privacy interest prevails over the employer's potential claims.[6] Accordingly, employees must be timely and thoroughly informed about the level of privacy they can expect in the workplace and when using official communication tools (Reljanović&Knežević Bojović, 2025b, 91). Access by employers to employees' professional electronic communications, where employees have been previously informed of such a possibility, may occur only when necessary for security or other justified reasons. In cases of employee absence, employers should take necessary measures and establish appropriate procedures to allow access to professional electronic communications only when such access is professionally necessary. Access should be carried out in the least intrusive manner and only after the concerned employees have been notified. Private electronic communications at work are excluded from monitoring under all circumstances (CM/Rec(2015)5, Art. 14). Essentially three main surveillance measures could be found in the case law of European Court of Human Rights: phone wiretapping and reading of emails, monitoring of activities on company devices (reading employees' communications or opening saved files) and video surveillance on company premises. In case (Florindo De Almeida Vasconcelos Gramaxo v. Portugal)[7] introduces a new surveillance technology into the Strasbourg jurisprudence: the Global Positioning System (GPS). Mr. Florindo's use of the company vehicle was continuously monitored for three years through two software systems, one publicly disclosed and one concealed. A technical inspection revealed interference with the primary GPS. By cross-referencing data from both GPS devices and the employee's own entries, the employer determined that Mr. Florindo had deactivated the primary GPS during weekends and public holidays,

[6] In the same vein, in *Copland v. United Kingdom,* the European Court of Human Rights affirmed that employee electronic communication enjoys privacy protection. Such protection, however, is not absolute and may be limited exceptionally, though in this particular decision it did not elaborate on what such circumstances might look like (Reljanović&Knežević Bojović, 2025c, 91). Employees must use electronic communication tools responsibly and refrain from misusing official resources for private purposes. Conversely, it is essential that the employer anticipates possible computer monitoring in its general acts, provided that less intrusive methods are employed in accordance with the principle of proportionality. Employers may also restrict access to non-essential applications not required for the performance of work (such as filters limiting access to Facebook, Twitter, YouTube, or TikTok), as these reduce efficiency and productivity and are not necessary for the execution of work tasks. Of course, such limitations depend on work design, since they may be useful for employees engaged in digital marketing.

[7] Florindo de Almeida Vasconcelos Gramaxo v. Portugal - 26968/16, Judgment 13.12.2022 [Section IV].

underreported mileage, and failed to fulfill the contractually required eight-hour workday. On these grounds, the pharmaceutical company terminated his employment (Molè& Mangan, 2022). The court found the termination of the contract lawful. The applicant's right to private life had been proportionally reduced to safeguard the employer's right to control his expenses (Molè& Mangan, 2022a, p. 698). This statement is problematic as it represents the first case before the European Court of Human Rights concerning GPS surveillance. The Court failed to address whether the employer could have relied on less intrusive means to achieve its objectives, raising significant concerns about the adequacy of its reasoning (Reljanović & Knežević Bojović 2025b, 107).

The fact is that digital surveillance is everywhere and at any time, and it's pervasive, including emotions, communication, and human behaviors. Jaser and Tourish stressed that in a neoliberal system, hegemonic surveillance prevails as part of a totalistic form of management. Therefore workers risks become cyberized (adaptible to digital technology or culture) and thespianized, in that they must perform in ways prescribed by the technology (Jaser&Tourish, 2024a).[8] Many employers still need to create or update policies that inform employees' expected use of technology (e.g. to avoid presenteeism), guide the managerial use of monitoring tools and set healthy boundaries in order to promote a better work–life balance among remote workers (Jaser&Tourish, 2024b, Jamal *et al.*, 2021; McDaniel *et al.*, 2021).

Video surveillance as a special form of digital surveillance

From a comparative law perspective, there are no general rules specifically regulating the use of video surveillance; its application is governed within the broader framework of personal data protection legislation.[9] Video surveillance has been widespread in employer practices

[8] There are too many examples of such a surveilance. There are examples of organizations that monitor how much employees exercise, what they eat and drink, and, in some cases, even how much they sleep. One company provided fitness-tracking devices for employees (e.g. Fitbit) while persuading insurance companies to reduce costs for the company. Some Chinese companies have adopted the use of 'helmets and hats to scan workers' brainwaves and detect fatigue, stress and even emotions such as anger' for drivers of high-speed trains. The suggestion that all this is beneficial neglects the erosion of workers' privacy and the increased blurring between employees' work and non-work lives (Jaser & Tourish, 2024c).

[9] Law on Personal Data Protection in Montenegro explicitly stipulates under which circumstances video surveillance is permitted only in official or business premises when necessary to protect persons, property, classified information, or trade secrets, and only if such protection cannot be achieved otherwise. Video surveillance is prohibited in official and business premises outside the workplace, particularly in changing rooms, elevators,

for several decades. It is permitted subject to certain exceptions, but it may not be introduced for the purpose of collecting evidence in disciplinary proceedings against employees, particularly in accordance with the case law of the French Court of Cassation. It remains an open and contested question whether monitoring employee efficiency during the work process can be categorized as a legitimate aim for the introduction of video surveillance (Reljanović&Knežević Bojović 2025d, 111)[10] Video surveillance is most commonly used in workplaces, yet there are instances where employees are required to keep it continuously on while working from home. Such practices raise concerns not only with respect to the employee's privacy but also with respect to their family members, unless the work is performed in a separate room inaccessible to others. The most common legitimate interests on the part of employers are those aimed at ensuring occupational safety, the protection of persons and property, the prevention of theft and damage to valuable assets, or the supervision of hazardous production processes. In workplace environments, video surveillance is most commonly conducted through visible cameras; however, there are also instances where cameras are disguised within everyday objects (such as clocks, pictures, or radios), which may be classified as covert surveillance measures (Žarković, 2015, 171). Before introducing video surveillance, the employer is advised to conduct a self-assessment. This involves determining the specific purpose (legitimate aim) for which surveillance is being implemented and assessing whether that aim could be achieved by other appropriate, less intrusive means that would impose a lesser restriction on the employee's privacy (Kovač Orlandić, 2018b, 136). In addition, the principle of transparency must be satisfied: employees must be informed, and the decision to introduce video surveillance should be prominently displayed together with a notice that the premises are under surveillance. Moreover, from a comparative law perspective, the consent of works councils or trade unions is often required prior to adopting such a decision, as is the case in Sweden. The International Labour Organization, in its Guide, states that if workers

sanitary facilities, and areas designated for clients and visitors. The introduction of video surveillance requires a formal decision, and before its adoption, the employer is obliged to obtain the opinion of the representative trade union or employee representatives (Law on Personal Data Protection, 2008, Art. 36, Par. 2–4).

[10]One of the opinions of the Commissioner for Information of Public Importance and Personal Data Protection emphasizes that if the purpose of video surveillance is solely to monitor employees' regular activities and behavior during working hours to monitor their performance, such processing of personal data is not permitted (Reljanović&Knežević Bojović 2025e, 114).

are monitored, they must be informed in advance of the reasons for monitoring, the schedule, the methods and techniques used, and the data that will be collected. The employer is obliged to minimize intrusion into workers' privacy. Monitoring must be time-limited until its purpose is achieved. Continuous monitoring should only be allowed if necessary for the protection of health and safety at work or for the protection of property (ILO, 1997, 4).

The regulation of video surveillance as an autonomous legal institution remains absent from the corpus of domestic legislation. In practice, the applicable framework is derived from the general principles and legal bases enshrined in the Personal Data Protection Act. Consequently, the introduction of such regulation *de lege ferenda* would be both necessary and desirable. Comparative insights, particularly the Montenegrin experience, provide a valuable reference point, illustrating how practice can inform the development of a coherent and specialized legal framework. Secret video surveillance should not normally be undertaken, but it may be used in rare situations, only for the purpose of property protection, i.e., to conduct an investigation into theft and fraud, and when it is in line with national legislation. Secret video surveillance in labour law is indeed interpreted very restrictively, especially in German judicial practice. The German Federal Labour Court held that such measures may be used only when the employer has no alternative and video surveillance is the only way to clarify a serious breach of the employee's obligations (Kovač Orlandić, 2018c, 139).

CONCLUSION

The use of digital monitoring in the workplace must be designed to establish a fair balance between the competing interests of employers and employees. This balance requires a clear delineation of the employer's legitimate interests, which should ideally be regulated by specialized provisions within labour law rather than being left solely to general data protection statutes.The introduction of algorithmic management and automated decision-making systems intensifies the inherent power asymmetry between employers and employees. In such a context, unilateral employer decisions regarding surveillance technologies risk undermining workers' rights and trust. Therefore, the governance of these tools should be addressed primarily through collective bargaining between social partners, rather than imposed unilaterally. Information and consultation with employees or employee representatives relating to monitoring might develop a more constructive relationship and also elicit views from

employees, helping develop a more transparent, fairer and tolerant workplace context. This could be beneficial to the mental health of workers in general and could create practices that are fairer and therefore more ethical.

An employer may utilize digital monitoring, as well as artificial intelligence systems and tools, to track workers' productivity and behavior, provided that constitutionally guaranteed labour rights and statutory rights are respected—particularly the right to privacy, the protection of personal data, and the prohibition of discrimination. Such monitoring should remain confined within the temporal and spatial boundaries of the working relationship, namely the workplace and working hours, taking into account the specific nature of certain types of jobs performed remotely, and must be accompanied by a clear emphasis on the employer's duty of care and the duty to foster trust to sustain a healthy and safe working environment.

It is important to conclude that the employer has the obligation to inform workers when certain digital surveillance systems are used to monitor their work. In accordance with the principle of transparency, any infringement of employees' labour and social rights - particularly the right to workplace privacy and the protection of personal data - must comply with the principles of proportionality and minimization, meaning only to the extent strictly necessary and with the least possible restriction of rights. The employer's interest in restricting rights must not only be legitimate but must also outweigh the employee's interest in preserving full privacy protection.

The current regulatory framework governing workplace digital monitoring in Serbia remains fragmented and insufficiently clear. A coherent regulatory framework requires integrating labour law with data protection and privacy safeguards. Technology should be treated not merely as an employer-controlled tool but as a subject of collective bargaining, ensuring fair and ethical regulation of digital systems, particularly algorithmic management and automated decision-making. Such systems must remain under human oversight to guarantee accountability and prevent discrimination. A forward-looking regulatory framework must explicitly prohibit the continuous monitoring of workers' behavior, particularly when aimed at predicting their future conduct on the basis of personal characteristics-especially beyond the temporal and spatial boundaries of employment, as well as in situations irrelevant to the performance of work. Embedding human oversight and collective bargaining into the governance of algorithmic tools is essential to prevent unlawful practices and to preserve trust, fairness, and dignity in the workplace.

REFERENCES

1. Abraha, H. (2025). *Navigating workers' data rights in the digital age: A historical, current, and future perspective on workers' data protection*, pp. 1-63, ILO Working Paper 149 (Geneva, ILO), https://doi.org/10.54394/MLUH5441
2. Charter of Fundamental Rights of the European Union, 2012/C 326/02
3. CM/Rec(2015)5 - Recommendation of the Committee of Ministers to member States on the processing of personal data in the context of employment (Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies)
4. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1985
5. Deborah J. (2022). Remote workers' experiences with electronic monitoring during Covid-19: Implications and recommendations, *International Journal of Workplace Health Management*, vol. 15, 3/2022, pp. 395-396, Emerald Publishing, https://doi.org/10.1108/IJWHM-02-2021-0042
6. Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community - Joint declaration of the European Parliament, the Council and the Commission on employee representation, *OJ L 80, 23.3.2002*
7. Eurofound. (2022). Ethics in the digital workplace, Publications Office of the European Union, Luxembourg, pp. 1-47, Downloaded, Jun 10, https://www.eurofound.europa.eu/en/publications/all/ethics-digital-workplace
8. International Labour Office. (2026). How will the new convention n°193 promote decent work in the platform economy?. Downloaded, Jun 10, https://www.ilo.org/resource/article/how-will-new-convention-n%C2%B0193-promote-decent-work-platform-economy.
9. Kovačević Lj. (2014). Internet i privatan život zaposlenih: granice poslodavčevih nadzornih, disciplinskih i normativnih ovlašćenja [The Internet and Employees' Private Life: Limits of the Employer's Supervisory, Disciplinary, and Normative Powers case law]: in book Internet and society (pp. 337-353). Beograd i Niš: Srpsko sociološko društvo, Univerzitet u Nišu–Filozofski fakultet, Institut za uporedno pravo, Downloaded, Jun 15, https://www.researchgate.net/publication/377771973_Internet_i_priva

tan_zivot_zaposlenih_granice_poslodavcevih_nadzornih_normativnih_i_disciplinskih_ovlascenja

10. Kovačević Lj. (2013). Radnopravna zaštita građanskih sloboda i prava zaposlenih na mestu rada-prodor demokratskih vrednosti u svet rada ili kompenzacija za veću nesigurnost [Labour-Law Protection of Employees' Civil Rights and Liberties in the Workplace: The Penetration of Democratic Values into the Sphere of Labour, or Compensation for Increased Job Insecurity?], *Teme, br. 4/2013*, pp. 1583-1599, Niš, *DOI*: https://doi.org/10.1007/978-3-031-14360-1
11. Kovač Orlandić M. (2018). Pravo zaposlenog na privatnost i njegova zaštita, doktorska disertacija (neobjavljena) [The Employee's Right to Privacy and Its Protection] (pp. 1-436). Beograd: Pravni fakultet Univerziteta u Beogradu. Downloaded, Jun 25, https://nardus.mpn.gov.rs/bitstream/handle/123456789/10214/Disertacija.pdf?sequence=6&isAllowed=y
12. Lockwood G. (2018).Workplace Monitoring and Surveillance: The British Context, *Athens Journal of Law, Volume 4, Issue 3*. pp. 205-228, https://doi.org/10.30958/ajl.4-3-1.
13. Michele M. & Mangan D. (2022). 'Just more surveillance': The ECtHR and workplace monitoring, *European Labour Law Journal 2023, Vol. 14(4),* pp. 694–700, https://dx.doi.org/10.2139/ssrn.4861231
14. Misailović, J. (2023). *Elektronski nadzor zaposlenih – problem uspostavljanja ravnoteže između ovlašćenja poslodavca i prava zaposlenih na privatnost* [Electronic Monitoring of Employees – The Challenge of Establishing a Balance Between the Employer's Powers and Employees' Right to Privacy] In: Uporednopravni izazovi u savremenom pravu - In memoriam Stefan Andonović (pp. 323-337). Beograd: Institut za uporedno pravo; Pravni fakultet Univerziteta u Kragujevcu, DOI:10.56461/ZR_23.SA.UPISP_JM
15. Protection of workers' personal data.(1997). An ILO code of practice, International Labour Office, Geneva, (pp. 1-24), Downloaded, June 20, file:///C:/Users/RS/Downloads/wcms_107797-1.pdf
16. Rajić Ćalić J. &, Živković A. (2025). Legal protection of workers and employers when using artificial intelligence in the working environment, *Serbian Political Thought, 1/2026, Vol. 95*, pp. 45-71, DOI: 10.5937/spm95-61584
17. Regulation (EU) 2024/1689 of the European Parliament and the of the Counci of 13 June 2024 (Artificial Intelligence Act)

18. 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) (Text with EEA relevance) *OJ L 119, 4.5.2016,* 2018
19. Reljanović, M. & Knežević Bojović, Ana.(2025). Pravo na privatnost na radu [Right to privacy at work] (pp. 1-187). Beograd: Institut za uporedno pravo. Downloaded, June 10, http://ricl.iup.rs/2204/1/2025-Pravo-na-privatnost-na-radu.pdf
20. Zahira J. & Dennis T. (2024). Hegemonic Surveillance at Work: Fabricating the cyberized, totalized and thespianized employee, *Organization Theory, Volume 5, Issue 1*, https://doi.org/10.1177/26317877241235940
21. Zakon o elektronskim komunikacijama [Law on Electronic Communications]. Službeni glasnik RS, br. 35/23
22. Zakon o ličnim podacima [Law on Personal Data].Službeni list Crne Gore, br. 079/08 od 23.12.2008, 070/09 od 21.10.2009, 044/12 od 09.08.2012, 022/17 od 03.04.2017
23. Zakon o radu [Labour Law]. Službeni glasnik Reppublike Srbije, br. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 – odluka US, 113/2017, 95/2018 – autentično tumačenje i 109/2025 – dr. zakon
24. Zakon o zaštiti podataka o ličnosti [Law on Personal Data Protection]. Službeni glasnik RS, br. 87/2018
25. Žarković I. (2015). Mere elektronskog nadzora zaposlenih i pravo na privatnost na radnom mestu [Measures of electronic surveillance of employees and the right to privacy in the workplace], *Nauka, bezbednost, policija*, 2015, vol. 20, br. 3, (pp. 165-182), Beograd: Kriminalističko –policijski univerzitet, DOI: 10.5937/NBP1503165Z .