Review Article
DOI: https://doi.org/10.22598/iele.2025.12.2.9

HOLISTIC APPROACH FOR EMPLOYEES' PRIVACY PROTECTION IN THE CONTEMPORARY WORKPLACE

Andrijana Bilić *

ABSTRACT

The digital revolution and artificial intelligence have brought an array of new tools employers use in their business models and methods to control their employees which even have the potential to substantially affect employee's outcome. The extent to which management can now monitor employees' behaviours, both on-and-off site using advanced surveillance technologies, has dramatically increased creating a scenario of panoptic power management, whilst causing significant harm to employees' privacy issues. This raises concern whether widespread surveillance of the employees goes far beyond what is reasonable and necessary. In that context, the author examines the possible solutions to the question of the paramount importance: what can be done to strike a right balance between employees' right to privacy and protection of employers' business interests, avoid elevated conflict and inefficiencies and potential litigation in transforming employment relations?

***Key words**: right to privacy, surveillance, principles of privacy protection at the workplace, European Convention on Human Rights (ECHR), GDPR, Platform Work Directive, Artificial Intelligence Act.*

1. INTRODUCTION

This article gives an overview of the current practices, developments and controversial issues surrounding surveillance in the workplace, in particular the protection of the employee's right to privacy[1] as one of the fundamental human

* University of Split, Faculty of Law, Split, Croatia, andrijana.bilic@pravst.hr

[1] United Nations General Assembly: *Universal Declaration of Human Rights from 1948*, 1948, art. 12; Council of Europe: *European Convention on Human Rights and Fundamental*

rights[2]. Following the changes imposed by globalization and digital transition, we are witnessing modern employment relationship which is characterized by an increasing importance of the employer's control over the activities and data related to the employee. That is, we are witnessing a shift from the traditional workplace to hybrid and remote practices in which companies have become reliant on digital technologies and AI platforms to conduct core business. But, the application of those technologies in the workplace increases the possibilities for hierarchical management and digital surveillance in the way that has been unimaginable by now and even not desired.[3] Thus, the possibility of consumption of the right to privacy by employees increasingly enters the domain of the employer's jurisdiction.[4] Work and employee become almost indivisible. In the context of transforming employment relationships, the concept of privacy has become full of ambiguities, paradoxical and often leading to the collision of certain categories which are going to be discussed in the following chapters.

2. THE RIGHT TO EMPLOYEE' PRIVACY V PROTECTION OF EMPLOYERS' INTERESTS

The right to privacy, as one of the fundamental human rights, is very hard to define. In the literature, there is no unique, universal definition of the concept of privacy.[5] Its precise determination is often burdened by historical and cultural factors. However, regardless of nuances deriving from different legal

Freedoms, 1950, art. 8; Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities*, C 364/1, 2000, art. 7.

[2] Fundamental human rights are classified into six basic categories: dignity, freedom, equality, solidarity, civil rights and justice.

[3] Moore, P. V., Upchurch, M., Whittacker, X.: Humans and machines at work: monitoring, surveillance and automation in contemporary capitalism, in: Moore, P. V., Upchurch, M., Whittacker, X (eds.): *Humans and machines at work: monitoring, surveillance and automation in contemporary capitalism, Dynamics of Virtual Work* (pp. 411-428), Cham: Palgrave Macmillan Cham, 2018.

[4] Ramm, T.: Introduction, in: Schmidt, F. (ed.): *Discrimination in employment*, Stockholm: Almquist &Wiksell International, 1978, p. 27.

[5] Moore, A.: Defining privacy, *Journal of Social Philosophy*, 39(3) 2008, p. 411; Kuner, C. et al.: Privacy-an elusive concept. *International Data Privacy Law*, 1(3) 2011, pp. 141-142; ALibeigi, A., Munir, A. B., Ershadul, K.: Right to Privacy, a Complicated Concept to Review, *SSRN Papers,* 2020.

texts, starting from international declarations[6], conventions[7], regulations[8], directives[9], guidelines[10] to national constitutions[11] and civil codes[12] in defining of the concept of privacy, it is necessary to start from common values, i.e. promotion of the necessity of defence against endangerment of a person and

[6] International Covenant on Civil and Political Rights: *United Nations Treaty Series 999* (entry into force 23 March 1976), United Nations, 1966 in art. 17 state: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

[7] European Convention on Human Rights states: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." Charter of Fundamental Rights of the European Union in art. 7 states: *"Everyone has the right to respect for his or her private and family life, home and communications."* Council of Europe: *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, (108) 1981.

[8] European Parliament and Council of the European Union: *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Official Journal of the European Union (L 119) 2016, pp. 1-88.

[9] European Parliament and Council of the European Union: *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal of the European Communities, (L 281) 1995, pp. 31-50.

[10] Organisation for Economic Co-operation and Development: *OECD guidelines on the protection of privacy and transborder flows of personal data*, Paris: OECD Publishing, 2002; Organisation for Economic Co-operation and Development: The OECD privacy framework, Paris: OECD Publishing, 2013.

[11] German constitution (Grundgesetz from 1949) in art. 10 states: "(1) The privacy of correspondence, posts and telecommunications shall be inviolable. Constitution of the Republic of Croatia states: "Respect for and legal protection of each person's private and family life, dignity, and reputation shall be guaranteed (art. 35) and "The freedom and privacy of correspondence and all other forms of communication shall be guaranteed and inviolable. Restrictions necessitated by the protection of national security and the conduct of criminal prosecution may be prescribed solely by law (art. 36), Federal Republic of Germany: *Bundesgesetzblatt*, (1), 23.05.1949).
(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

[12] Republic of Italy: *Gazzetta Ufficiale della Repubblica Italiana, Serie Generale, n. 174, Supplemento Ordinario*, (123), 29.07.2003 legislative decree n. 196 of 30 June 2003 (the "Italian Privacy Code") modified by legislative decree n. 101 of 10 August 2018.

his/hers closest determining features. However, without knowing what privacy is, it is hard to ensure an effective legal protection against infringements. It means that privacy must be reinterpreted in the light of the current era and be examined in the current context. So, we could cite here as a starting point one definition of privacy: "A person has privacy to the extent that others have limited access to information about him, limited access to the intimacies of his life, or limited access to his thoughts or his body". This definition is especially interesting in the context of intrusion into privacy of employees in the workplace which will be in the focus of this paper.

In the contemporary workspaces, some human resource management techniques require stronger loyalty of the employee to the employer by strengthening the employer's control over the activities, behaviour and attitudes of employees, not just at work, but also in his/her private sphere, in other words, by the intrusion into employee's privacy. Such employer's control can, in short, be justified by the need[13] for reliability, responsibility, productivity, and effectiveness.[14] As a result, the need for employers to be familiar with the physical and mental state of employees, their motivations, relationships, beliefs, experiences, abilities, ideas, religious beliefs, political opinions, offspring, ethnic background, etc., is growing exponentially.[15] On the other side of the employment relationship. there are opposed interests for the protection of the employee's privacy. The justification for the protection of the privacy of the employee can be observed from several aspects, such as the protection of the limited autonomy, dignity and well-being and freedom of expression of employees[16], possibility of self-evaluation of employees and the creation and maintaining

[13] Regan, P. M., *Legislation Privacy: Technology, Social Values, and Public Policy*, New York: Oxford University Press, 1995, p.188.

[14] Vaught, B. C., Taylor, R. E., Vaught, S. F.: The attitudes of managers regarding the electronic monitoring of employee behaviour: Procedural and ethical considerations, *American Business Review*, 18(1) 2000, pp.107–114.
Hendrickx, F.: Employee Privacy, in: Blanpain, R. (ed.): *Comparative Labour Law and Industrial Relations in Industrialized Market Economies*, Alphen aan den Rijn: Kluwer Law International, 200l, pp. 465-488.

[15] Blanpain, R.: Employee Privacy Issues: Belgian report, *Comparative Labour Law Journal*, 17 1995, pp. 38-39.

[16] Weiss, M.: Re-Inventing Labour Law?, in: Davidov, G., Langille, B. (eds.): *The Idea of Labour Law*, Oxford: Oxford Academic., 2011, p. 44; Finkin, M, W.: Menchenbild: The Conception of the Employee as a Person in Western Law, *Comparative Labor Law & Policy Journal*, 23(2) 2002, p. 577; Freedland, M, Kontouris, N.: *The Legal Construction of Personal Work Relation*, Oxord: Oxford University Press, 2011, p. 373. Also, importance of the dignity can be seen in the Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities*, (C 364/1) 2000 in art. 31 *"every employee has the right to working conditions which respect his or her health, safety and dignity"*.

of a relationship of mutual trust between the employee and the employer.[17] So, in the employment relationship, there is inherent conflict between aforementioned interests of the employer and free enjoyment of employees' human rights, more precisely, the right to privacy. To what degree these rights can be limited will depend primarily on the balance of concrete interests. So, it is of utmost importance to strike the right balance between aforementioned competing interests. But it is easier said then done. Namely, the employment relationship is characterised by the inequality of bargaining power between employer and employee. Although the inequality of bargaining power is mostly evident before the commencement of employment relationship, in the bargaining phase, it continues through the duration of employment relationship. So, act of concluding an employment contract is an act of employee's voluntary submission[18] to employers' control and supervision of the activities regarding the execution of the work, the possibility of applying disciplinary powers and organizing the work. This is possible due to the fact that employment relation is, in organisational sense, best described as a structure of governance with democratic deficits[19] or subordination.

3. SURVEILLANCE IN THE CONTEMPORARY EMPLOYMENT RELATIONS

In the last several decades, we have witnessed increased use of digital technologies by the employers in the workplace to capture and analyse employee data, electronically monitor their employees and manage them using algorithms.[20] Employers are using algorithms to track their productivity (so called Bossware), predict employees behaviours at work and future health condition, their intention to become member of the trade union, private plans such as family planning as well as to bring decisions about their job assignment and promotion. The revolution in big data and artificial intelligence has brought an array of new tools employers use in their business models and methods they employ to control their employees which even have the potential to substantially af-

[17] Wacks, R.: *Privacy and the Law, Oxford: Clarendon Press, 1989*, pp. 11-12.

[18] Freedland, M., Davies, P.: *Kahn-Freund's Labour and the Law*, London: Stevens & Sons, 1983, p. 18.

[19] Davidov, G.: *A Purposive Approach to Labour Law*, Oxford: Oxford University Press, 2016, p. 36.

[20] Kellogg, K., C., Valentine, M. A., Christin, A.: Algorithms at work: The new contested terrain of control, *Academy of Management Annals,* 14(1) 2020, pp. 366-410; Bailey Diane E., Emerging technologies at work: Policy ideas to address negative consequences for work, employees, and society. *ILR Review* 75(3) 2022, pp. 527-551.

fect employee's outcome.[21] The way employers use those technologies is often unclear, not only to employees, but also to policy makers. They are either still operating in the legal vacuum or within legislation that reinforce managerial prerogatives or reflect distrust in employees. The lack of regulation leads to strong incentives for employers to use digital technologies at will, in the ways that can directly or indirectly harm employees. Some of this harm stems from technology design decisions, but more often is derived from employers' poor decisions regarding when, why, where and how to use this technology.[22] Bad decision could, beside the danger of the intrusion into the privacy[23], lead to other common harms for employees such as: work intensification[24], health and safety harms[25], de-skilling[26], job loss[27], bias, discrimination[28], suppression of

[21] In more detail: Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: Public Affairs, an imprint of Perseus Books, 2019.

[22] Cappelli, P.: Stop overengineering people management, *Harvard Business Review*, (September-October) 2020.

[23] Segal, E.: How productivity and surveillance Technology can create a Crisis for Businesses, *Forbes*, 18.08.2022; Stanley, J., The Nightmarish loss of workplace Privacy, ACLU, 26.08.2022; Schaub, F., Andalibi, N.: Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy, in: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, (pp. 1-20), Hamburg; ACM.

[24] Schaupp, S.: Cybernetic proletarianization: Spirals of devaluation and conflict in digitalized production, *Capital & Class,* 46(1) 2021, pp. 11-31; Gutelius, B., Theodore, N.: *The Future of Warehouse Work: Technological Change in the U.S. Logistics Industry*, Berkeley: UC Berkeley Labor Center; Working Partnerships USA, October 2019, pp. 53-56; Carre´, F., Tilly, C.: Digital technology implementation in US retail stores: Trends, potentials, and contingencies, *ILR Review*, 75(4) 2022. pp. 807-856.

[25] Ravid, D. M. et al.: A meta-analysis of the effects of electronic performance monitoring on work outcomes, *Personnel Psychology*, 76(1) 2022, pp. 5-40; Ockenfels-Martinez, M., Sukhdip P. B.: *The public health crisis hidden in Amazon warehouses*, Human Impact Partners and Warehouse Employees Resource Centre, January 2021; O'Brady, S., Doellgast, V.: Collective voice and employee well-being: Union influence on performance monitoring and emotional exhaustion in call centres, *Industrial Relations: A Journal of Economy and Society*, 60(3) 2021, pp. 307-337; Gordon, J. L.: Under pressure: Addressing warehouse productivity quotas and the rise in injuries, *Fordham Urban Law Journal*, 49(1) 2021, pp. 149-189.

[26] Levy, K., Barocas, S.: Privacy at the Margins| refractive surveillance: Monitoring customers to manage workers, *International Journal of Communication*, 12 2018, pp. 1166-1188.

[27] Kuang-Hsien Wang, K. H., Lu, W. C.: AI-induced job impact: Complementary or substitution? Empirical insights and sustainable technology considerations, *Sustainable Technology and Entrepreneurship*, 4(1) 2025, pp. 100085; Soueidan, M., H., Rodwan, S.: The impact of artificial intelligence on job loss: risks for governments, *Technium Social Sciences Journal*, 57 2024, pp. 206-223.

[28] Rosenblat, A. et al.: Discriminating tastes: Customer ratings as vehicles for bias, *Data & Society: Intelligence and Autonomy,* 9(3) 2016, pp. 1-21.

the right to organise[29]and loss of autonomy and dignity[30]. So, taking into account all those harms for the employees coming from the use of surveillance technology the following question arises: what leads organisations (employers) to further jeopardize trust issue, be it between collective parties of employment relationship or between employer and employee, promoting that way the constructive conflict management?

It is completely obvious that these days socioeconomic environment has changed forcing organizations to high-speed adaptation. Among challenges that current organisations are facing are: decrease of working conditions which creates a tension in the workplace, deinstitutionalisation and alternative forms of employees' representation, globalisation, decrease of unionisation rates, decentralization of collective bargaining (from sectoral to organisational level), individualisation of employment relations, participative decision making process – social dialogue and power asymmetry; adaptation to environmental changes, diversity and gender inequality, digital workplace and ageing and youth employment.[31] So, aforementioned challenges could explain, but could they necessarily justify employers' behaviour regarding lack of trust in their employees and increased need for their surveillance?

So, when employer's need for information and employee's privacy intersect, it is of utmost importance to maintain the correct balance between rights, policies and practices. Incorrect balance can result in negative repercussions such as elevated conflict and inefficiencies, possible perception of person violation and potential litigation.[32] The next question of paramount importance is: what can be done to avoid or to minimize the aforementioned risk of intrusion into employees' privacy?

In order to strike the right balance between employees' right to privacy and protection of employers' business interests, avoid elevated conflict and inefficiencies and potential litigation,this author is advocating the general principles for the employees' privacy protection set by the European Court of Human Rights as well as those which can be drawn from legal, binding, but mostly

[29] Kessler, S.: Companies are using employee survey data to predict - and squash - Union organizing, 14.01.2021.

[30] Groves, K. S., Margolis, J., Gibson, C.: Cultivating the experience of dignity at work during digital transformation: Protective & proactive strategies for leaders and organizations, *Organizational Dynamics*, 54(3) 2024, pp. 101103.

[31] Elgoibar P., Euwema M., Munduate, L.: Building Trust and Constructive Conflict Management in the Organisations, in: Elgoibar, P., Munduate, L., Euwema, M. (eds.): *Industrial Relations and Conflict Management*, Cham: Springer International, 2016, pp. 6-8.

[32] Brown, W. S.: Technology, workplace privacy and personhood, *Journal of Business Ethics* 15(November) 1996, p. 1244.

non-binding instruments regarding processing of the personal data in employment context. These principles should serve as a guidance in the creation of legal arsenal, be it on the national or supranational scale, regulating the issue of the protection of the right to privacy and personal data protection specially designed for the workplace. Also, those principles should be used by national courts, as well as by the European Court of Human Rights (further: ECtHR) in the assessment of the compatibility of employees' surveillance with employees' right to privacy in the case of litigation.

Furthermore, this author is suggesting trust-based management as a better approach for striking the right balance between employees' right to privacy and protection of employers' business interests with the involvement of trade unions and other workers' representatives. Namely, collective agreements, information and consultation rights, and co-determination also enable *ex-ante* controls on the introduction of new technologies and limit risks and abusive practices for the intrusion into workers' privacy.

4. FUNDAMENTAL PRINCIPLES OF PRIVACY AND DATA PROTECTION IN THE WORKPLACE

The limitation of fundamental rights and freedoms, such as right to privacy, should be an exception and done only in the reasonable manner. At this point, the general principles of privacy protection at the workplace that should be respected so that intrusion into employee' privacy would be justified are going to be explained.

So, before looking into the principles set by the European Court of Human Rights in Barbulescu case, as well as those derived from binding and non-binding legal instruments, the proportionality principle and the concept of reasonable expectation of privacy should be clarified here.

4.1. PRINCIPLE OF PROPORTIONALITY

Related to this discussion is the idea of the concept or principle of the proportionality that has been applied in the field of labour law, specifically with regard to the right to privacy. It is an age-old ethical principle[33], but has originally become legally binding in the nineteenth century in Germany[34]. Originally it was

[33] Wattles, J.: *The Golden rule*, Oxford: Oxford University Press, 1996.

[34] Emiliou, N.: *The Principle of Proportionality in European Law, A Comparative Study*, Boston: Kluwer Law International, 1996, pp. 23-43.

used as a legal tool to restrict the use of police power, then the power of state[35] and its administrative bodies[36]. In recent years it has become a prominent principle in the sphere of labour law used for the restriction employers' prerogatives[37], as well as power by unions. The proportionality principle determines whether a specific violation of the rights or interests of an individual is proportional and therefore valid. So far, this principle has shown its value as a legal tool to prevent abuse of power and strike the right balance between conflicting interests. The decision considers to be proportional if it follows three secondary criteria (tests):

(1) there is a rational connection between the goal of violating the right/interests and the means of accomplishing it,
(2) there are no other possible and less restrictive means of achieving the goal,
(3) there is a proportionate balance between the social benefit of achieving the goal and the harm that may be caused to the rights or interests of the individual (proportionality *stricto sensu*).[38] Accordingly, in order to decide whether the violation of an employee's right to privacy by employers' decision or policy was proportional or not, three secondary criteria need to be implemented and specific rights and interests at stake need to be balanced (managing of the business *v* right to privacy). This means that in making decision which could possibly violate employees' right to privacy the employer must be considerate and, in protecting their own interests, choose rational and less intrusive means by which he could achieve the same goals, but at the same time minimize the extent of the intrusion into the employees' privacy. Those means should be beneficial for the employer, but at the same time should not be outweighed by greater harms to the employees. In the case of litigation regarding intrusion into the right of privacy of employee the judges are required to make proper evaluation about the importance of specific rights and interests in the concrete case. With that aim, the following questions should be posed: Is the measure introduced by the employer necessary to achieve specific interest? Is the loss of employees' privacy proportional to the benefit gained by the employer? Are there any

[35] Steiner, T., Netzer, L., Sulitzeanu-Kenan, R.: Necessity or balancing: The protection of rights under different proportionality tests-Experimental evidence, *International Journal of Constitutional Law*, 20(2) 2022, pp. 642-663.

[36] Borriello, F.: Principle of Proportionality and The Principle of Reasonableness, *Review of European Administrative Law*, 13(2) 2020, pp. 155-174.

[37] On the implementation of the principle of the proportionality in the sphere of the constitutional and labour law in the time of corona crisis in Croatia see more: Bilić, A.: Utjecaj COVID-potvrda na pravo na rad i radnopravni status radnika u Republici Hrvatskoj, *Zbornik radova Pravnog fakulteta u Splitu*, 59(3) 2022, pp. 513-548.

[38] Barak, A.: Proportionality and Principled Balancing, *Law & Ethics of human rights*, 4(1) 2010, pp. 1-16.

less privacy intrusive means for achieving the same result? The employer's behaviour in this context must be evaluated from the perspective of a "reasonable employer".[39]

4.2. REASONABLE EXPECTATION OF PRIVACY

This principle has a fundamental role regarding applicability of the art. 8 of the European Convention on Human Rights[40] (further: ECHR) which guarantees the right to respect for private, family life, home and correspondence. The first assumption of the meaning of the concept "reasonable expectation of privacy" would be that the employer is authorized to supervise the work of the employees during the working hours, since this period should be used for the implementation and improvement of the production process. The employee's right to privacy would therefore include those areas in the workplace where there is heightened expectation of privacy (toilets, cloakrooms, changing rooms etc.) as well as those spheres of employees' life that are realized outside of his work[41]. But areas where the public has access should be treated differently, that is with a low expectation of privacy. Although, the right to private life could cover activities that take place in public, but outside the work space and working time.[42] However, it is difficult and controversial to define those spheres of employee's life that are outside of the domain of his/her work for the employer. It should include not only those aspects of his/her life that are realized outside of working hours, but also those that do not have an indirect effect on their business life, and those that are not in the immediate domain of the employer. Let's clarify. It is difficult to specify those areas of an employee's life that do not have a potential impact on his/her business life.[43] Furthermore,

[39] Wedderburn, M.: Labour Law and the Individual, in: Rood, M., Lyon-Caen, G., Daubler van der Heijden, W. (eds.): *Labour Law in the post-industrial era. Essays in Honour of Hugo Sinzheimer*, Aldershot: Dartmouth, 1991, p. 41.

[40] Council of Europe: *European Convention on Human Rights and Fundamental Freedoms*, 1950 and additional protocols to the Convention (Protocols 1 (ETS No. 009), 4 (ETS No. 046), 6 (ETS No. 114), 7 (ETS No. 117), 12 (ETS No. 177), 13 (ETS No. 187), 14 (CETS No. 194), 15 (CETS No. 213) and 16 (CETS No. 214).

[41] European Court of Human Rights: *Halford v. the United Kingdom* (Application No. 20605/92), ECHR 32, 25.06.1997; European Court of Human Rights: *Copland v. the United Kingdom* (Application No. 62617/00), ECHR 253, 2007; European Court of Human Rights: *Özpınar v. Turkey* (Application No. 20999/04), ECHR 2268, 2010.

[42] European Court of Human Rights: *Sidabras and Džiautas v. Lithuania* (Applications Nos. 55480/00 and 59330/00), ECHR 395, 2004.

[43] In the judgment R v Dyment, the Supreme Court of Canada adopted the categorization of employee's privacy into three spheres: territorial (for example: search of personal mailboxes or

many activities undertaken outside working hours can also have a direct or indirect effect on the work relationship, for example if a truck driver loses their driving licence due to alcohol consumption. Also, there are aspects of the employee's personal life about which the employer must be informed, for example about their state of health if that state prevents them from performing their work efficiently. In addition, the presented assumption excludes some activities that (*per se*) represent an invasion of the employee's privacy, for example, installing hidden (covert) video surveillance or intercepting telephone calls[44] in the workplace. Finally, new forms of the work have brought blurring of the work and private life. When employees work remotely (e.g. from home)[45], or whilst they are travelling for business, monitoring of activities outside of the physical work environment can take place and can potentially include monitoring of the individual in a private context. On the other hand, in the information society, employees spend more time at the workplace than ever before.[46] Therefore, they should be able to interact with the outside world, that is, they should be able to perform their daily private obligations via internet banking, online shopping or via other types of electronic media, i.e. the internet. The precondition is that the performance of these private obligations does not harm business interests of the employer.

The second assumption of the concept of reasonable expectation of privacy could imply that if the employer notifies an employee that he would be monitored, then the employee has no reasonable expectation of privacy. But, taking into account the inequality of the bargaining power between the employer and the employee, this interpretation would be unsuitable. Namely, the employer could set terms in employment contract that allow extensive surveillance practice. In that context, the contract of employment could serve as an instrument of domination of the employer over the employee.[47] This would mean that the employer can monitor every aspect of the employee's life, under the condition that the employee was

mailboxes, office, employee's vehicle); personal/physical (for example: drug testing, polygraph privacy testing; search and surveillance of employees); informational (for example: polygraph personality tests, drug tests, medical examinations, and supervision). See: Supreme Court of Canada: *R. v. Dyment*, 2 S.C.R. 417, 1988.

44 European Court of Human Rights: *Halford v. the United Kingdom* (Application No. 20605/92), ECHR 32, 25.06.1997.

45 Arroyo-Abad C.: Teleworking: A New Reality Conditioned by the Right to Privacy, *Laws,* 10(3) 2021, pp. 64.

46 Coyle, A.: E-mail and Internet Surveillance: Do Employees have a Right to Privacy? *Internet Law 'Bulletin*, 6(3) 2003, pp. 31-33.

47 Mantouvalou, V.: Advancing Human Rights, Capabilities and Non-Domination at work, in: Davidov, G., Langille, B., Lester, G. (eds.): *Oxford Handbook on the Law of Work*, Oxford: Oxford Academic, 2024, p. 118.

previously informed. In this way, the contractual terms could waive employees' right to privacy which is not compatible with art. 8 of ECHR.

4.3. EUROPEAN COURT OF HUMAN RIGHTS – LIST OF EMPLOYEES' PRIVACY PROTECTION PRINCIPLES

The European Court of Human Rights (further: The Court) in the case of Barbulescu v Romania[48] stated that reasonable expectation of privacy could not only depend on notification by the employer, but also on the normative threshold. Otherwise, this could lead to employer dominion over the worker. So, the Court listed the following relevant factors that national courts use in the assessment of the compatibility of monitoring with the art. 8 of the Convention:

- whether the employee has been clearly and in advance notified about monitoring and its nature;
- the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy;
- whether the employer has provided legitimate reasons to justify monitoring;
- whether it would have been possible to establish a monitoring system based on less intrusive methods and measures;
- the consequences of the monitoring for the employee concerned;
- whether the employee has been provided with adequate safeguards.

4.4. EMPLOYEES' PRIVACY AND DATA PROTECTION PRINCIPLES DERIVED FROM BINDING AND NON-BINDING SUPRANATIONAL LEGAL INSTRUMENTS

Regarding the protection of employees' personal data, general data protection instruments[49], particularly The General Data Protection Regulation (GDPR),

[48] European Court of Human Rights: *Bărbulescu v. Romania* (Application No. 61496/08), ECHR 742, 2017.

[49] European Parliament and Council of the European Union: *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal of the European Communities, (L 281) 1995, pp. 31-50; European Parliament and Council of the European Union: *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Official Journal of the European Union (L 119) 2016, pp. 1-88 and European Parliament and Council of the European Union: *Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such*

have created a harmonised, consistent and comprehensive regulation of personal data processing, built around the data protection principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.[50] Although they are generally applicable in the employment context, in the sphere of employment they do not have such a successful story. Namely, data protection is one of the few areas where Member States could not reach agreement. So, what is distinctive about personal data protection in employment context and why does it need special regulatory treatment? In the first instance, there is the intrusiveness and scale of technologies deployed, meaning that processing of personal data in the context of employment is greater in range, volume and impact than in other contexts. The second distinct feature is the specific nature of the employer-employee relations characterised by the inequality of bargaining power and, in that regard, the consent of the employee regarding surveillance in the workplace is questionable. The third distinguished feature of personal data processing in employment context is its collective dimension. Namely, collective rights and interests are characteristic of labour law, but they do not easy fit in the GDPR, which regulates individual data subjects and individual rights.[51] So, political and legislative compromise regarding the protection of the personal data in the employment relationship context was "opening clause" under art. 88 of the GDPR, granting Member States regulatory leeway to enact their own legislation in the area of employee data protection adopting diverse regulatory rules (legislation, collective agreements, or combination of those two) which should include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights. But still two issues remain. The first one refers to the quality of the substantive content. Namely, should these regulatory models stick to the minimum requirements of the GDPR or provide stricter and more protective provisions.[52] The second issue refers to the

data, Official Journal of the European Union, L 295, 2018, pp. 39-98, and repealing European Parliament and Council of the European Union: *Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*, Official Journal of the European Communities, L 8, 2001, pp. 1-22.

[50] European Parliament and Council of the European Union: *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Official Journal of the European Union, L 119, 2016, art. 5.

[51] Abraha, H. H.: A pragmatic compromise? The role of the Article 88 GDPR in upholding privacy in the workplace, *International Data Privacy Law*, 12(4) 2022, pp. 278-279.

[52] Müller, M., *Die Öffnungsklauseln der Datenschutzgrundverordnung: Ein Beitrag zur Europaïschen Handlungsformenlehre*, Muenster: Wissenschaftliche Schriften der WWU Münste, 2018.

purport of the concept 'suitable and specific measures' within the meaning of Article 88(2). It stays unclear how these substantive requirements and standards should be interpreted and transposed into the national provisions.

In search for answers, CJEU case law was consulted, as well as international and European regulatory, mostly non-binding, guidance for the work environment. Namely, as previously stated, the Court in Bărbulescu v Romania case set out a list of criteria that employee monitoring must meet in order to be proportionate. Also, great help could be provided by the ILO Code of practice on the protection of workers' personal data from 1997.[53], Recommendation CM/Rec (2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment,[54] Opinion 8/2001 on the processing of personal data in the employment context (WP48)[55], Working Document on the surveillance of electronic communications in the workplace (WP55)[56]and Opinion 2/2017 on data processing at work[57] adopted on 8 June 2017. Amongst the principles which can be drawn from these instruments regarding processing of the personal data in employment context are the following:

- the principle of legitimacy – personal data must be processed on a legitimate basis;
- the principle of necessity and proportionality - processing must be strictly necessary for these legitimate purposes (legitimacy) and proportionate to the risks faced by the employer;
- the principle of transparency - the employer must inform the employee in advance about the processing operations,
- the principle of finality - that workers' personal data should be processed only for specified, explicit, and legitimate purposes (purpose specification) and not further processed in a way incompatible with those purposes (fairness);
- the principle of information and consultation - workers' representative bodies (if applicable)
- must be informed and consulted in advance about specific data practices such as monitoring and surveillance.

[53] International Labour Organization: *Code of practice on the protection of workers' personal dana*, Geneva: ILO, 1997.

[54] Council of Europe, Committee of Ministers: *Recommendation CM/Rec(2015)5 to Member States on the processing of personal data in the context of employment*, 2015.

[55] WP291: *Opinion 08/2001 on the processing of personal data in the employment context (WP 48)*, European Commission, 2001.

[56] European Parliament and Council of the European Union: *Directive (EU) 2024/2831 on platform work*, Official Journal of the European Union, L 2831, 2024.

[57] WP29: *Opinion 2/2017 on data processing at work*, European Commission, 2017.

Given that the principle of proportionality has already been explained and the role of social partners in the protection of the right of privacy of employees would be explained in a separate chapter, in the following sections, the principle of legitimacy, the principle of transparency and the principle of finality will be explained.

The principle of legitimacy is in the centre of privacy and data protection law.[58] It means that processing personal data of employees would be legitimate when employer is obliged to process these data based on the legal obligations to which the controller is the subject, in the case of contractual or other legitimate interests and in order to protect the vital interests of data subject or some other natural person. So, what could represent employers' legitimate interests (purpose)? In particular, for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.[59]

The principle of transparency[60], in the sphere of data protection law, includes both, a prospective and retrospective element.[61] Prospective transparency

[58] ILO Code of Practice concerning the protection of worker personal data from 1996 states in art. 5.1. *"Personal data should be processed lawfully and fairly, and only for the reasons directly relevant to the employment of the worker"*; GDPR in art.6 states: *"Processing shall be lawful only if and to the extent that at least one of the following applies: the data subject has given consent to the processing of his or her personal data for one or more specific purposes; processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*

[59] GDPR, art. 88, p. 1.

[60] GDPR, art. 5 (1)(a). About the importance of the principle of transparency and the corporate responsibility in the digital area see more in: Reischauer, G. et al.: Transparency in an Age of Digitalization and Responsibility, *Schmalenbach Journal of Business Research*, 76 2024, pp. 483-494.

[61] Felzmann, H. et al.: Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns, *Big Data & Society*, 6(1) 2019, pp. 2053951719860542.

(*ex-ante* transparency) means that individuals (data subjects) must be informed by the data controllers (i.e. the organization processing personal data) about the ongoing data processing before such processing takes place. Such information must be provided in writing, in concise, easily accessible, easy-to-understand and clear and plain language, containing data on the controller, the quantity and quality of processed data, the time frame of the processing activities, the reason, and the purpose of processing. Retrospective transparency (*ex pos*t transparency) refers to the need for the explanation of how the particular decision was reached. This can be read out from the data controller obligation to produce a meaningful information to data subject about the logic involved as well as the significance and the envisaged consequences of data processing.[62] Although the right of the data subject to be given an explanation could give data subject remedies via *ex post* liability, it does not per se offer the data subject the protection from the consequences linked to that decision. So, it is of utmost importance to, taking into account the fact that current legal framework does not accurately protect the data subject from high-risk intrusion into their privacy, to give more weight to prospective element of the principle of transparency. This means that before collecting and processing data, the data controller should provide the data subject with the justification of the interference. In other words, reasonable interference demands the disclosure of why certain data is needed, why these inferences are necessary to achieve a specific processing purpose or decision, and *''whether the data and methods used to draw the inferences are accurate and statistically reliable[63]''*.

The principle of finality consists of two principles: the principle of purpose specification and the principle of fairness. Purpose specification means that personal data should be processed only for specified, defined, explicit and legitimate purposes which are adequate, relevant and limited to what is necessary. If personal data are to be processed for purposes other than those for which they were collected, the employer should ensure that they are not used in a manner incompatible with the original purpose, and should take the necessary measures to avoid any misinterpretations caused by a change of context.[64] Such a data in employment context could possibly be: application forms and work references; payroll and tax information-tax and social benefits information; sickness records; annual leave records; unpaid leave/special leave

[62] GDPR, arts. 13(2)(f), 15(1)(h).

[63] Wachter S, Mittelstadt B., Floridi L.: Why a right to explanation of automated decision-making does not exist in the general data protection regulation, *International Data Privacy Law*, 7(2) 2017, pp. 76-99.

[64] International Labour Organization: *Code of practice on the protection of workers' personal dana*, Geneva: ILO, 1997.

records; annual appraisal/assessment records; records relating to promoting, transfer; training, disciplinary matters; records relating to accident at work; information generated by computer systems; attendance records; family members; reimbursement of expenses, e.g. travel.[65]

Fairness means that personal data should be processed fairly in non-discriminatory manner and with the absence of fraud. According to art. 8 of the Charter of fundamental rights of the European Union[66], everyone has the right to fair personal data processing. Fairness can be seen broadly and interpreted in many ways. It is certainly connected with the question of legitimacy and with the purpose-limitation principle. Fairness of data processing also implies transparency.[67]

5. EMPLOYEES' PRIVACY AND DATA PROTECTION IN THE PLATFORM WORK DIRECTIVE AND THE ARTIFICIAL INTELLIGENCE ACT

At this point, the Platform Work Directive and the Artificial Intelligence Act in the context of employee privacy and data protection will be analysed in more detail. Directive 2024/2831 on improving working conditions in platform work [68] stresses that although digitalisation is changing the world of work, improving productivity and enhancing flexibility, it is also carrying some risks for employment and working conditions. Algorithm-based technologies, including automated monitoring systems and automated decision-making systems, have enabled the emergence and growth of digital labour platforms. But if unregulated, they can also result in technology-enabled surveillance, increase power imbalances and opacity about decision-making, and entail risks for decent working conditions, for the health and safety at work, for equal treatment and for the right to privacy.[69] In the sphere of algorithmic management, the Directive provides limitation on the procession on personal data by means of automated monitoring systems or automated decision-making systems from

[65] WP291: *Opinion 08/2001 on the processing of personal data in the employment context (WP 48)*, European Commission, 2001.

[66] Charter of Fundamental Rights of the European Union, *Official Journal of the European Union*, C 326, 2012, pp. 391-407.

[67] Council of Europe, Committee of Ministers: *Recommendation CM/Rec(2015)5 to Member States on the processing of personal data in the context of employment*, 2015.

[68] European Parliament and Council of the European Union: *Directive (EU) 2024/2831 on platform work*, Official Journal of the European Union, L 2831, 2024.

[69] European Parliament and Council of the European Union: *Directive (EU) 2024/2831 on platform work*, Official Journal of the European Union, L 2831, 2024, preamble (4).

the recruitment until the end of the employment relationship in the following situations:

(a) process any personal data on the emotional or psychological state of a person performing platform work;
(b) process any personal data in relation to private conversations, including exchanges with other persons performing platform work and the representatives of persons performing platform work;
(c) collect any personal data of a person performing platform work while that person is not offering or performing platform work;
(d) process personal data to predict the exercise of fundamental rights, including the freedom of association, the right of collective bargaining and action or the right to information and consultation as laid down in the Charter;
(e) process any personal data to infer the racial or ethnic origin, migration status, political opinions, religious or philosophical beliefs, disability, state of health, including chronic disease or HIV status, emotional or psychological state, trade union membership, sex life or sexual orientation;
(f) process any biometric data of a person performing platform work to establish that person's identity by comparing that data to stored biometric data of natural persons in a database.[70]

Taking into account that processing of personal data by a digital labour platform by means of automated monitoring systems or automated decision-making systems is a type of processing which is likely to result in a high risk to the rights and freedoms of natural persons, it is of utmost importance to carry out the assessment of the impact of the processing of personal data of this kind. Digital labour platforms, acting as controllers, shall seek the views of persons performing platform work and their representatives.[71]

Furthermore, in order to protect platform workers from unjustified intrusion into their fundamental rights to dignity and privacy, the Platform Work Directive obliges Member States to require from digital labour platforms to inform persons performing platform work, platform workers' representatives and, upon request, national competent authorities, of the use of automated monitoring systems or automated decision-making systems regarding the categories of data and action monitored, supervised or evaluated by such systems, including evaluation by the recipient of the service and the aim of the monitoring and how the system is to carry out that monitoring. The information shall be presented in written document, which may be in electronic form, in a transparent, intelligible and easily accessible form, using clear and plain language at the

[70] Art. 7, para 1.

[71] Art. 8.

latest on the first working day, prior to the introduction of changes affecting working conditions, the organisation of work or monitoring work performance or at any time upon their request.[72] Persons performing platform work shall have the right to the portability of personal data generated through their performance of work including ratings and reviews. Where the person performing platform work so requests, the digital labour platform shall transmit such personal data directly to a third party.[73]

One of the main concerns in the Artificial Intelligence Act[74] is to ensure that AI is trustworthy and ethically sound. The seven principles, established in 2019 Ethics guidelines for trustworthy AI[75], include human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being and accountability. Although recitals do not have the same legally binding status as the operative provisions which follow them and cannot overrule an operative provision, they can help with interpretation and to determine meaning. Privacy and data governance means that AI systems are developed and used in accordance with privacy and data protection rules, while processing data that meets high standards in terms of quality and integrity.[76] This is evident from the fact that the GDPR is a technology-neutral regulation. As the definition of "*processing*" under the GDPR is broad (and in practice includes nearly all activities conducted on personal data, including data storage), it is evident that the GDPR applies to AI systems. While AI is not explicitly mentioned in the GDPR, the automated decision-making framework[77] serves as a form of indirect control over the use of AI systems, on the basis that AI systems are frequently used to take automated decisions that impact individuals. At the same time, the relationship between AI and data protection is expressly recognised in the text of the EU AI Act, which states that it is without prejudice to the GDPR.

Although there is a clear overlap between many of the data protection principles and the principles and requirements established by the EU AI Act for the

72 Art. 9.

73 Art.9, para 6.

74 European Parliament and Council of the European Union: *Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, Official Journal of the European Union, L 1689, 12.07.2024.

75 High-Level Expert Group on Artificial Intelligence: *Ethics guidelines for trustworthy AI*, European Commission, 2019.

76 AI Act, recital 27.

77 GDPR, art. 22.

safe development and use of AI systems, understanding the synergies and differences between the GDPR principles and the EU AI Act principles will allow organisations to leverage their existing knowledge of the GDPR and their existing GDPR compliance programmes. This is therefore a crucial step to lower compliance costs. In order to guarantee right to privacy and protection of personal data throughout the entire lifecycle of the AI systems its, regular reviews and external audits are necessary to ensure regulatory compliance.

Some practice such as use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage, are considered high-risk practices and should be prohibited because they add to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy.[78]

Some AI systems used in employment for the recruitment and selection of persons, for making decisions affecting terms of the work-related relationship, promotion and termination of work-related contractual relationships, for allocating tasks on the basis of individual behaviour, personal traits or characteristics and for monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights. AI systems used to monitor the performance and behaviour of such persons may also undermine their fundamental rights to data protection and privacy.[79]

6. WHAT ABOUT MUTUAL TRUST? A LITTLE HELP FROM A FRIEND – TRADE UNIONS AND COLLECTIVE BARGAINING

These days socioeconomic environment has changed forcing organizations to high-speed adaptation. So, he aforementioned challenges could explain, but could they necessarily justify, employers' behaviour regarding lack of trust in their employees and increased needs for their surveillance? Is the fact that labour law has traditionally been structured and organized in a manner that demonstrates a lack of trust towards employees still actual, or has the trust issue become even more eroded?

In the recent period, managerial studies have shown that it is in the best interest of managers to trust their subordinates and to behave accordingly"[80]

[78] AI Act, recital 43.

[79] AI Act, recital 57.

[80] Brower, H.: A Closer Look at Trust Between Managers and Subordinates: Understanding the Effects of Both Trusting and Being Trusted on Subordinate Outcomes, *Journal of Management*, 35(2) 2009, p. 343.

and *vice versa* to support policies that make employee trust their managers. Despite that, most employers still behave in an old fashioned, traditional way. But we can see the sun emerge on the horizon. In line with an assertion: "… we could stress that trust is essential component of organisational success, stability and employee well-being"[81] as a main conclusion of new management studies, some businesses have adopted alternative management techniques – trust-based management[82] aimed at creation of workplace environment of mutual trust, less hierarchical structure[83] and increase in work time sovereignty for employees[84]. But, it is worth noting that although employees may feel more trusted by their employer, they still remain legally subordinated to their employers' prerogatives. Moreover, some scholars stress that trust and control are complementary rather than substitutes and that trust can reinforce control. To avoid this risk, it is of utmost importance to involve trade unions and other workers' representatives in the trust-based management process bolstering their right to collective bargaining[85] whose primary function is to rectify the

[81] Cheung, M., Wong, C., Yuan G.: Why mutual trust leads to highest performance: the mediating role of psychological contract fulfilment, *Asia Pacific Journal of Human Resources,* 55(4) 2017, p. 443; Connell, J., Ferres, N., Travaglione, T.: Engendering trust in manager-subordinate relationships: Predictors and outcomes, *Personnel review,* 32(5) 2003, p. 570.

[82] Tyagi, H., Kumar, R., Pandey, S.: A detailed study on trust management techniques for security and privacy in IoT: challenges, trends, and research directions, *High-Confidence Computing*, 3(2) 2023, pp. 100127; Tabak, F., Smith, W. P.: Privacy and electronic monitoring in the workplace: a model of managerial cognition and relational trust development, *Employee Responsibilities and Rights Journal,* 17(3) 2005, pp. 173-189; Richards, N., Hartzog, W.: Taking trust seriously in privacy law, *Stanord Technology Law Review,* (19) 2016, pp. 431-472; Xu, C. et al.: Trust-Based Collaborative Privacy Management in Online Social Networks, *IEEE Transactions on Information Forensics and Security*, 14(1) 2019, pp. 48-60; Ebert, I., Wildhaber, I., Adams-Prassl, J.: Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection, *Big Data & Society*, 8(1) 2021, pp. 20539517211013051.

[83] Kastelle, T.: Hierarchy is overrated, *Harvard Business Review,* 20.11.2013; Hamel, G., Zanini, M.: The $3 Trillion Prize for Busting Bureaucracy (and how to claim it), (28/16) 2016, p. 11.

[84] Ilsøe, A.: Between trust and control: company-level bargaining on flexible working hours in the Danish and German metal industries, *Industrial Relations Journal,* 41(1) 2010, pp. 34-51; Galea, C., Houkes, I., De Rijk, A.: An insider's point of view: how a system of flexible working hours helps employees to strike a proper balance between work and personal life, *The International Journal of Human Resource Management,* 25(8) 2014, pp. 1090-1111; Godart, O., Görg, H., Hanley A.: Trust-based Work Time and Innovation: Evidence from Firm-level Data, *ILR Review,* 70(4) 2017, pp. 894-918.

[85] De Stefano, V. et al.: Does Labour Law Trust Workers? Questioning Underlying Assumptions Behind Managerial Prerogatives, *Industrial Law Journal*, 53(2) 2024, pp. 206-238; Calacci, D., Stein, J.: From access to understanding: Collective data governance for workers. *European Labour Law Journal*, 14(2) 2023, pp. 253-282.

democratic deficit that is prevalent in employment relationship[86]. Harmonious coexistence between trust-based management and collective bargaining is also supported by the International Labour Organisation (ILO) and the Organisation for Economic Co-operation and Development (OECD)[87] and is also observed in some countries[88].

So, it should be stressed again that collective bargaining has a crucial role in the transition to a trust-based work environment. Collective labour rights and trade union initiatives are essential here because they make it possible to respond to employers' powers and initiatives comprehensively and to tailor responses to the reality of the sector or the company. Collective agreements, information and consultation rights, and co-determination also enable *ex-ante* controls on the introduction of new technologies and limit risks and abusive practices for the intrusion into workers' privacy.[89]

Before presenting surveillance policies at the workplace to the trade unions in the process of collective bargaining, especially when introducing new surveillance technologies, employers should constantly monitor employees' attitudes regarding proposed policies and procedures. At the end of the day such a behaviour on the side of employer increases chances of policy/practice acceptance and workplace harmony. Moreover, employers should take into account serious ethical dilemmas regarding workplace surveillance and in that regard three key variables in managing the ethics of workplace privacy: relevance (possible surveillance of employee's lives that are clearly and distinctly related to employment issues), consent (employee should have the right to withhold consent prior to any query that might violate privacy) and methods (use only methods that are reasonable and customary, and not those that are ethically questionable).[90]

[86] Davidov, G.: Collective Bargaining Laws: Purpose and Scope, *International Journal of Comparative Labour Law and Industrial Relations,* 20(1) 2004, pp. 81-106.

[87] ILO and OECD, *Building Trust in a Changing World of Work. The Global Deal for Decent Work and Inclusive Growth Flagship Report 2018*, Paris: Global Deal , ILO & OECD, 2018.

[88] Ilsøe, A.: Between trust and control: company-level bargaining on flexible working hours in the Danish and German metal industries, *Industrial Relations Journal,* 41(1) 2010, p. 46; Berg, P., Bosch, G., Charest, J.: Working-time configurations: A framework for analysing diversity across countries, *Industrial & Labor Relations Review,* 67(3) 2014, p. 830; Andreasson, U., Lundqvist, M.: *Nordic leadership*, Copenhagen: Nordic Council of Ministers Secretariat, 2018, p. 25.

[89] De Stefano, V., Taes, S.: Algorithmic management and collective bargaining. *Transfer: European Review of Labour and Research,* 29(1) 2023. pp. 21-36.

[90] Velasquez, M. G.: *Business Ethics: Concepts and Cases*, Englewood Cliffs NJ: Prentice-Hall, 1992, p. 399.

So, to be more precise, before introducing new surveillance technologies in the workplace, employer should make risk assessment of the impact of the surveillance, taking into account the following: proposed surveillance operation, purpose and legitimate interests, assessment of proportionality and necessity, risk to the rights and freedoms of data subject, possible use of the least intrusive means of obtaining the information and physical, technological and organisational safeguards. In short, in formulating and implementing of the policies on privacy at the workplace, the employers should be using the due diligence process.[91] It should be stressed that the privacy due diligence process is on-going process with an aim of continuous improvement.

7. CONCLUSION

Employment relationships are characterized by the inequality of bargaining power between an employer and an employee which gives rise for the employers to exercise their managerial prerogatives with exclusive rights to the control and supervision of the activities of the employees regarding the execution of the work, the possibility of applying disciplinary powers and organizing the work. Furthermore, in the employment relationship, there is inherent conflict between the employers' interest for reliability, responsibility, productivity, and effectiveness on the one hand and the employees' need for the protection of privacy on the other. The standard question of how to strike the right balance between protection of employers' interests and protection of the employees' right to privacy still remains. The novelty is that the extent to which management can now monitor employees' behaviours, both on and off site using advanced surveillance technologies, has dramatically increased creating situation of significant harm to employees' privacy issues. This raises concerns that widespread surveillance of the employees goes far beyond what is reasonable and necessary.

Due to the fact that employer-employee relationship is characterized by a number of specificities, especially regarding augmented managerial prerogatives and control power which give a rise to novel issues, existing legal arsenal regulating the issue of the protection of the right to privacy in general is not fully suitable. Due to the fact that there was a lack of policy provision regarding AI surveillance by employers and subsequent lack of awareness of monitoring practice and policy on the part of employees which create even more information asymmetry, the EU has adopted the Platform Work Directive and the AI Act. Taking into account the fact that these acts are fresh in force, the time

[91] Ebert, I., Wildhaber, I., Adams-Prassl, J.: Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection, *Big Data & Society*, 8(1) 2021, supra note 83.

will show how successful the solutions contained in the mentioned regulations are in striking the right balance between employees' right to privacy and protection of employers' business interests, in avoiding elevated conflict and inefficiencies and potential litigation. In the context of platform work and application of algorithmic management the authors of this paper are advocating the application of general principles for the employees' privacy protection that have been explained thoroughly.

Furthermore, although labour law has traditionally been structured and organized in a manner that demonstrates a lack of trust towards employees, recent period managerial studies have shown that trust-based management is much better approach for striking the right balance between employees' right to privacy and protection of employers' business interests. To ease the transition to a trust-based work environment it is of utmost importance to involve trade unions and other worker' representatives in the trust-based management process bolstering their right to collective bargaining whose primary function is to rectify the democratic deficit that is prevalent in employment relationship. Collective agreements, information and consultation rights, and co-determination also enable *ex-ante* controls on the introduction of new technologies and limit risks and abusive practices for the intrusion into workers' privacy. The main prerequisite is raising awareness of employees regarding the importance of unionisation in protection of their rights at work, in this context the right to privacy, in the era of advanced surveillance technologies and blurred boundaries between work and private life. It is too late to ask who's to blame when the cart rolls over. Employees should be aware more than ever before that the clock is ticking regarding their active role in creation of privacy policy protection in the workplace. It is time to finally leave aside what Erich Fromm calls pathological human passivity of industrial society as a syndrome of alienation.[92] Symptoms of that syndrome include feelings of powerlessness, loneliness and isolation which all together lead to uncritical and unquestioning submission to the control of authority.

Also, in formulating and implementing the policies on privacy at the workplace, the employers should be using the privacy due diligence process which could bring a win – win situation. In conclusion, if policies on privacy at the workplace are efficiently and effectively implemented , the employers could be shielded from legal, regulatory and financial risks to the business as a whole. On the other hand this would protect employees' right to privacy, autonomy, dignity and give a sense that a person's work is not commodity, but crucial to an individuals' dignity, well-being, and evolution as a Human Being.

[92] Fromm, E.: *The Revolution of Hope: Toward a Humanised Technology*, New York: Bantam Books, 1968, p. 41.

LITERATURE

1. Abraha, H. H.: A pragmatic compromise? The role of the Article 88 GDPR in upholding privacy in the workplace, *International Data Privacy Law*, 12(4) 2022, pp. 276-296.
   - DOI: https://doi.org/10.1093/idpl/ipac015
2. ALibeigi, A., Munir, A. B., Ershadul, K.: Right to Privacy, a Complicated Concept to Review, *SSRN Papers,* 2020.
   - DOI: https://doi.org/10.2139/ssrn.3537968
3. Andreasson, U., Lundqvist, M.: *Nordic leadership*, Copenhagen: Nordic Council of Ministers Secretariat, 2018.
   - DOI: https://doi.org/10.6027/ANP2018-535
4. Arroyo-Abad C.: Teleworking: A New Reality Conditioned by the Right to Privacy, *Laws,* 10(3) 2021, pp. 64.
   - DOI: https://doi.org/10.3390/laws10030064
5. Bailey Diane E.: Emerging technologies at work: Policy ideas to address negative consequences for work, employees, and society. *ILR Review* 75(3) 2022, pp. 527-551.
   - DOI: https://doi.org/10.1177/00197939221076747
6. Barak, A.: Proportionality and Principled Balancing, *Law & Ethics of human rights*, 4(1) 2010, pp. 1-16.
   - DOI: https://doi.org/10.2202/1938-2545.1041
7. Berg, P., Bosch, G., Charest, J.: Working-time configurations: A framework for analysing diversity across countries, *Industrial & Labor Relations Review,* 67(3) 2014, pp. 805-837.
   - DOI: https://doi.org/10.1177/0019793914537452
8. Bilić, A.: Utjecaj COVID-potvrda na pravo na rad i radnopravni status radnika u Republici Hrvatskoj, *Zbornik radova Pravnog fakulteta u Splitu*, 59(3) 2022, pp. 513-548.
   - DOI: https://doi.org/10.31141/zrpfs.2022.59.145.513
9. Blanpain, R.: Employee Privacy Issues: Belgian report, *Comparative Labour Law Journal*, 17 1995, pp. 38.
10. Borriello, F.: Principle of Proportionality and The Principle of Reasonableness, *Review of European Administrative Law*, 13(2) 2020, pp. 155-174.
    - DOI: https://doi.org/10.7590/187479820X15930701852292
11. Brower, H., Lester, S., Korsgaard, M., Dineen, B.: A Closer Look at Trust Between Managers and Subordinates: Understanding the Effects of Both Trusting and Being Trusted on Subordinate Outcomes, *Journal of Management*, 35(2) 2009, pp. 327-347.
    - DOI: https://doi.org/10.1177/0149206307312511

12. Brown, W. S.: Technology, workplace privacy and personhood, *Journal of Business Ethics*, 15(November) 1996, pp. 1237-1248.
    - DOI: https://doi.org/10.1007/BF00412822

13. Calacci, D., Stein, J.: From access to understanding: Collective data governance for workers. *European Labour Law Journal*, 14(2) 2023, pp. 253-282.
    - DOI: https://doi.org/10.1177/20319525231167981

14. Cappelli, P.: Stop overengineering people management, *Harvard Business Review*, (September-October) 2020.

15. Carre´, F., Tilly, C.: Digital technology implementation in US retail stores: Trends, potentials, and contingencies, *ILR Review*, 75(4) 2022. pp. 807-856.
    - DOI: https://doi.org/10.1177/00197939221095527

16. Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities*, C 364/1, 2000.

17. Charter of Fundamental Rights of the European Union, *Official Journal of the European Union*, C 326, 2012, pp. 391-407.

18. Cheung, M., Wong, C., Yuan G.: Why mutual trust leads to highest performance: the mediating role of psychological contract fulfilment, *Asia Pacific Journal of Human Resources,* 55(4) 2017, pp. 430-453.
    - DOI: https://doi.org/10.1111/1744-7941.12117

19. Connell, J., Ferres, N., Travaglione, T.: Engendering trust in manager-subordinate relationships: Predictors and outcomes, *Personnel review,* 32(5) 2003, pp. 569-587.
    - DOI: https://doi.org/10.1108/00483480310488342

20. Council of Europe, Committee of Ministers: *Recommendation CM/Rec(2015)5 to Member States on the processing of personal data in the context of employment*, 2015.

21. Council of Europe: *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, (108) 1981.

22. Council of Europe: *European Convention on Human Rights and Fundamental Freedoms*, 1950, <https://www.echr.coe.int/documents/d/echr/Convention_ENG>, last accessed on 3/2/2025.

23. Coyle, A.: E-mail and Internet Surveillance: Do Employees have a Right to Privacy? *Internet Law 'Bulletin*, 6(3) 2003, pp. 31-33.

24. Davidov, G.: *A Purposive Approach to Labour Law*, Oxford: Oxford University Press, 2016.
    - DOI: https://doi.org/10.1093/acprof:oso/9780198759034.001.0001

25. Davidov, G.: Collective Bargaining Laws: Purpose and Scope, *International Journal of Comparative Labour Law and Industrial Relations,* 20(1) 2004, pp. 81-106.
    - DOI: https://doi.org/10.54648/IJCL2004005

26. De Stefano, V., Durri, I., Stylogiannis, C., Wouters, M.: Does Labour Law Trust Workers? Questioning Underlying Assumptions Behind Managerial Prerogatives, *Industrial Law Journal*, 53(2) 2024, pp. 206-238.
    - DOI: https://doi.org/10.1093/indlaw/dwad022

27. De Stefano, V., Taes, S.: Algorithmic management and collective bargaining. *Transfer: European Review of Labour and Research,* 29(1) 2023. pp. 21-36.
    - DOI: https://doi.org/10.1177/10242589221141055

28. Ebert, I., Wildhaber, I., Adams-Prassl, J.: Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection, *Big Data & Society*, 8(1) 2021, pp. 20539517211013051.
    - DOI: https://doi.org/10.1177/20539517211013051

29. Elgoibar P., Euwema M., Munduate, L.: Building Trust and Constructive Conflict Management in the Organisations, in: Elgoibar, P., Munduate, L., Euwema, M. (eds.): *Industrial Relations and Conflict Management* (pp. 1-13), Cham: Springer International, 2016.
    - DOI: https://doi.org/10.1007/978-3-319-31475-4

30. Emiliou, N.: *The Principle of Proportionality in European Law, A Comparative Study,* Boston: Kluwer Law International, 1996.

31. European Court of Human Rights: *Bărbulescu v. Romania* (Application No. 61496/08), ECHR 742, 2017.

32. European Court of Human Rights: *Copland v. the United Kingdom* (Application No. 62617/00), ECHR 253, 2007.

33. European Court of Human Rights: *Halford v. the United Kingdom* (Application No. 20605/92), ECHR 32, 25.06.1997.

34. European Court of Human Rights: *Özpınar v. Turkey* (Application No. 20999/04), ECHR 2268, 2010.

35. European Court of Human Rights: *Sidabras and Džiautas v. Lithuania* (Applications Nos. 55480/00 and 59330/00), ECHR 395, 2004.

36. European Parliament and Council of the European Union: *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal of the European Communities, (L 281) 1995, pp. 31-50.

37. European Parliament and Council of the European Union: *Directive (EU) 2024/2831 on platform work*, Official Journal of the European Union, L 2831, 2024.

38. European Parliament and Council of the European Union: *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Official Journal of the European Union (L 119) 2016, pp. 1-88.

39. European Parliament and Council of the European Union: *Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such dana*, Official Journal of the European Union, L 295, 2018, pp. 39-98.

40. European Parliament and Council of the European Union: *Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*, Official Journal of the European Communities, L 8, 2001, pp. 1-22.

41. European Parliament and Council of the European Union: *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Official Journal of the European Union, L 119, 2016, pp. 1-88.

42. European Parliament and Council of the European Union: *Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, Official Journal of the European Union, L 1689, 12.07.2024.

43. Federal Republic of Germany: *Bundesgesetzblatt*, (1), 23.05.1949.

44. Felzmann, H., Fosch Villaronga, E., Lutz, C., Tamò-Larrieux, A.: Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns, *Big Data & Society*, 6(1) 2019, pp. 2053951719860542.
    - DOI: https://doi.org/10.1177/2053951719860542

45. Finkin, M. W.: Menchenbild: The Conception of the Employee as a Person in Western Law, *Comparative Labor Law & Policy Journal*, 23(2) 2002, pp. 577-594.

46. Freedland, M., Davies, P.: *Kahn-Freund's Labour and the Law*, London: Stevens & Sons, 1983.

47. Freedland, M., Kontouris, N.: *The Legal Construction of Personal Work Relation*, Oxord: Oxford University Press, 2011.
    - DOI: https://doi.org/10.1093/acprof:oso/9780199551750.001.0001

48. Fromm, E.: *The Revolution of Hope: Toward a Humanised Technology*, New York: Bantam Books, 1968.

49. Galea, C., Houkes, I., De Rijk, A.: An insider's point of view: how a system of flexible working hours helps employees to strike a proper balance between work and personal life, *The International Journal of Human Resource Management*, 25(8) 2014, pp. 1090-1111.
    - DOI: https://doi.org/10.1080/09585192.2013.816862

50. Godart, O., Görg, H., Hanley A.: Trust-based Work Time and Innovation: Evidence from Firm-level Data, *ILR Review,* 70(4) 2017, pp. 894-918.
    - DOI: https://doi.org/10.1177/0019793916676259

51. Gordon, J. L.: Under pressure: Addressing warehouse productivity quotas and the rise in injuries, *Fordham Urban Law Journal*, 49(1) 2021, pp. 149-189.

52. Groves, K. S., Margolis, J., Gibson, C.: Cultivating the experience of dignity at work during digital transformation: Protective & proactive strategies for leaders and organizations, *Organizational Dynamics*, 54(3) 2024, pp. 101103.
    - DOI: https://doi.org/10.1016/j.orgdyn.2024.101103

53. Gutelius, B., Theodore, N.: *The Future of Warehouse Work: Technological Change in the U.S. Logistics Industry*, Berkeley: UC Berkeley Labor Center; Working Partnerships USA, October 2019.

54. Hamel, G., Zanini, M.: The $3 Trillion Prize for Busting Bureaucracy (and how to claim it), (28/16) 2016.
    - DOI: https://doi.org/10.2139/ssrn.2748842

55. Hendrickx, F.: Employee Privacy, in: Blanpain, R. (ed.): *Comparative Labour Law and Industrial Relations in Industrialized Market Economies* (pp. 465-488), Alphen aan den Rijn: Kluwer Law International, 200l.

56. High-Level Expert Group on Artificial Intelligence: *Ethics guidelines for trustworthy AI*, European Commission, 2019.

57. ILO and OECD, *Building Trust in a Changing World of Work. The Global Deal for Decent Work and Inclusive Growth Flagship Report 2018*, Paris: Global Deal, ILO & OECD, 2018.

58. Ilsøe, A.: Between trust and control: company-level bargaining on flexible working hours in the Danish and German metal industries, *Industrial Relations Journal,* 41(1) 2010, pp. 34-51.
    - DOI: https://doi.org/10.1111/j.1468-2338.2009.00552.x

59. International Covenant on Civil and Political Rights: *United Nations Treaty Series 999* (entry into force 23 March 1976), United Nations, 1966, <https://treaties.un.org/doc/Treaties/1976/03/19760323%2006-17%20AM/Ch_IV_04.pdf>, last accessed on 3/2/2025.

60. International Labour Organization: *Code of practice on the protection of workers' personal dana*, Geneva: ILO, 1997.

61. Kastelle, T.: Hierarchy is overrated, *Harvard Business Review,* 20.11.2013.

62. Kellogg, K., C., Valentine, M. A., Christin, A.: Algorithms at work: The new contested terrain of control*, Academy of Management Annals,* 14(1) 2020, pp. 366-410.
    - DOI: https://doi.org/10.5465/annals.2018.0174

63. Kessler, S.: Companies are using employee survey data to predict - and squash - Union organizing, 14.01.2021, <https://onezero.medium.com/companies-are-us-

ing-employee-survey-data-to-predict-and-squash-union-organizing-a7e-28a8c2158>, last accessed on 10/3/2025.

64. Kuang-Hsien Wang, K. H., Lu, W. C.: AI-induced job impact: Complementary or substitution? Empirical insights and sustainable technology considerations, *Sustainable Technology and Entrepreneurship*, 4(1) 2025, pp. 100085.
    - DOI: https://doi.org/10.1016/j.stae.2024.100085

65. Kuner, C., Cate, F. H., Millard, C., Svantesson, D. J. B.: Privacy-an elusive concept. *International Data Privacy Law*, 1(3) 2011, pp. 141-142.
    - DOI: https://doi.org/10.1093/idpl/ipr014

66. Levy, K., Barocas, S.: Privacy at the Marginsl refractive surveillance: Monitoring customers to manage workers, *International Journal of Communication*, 12 2018, pp. 1166-1188.

67. Mantouvalou, V.: Advancing Human Rights, Capabilities and Non-Domination at work, in: Davidov, G., Langille, B., Lester, G. (eds.): *Oxford Handbook on the Law of Work* (pp. 115-128), Oxford: Oxford Academic, 2024.
    - DOI: https://doi.org/10.1093/oxfordhb/9780192870360.013.10

68. Moore, A.: Defining privacy, *Journal of Social Philosophy*, 39(3) 2008, pp. 411-428.
    - DOI: https://doi.org/10.1111/j.1467-9833.2008.00433.x

69. Moore, P. V., Upchurch, M., Whittacker, X.: Humans and machines at work: monitoring, surveillance and automation in contemporary capitalism, in: Moore, P. V., Upchurch, M., Whittacker, X (eds.): *Humans and machines at work: monitoring, surveillance and automation in contemporary capitalism, Dynamics of Virtual Work* (pp. 411-428), Cham: Palgrave Macmillan Cham, 2018.
    - DOI: https://doi.org/10.1007/978-3-319-58232-0

70. Müller, M.: *Die Öffnungsklauseln der Datenschutzgrundverordnung: Ein Beitrag zur Europaïschen Handlungsformenlehre*, Muenster: Wissenschaftliche Schriften der WWU Münste, 2018.

71. O'Brady, S., Doellgast, V.: Collective voice and employee well-being: Union influence on performance monitoring and emotional exhaustion in call centres, *Industrial Relations: A Journal of Economy and Society*, 60(3) 2021, pp. 307-337.
    - DOI: https://doi.org/10.1111/irel.12286

72. Ockenfels-Martinez, M., Sukhdip P. B.: *The public health crisis hidden in Amazon warehouses*, Human Impact Partners and Warehouse Employees Resource Centre, January 2021, <https://cdn.prod.website-files.com/67465c90aaa0a803cd5503ad/6748276f01a9f192749b924a_The-Public-Health-Crisis-Hidden-In-Amazon-Warehouses-HIP-WWRC-01-21.pdf>, last accessed on 10/4/2025.

73. Organisation for Economic Co-operation and Development: *OECD guidelines on the protection of privacy and transborder flows of personal data*, Paris: OECD Publishing, 2002.

74. Organisation for Economic Co-operation and Development: *The OECD privacy framework*, Paris: OECD Publishing, 2013.

75. Ramm, T.: Introduction, in: Schmidt, F. (ed.): *Discrimination in employment*, Stockholm: Almquist &Wiksell International, 1978.

76. Ravid, D. M., White, J. C., Tomczak, D. L. Miles, A. F., Behrend, T. S.: A meta-analysis of the effects of electronic performance monitoring on work outcomes, *Personnel Psychology*, 76(1) 2022, pp. 5-40.
    - DOI: https://doi.org/10.1111/peps.12514

77. Regan, P. M.: *Legislation Privacy: Technology, Social Values, and Public Policy*, New York: Oxford University Press, 1995.

78. Reischauer, G., Hess, T., Sellhorn, T., Theissen, E.: Transparency in an Age of Digitalization and Responsibility, *Schmalenbach Journal of Business Research*, 76 2024, pp. 483-494.
    - DOI: https://doi.org/10.1007/s41471-024-00203-4

79. Republic of Italy: *Gazzetta Ufficiale della Repubblica Italiana, Serie Generale, n. 174, Supplemento Ordinario*, (123), 29.07.2003.

80. Richards, N., Hartzog, W.: Taking trust seriously in privacy law, *Stanord Technology Law Review,* (19) 2016, pp. 431-472.
    - DOI: https://doi.org/10.2139/ssrn.2655719

81. Roemmich, K., Schaub, F., Andalibi, N.: Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy, in: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, (pp. 1-20), Hamburg; ACM.
    - DOI: https://doi.org/10.1145/3544548.3580950

82. Rosenblat, A., Levy, K., Barocas, S., Hwang, T.: Discriminating tastes: Customer ratings as vehicles for bias, *Data & Society: Intelligence and Autonomy,* 9(3) 2016, pp. 1-21.
    - DOI: https://doi.org/10.2139/ssrn.2858946

83. Schaupp, S.: Cybernetic proletarianization: Spirals of devaluation and conflict in digitalized production, *Capital & Class,* 46(1) 2021, pp. 11-31.
    - DOI: https://doi.org/10.1177/03098168211017614

84. Segal, E.: How productivity and surveillance Technology can create a Crisis for Businesses, *Forbes*, 18.08.2022.

85. Soueidan, M., H., Rodwan, S.: The impact of artificial intelligence on job loss: risks for governments, *Technium Social Sciences Journal*, 57 2024, pp. 206-223.
    - DOI: https://doi.org/10.47577/tssj.v57i1.10917

86. Stanley, J.: The Nightmarish loss of workplace Privacy, ACLU, 26.08.2022, <https://www.aclu.org/news/privacy-technology/the-nightmarish-loss-of-workplace-privacy>, last accessed on 10/4/2025.

87. Steiner, T., Netzer, L., Sulitzeanu-Kenan, R.: Necessity or balancing: The protection of rights under different proportionality tests-Experimental evidence, *International Journal of Constitutional Law*, 20(2) 2022, pp. 642-663.
- DOI: https://doi.org/10.1093/icon/moac036

88. Supreme Court of Canada: *R. v. Dyment*, 2 S.C.R. 417, 1988

89. Tabak, F., Smith, W. P.: Privacy and electronic monitoring in the workplace: a model of managerial cognition and relational trust development, *Employee Responsibilities and Rights Journal,* 17(3) 2005, pp. 173-189.
- DOI: https://doi.org/10.1007/s10672-005-6940-z

90. Tyagi, H., Kumar, R., Pandey, S.: A detailed study on trust management techniques for security and privacy in IoT: challenges, trends, and research directions, *High-Confidence Computing*, 3(2) 2023, pp. 100127.
- DOI: https://doi.org/10.1016/j.hcc.2023.100127

91. United Nations General Assembly: *Universal Declaration of Human Rights from 1948*, 1948, <http://www.un-documents.net/a3r217a.htm>, last accessed on 2/2/2025.

92. Vaught, B. C., Taylor, R. E., Vaught, S. F.: The attitudes of managers regarding the electronic monitoring of employee behaviour: Procedural and ethical considerations, *American Business Review*, 18(1) 2000.

93. Velasquez, M. G.: *Business Ethics: Concepts and Cases*, Englewood Cliffs NJ: Prentice-Hall, 1992.

94. Wachter S, Mittelstadt B., Floridi L.: Why a right to explanation of automated decision-making does not exist in the general data protection regulation, *International Data Privacy Law*, 7(2) 2017, pp. 76-99.
- DOI: https://doi.org/10.1093/idpl/ipx005

95. Wacks, R.: *Privacy and the Law*, Oxford: Clarendon Press, 1989.

96. Wattles, J.: *The Golden rule*, Oxford: Oxford University Press, 1996.
- DOI: https://doi.org/10.1093/oso/9780195101874.001.0001

97. Wedderburn, M.: Labour Law and the Individual, in: Rood, M., Lyon-Caen, G., Daubler van der Heijden, W. (eds.): *Labour Law in the post-industrial era. Essays in Honour of Hugo Sinzheimer*, Aldershot: Dartmouth, 1991.

98. Weiss, M.: Re-Inventing Labour Law?, in: Davidov, G., Langille, B. (eds.): *The Idea of Labour Law* (pp. 43-56), Oxford: Oxford Academic.
- DOI: https://doi.org/10.1093/acprof:oso/9780199693610.003.0004

99. WP29: *Opinion 2/2017 on data processing at work*, European Commission, 2017.

100. WP291: *Opinion 08/2001 on the processing of personal data in the employment context (WP 48)*, European Commission, 2001.

101. Xu, L., Jiang, C., He, N., Han, Z., Benslimane, A.: Trust-Based Collaborative Privacy Management in Online Social Networks, *IEEE Transactions on Information Forensics and Security*, 14(1) 2019, pp. 48-60.
- DOI: https://doi.org/10.1109/TIFS.2018.2840488

102. Zuboff, S.: *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: Public Affairs, an imprint of Perseus Books, 2019.