MITIGATING DIGITAL PANOPTICISM IN THE WORKPLACE BY INTEGRATING HUMAN RIGHTS DUE DILIGENCE AND PRIVACY BY DESIGN FRAMEWORK

*Prof. dr. sc. Andrijana Bilić**

UDK 342.738:349.2
341.231.14
https://doi.org/10.30925/zpfsr.46.3.1
Ur.: 11. srpnja 2025.
Pr.: 4. studenoga 2025.
Izvorni znanstveni rad

Summary

The rise of digital surveillance technologies in the workplace has transformed labour practice, but has also raised concerns about employee privacy, autonomy and ethical issues, often resulting in what is termed "digital panopticism." Therefore, in this article the possibilities of the existing legal framework and privacy design-based approach to tackle the challenges of privacy protection in the workplace were explored. After identifying several shortcomings of legislative approaches, business practices and the demands of workers and their representatives - factors which impede a proper balance between managerial prerogatives and employee privacy protection - the potential of Human Rights Due Diligence (HRDD) to address these issues was examined. After identifying several shortcomings of HRDD framework it is furthermore argued that a holistic approach, integrating both HRDD and Privacy by Design (PbD) frameworks, can create a comprehensive privacy protection system. Such an approach mitigates the adverse effects of surveillance while prioritizing employee rights, thereby fostering a healthier work environment that enhances mutual trust, respect for human rights, and organizational productivity.

***Keywords**: panopticon surveillance; employee privacy protection; privacy by design; human rights due diligence; Croatian privacy protection legal framework.*

* Andrijana Bilić, Ph.D., Full Professor, University of Split, Faculty of Law; andrijana.bilic@pravst.hr. ORCID: https://orcid.org/0000-0002-1272-4749.

1 INTRODUCTORY REMARKS

The digital revolution and artificial intelligence have brought an array of new tools that employers now use in their business models and methods to monitor their employees. Digital surveillance practices have proliferated across sectors under the rationales of security, compliance, and risk management.

The extent to which management can now monitor employees' behaviours, both on-site and remotely, using advanced surveillance technologies has dramatically increased, creating a scenario of panoptic power management, or "digital panopticism." This phenomenon mirrors Michel Foucault's concept of the "Panopticon" - a structure of control wherein subjects self-regulate under the possibility of constant observation.[1] In the corporate realm, digital panopticism raises ethical and legal issues around autonomy, privacy, and power asymmetry. Namely, the collection of personal data through various digital means (e.g., emails, productivity software) raises concerns about how this data is used, stored and shared, potentially causing significant harm to employees' privacy issues which exacerbates mistrust. In that process of collection, employees may not be fully aware of what data is being collected or how it is being used, leading to a mistrust of employers. Also, the data collected can be misused for purposes such as discrimination, bias in performance evaluations, or unjustified disciplinary actions. Furthermore, organizations may face legal challenges if they fail to comply with privacy regulations leading to financial and reputational damages.

This article explores the mechanisms driving digital panopticism in business environments and point out some controversial issues related to privacy protection in the contemporary workplace. The aim of this article is to explore the possibilities and shortcomings of existing privacy protection legal framework, as well as privacy design-based framework and human rights due diligence framework in order to offer strategies to mitigate the effects of digital panopticism which dangerously threaten the right to employee privacy in the contemporary workplace, particularly in multinational corporations. Bridging this gap requires integration of human rights due diligence (HRDD) and privacy by design (PbD) which can offer both normative and technical guidance for ethical workplace surveillance.

---

1 Panopticon was elaborated by Jeremy Bentham at the end of the eighteen century and later on Michel Foucault used it as a symbol of disciplinary power. The simple idea of Bentham can be described as follows: "a circular building with the cells of the prisoners located in the circumference and, separated by an empty space, the tower of the inspector located in the centre. The side of each cell facing outwards would be occupied by a large window and the inner one by a thin iron grating in order to make the whole room perfectly visible from the tower, while also contributing to let sunlight inside the Panopticon." The Panopticon is an image for this discipline: in Foucault's opinion its objective is "to improve the exercise of power, making it faster, lighter and more effective. The individual in the Panopticon, being subjected to a regime of constant visibility, is caught in a power relationship within which he becomes the principle of his own subjection." Carl Botan, "Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects," *Communication Monographs* 63, no. 4 (1996): 293-313; Michael Foucault, "'Panopticism' from 'Discipline & Punish: The Birth of the Prison'," *Race/Ethnicity: Multidisciplinary Global Contexts* 2, no. 1 (1996): 1-12.

In the following sections, this paper explores the limitations of legislative and corporate approaches, outlines the principles of HRDD and PbD, and proposes an integrated model for mitigating digital panopticism in the workplace. In this context special focus has been put on Croatian privacy protection legal framework.

2 THE RIGHT TO PRIVACY IN EMPLOYMENT CONTEXT

In the employment relationship, there is inherent conflict between free enjoyment of the employees' right to privacy and the employer's interest in protecting business operations. The employer's higher hierarchical position, due to the unequal bargaining power in employment contracts, enables them to exercise managerial prerogatives. As the master of the workplace, the employer retains the exclusive right to control and supervise employee activities, apply disciplinary measures, and organize work processes. Such control can be justified by the need[2] for reliability, productivity, and operational efficiency.[3]

However, contemporary human resource management techniques increasingly encroach on employees' private spheres, extending employer oversight beyond the workplace. These practices challenge the limits of acceptable workplace surveillance and call into question the balance between managerial authority and employee rights.

Conversely, employees have legitimate interests in protecting their privacy, grounded in autonomy, dignity, well-being, and freedom of expression. The justification for the protection of the privacy of the employee can be observed from several aspects such as the protection of employee's limited autonomy, dignity and well-being, freedom of expression,[4] possibility of self-evaluation and the creation and maintaining of a relationship of mutual trust between the employee and the employer.[5] To what extent these rights and interests can be limited depend primarily on the bargaining power of the parties of the employment relationship. Therefore, it is not hard to conclude why has digital panopticism prevailed in the contemporary workplace.

---

2 Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995), 188.

3 Bobby C. Vaught, Raymond E. Taylor and Steven F. Vaught, "The Attitudes of Managers Regarding the Electronic Monitoring of Employee Behaviour: Procedural and Ethical Considerations," *American Business Review* 1, no. 1 (2000): 107-114. Frank Hendrickx, "Employee Privacy," in *Comparative Labour Law and Industrial Relations in Industrialized Market Economies*, ed. Roger Blanpain (Alphen aan den Rijn: Kluwer Law International, 2001), 400.

4 Manfred Weiss, "Re- inventing Labour Law," in *The Idea of Labour Law*, eds. Guy Davidov and Brian Langille (Oxford: Oxford University Press, 2011), 44; Matthew W. Finkin, "Menchenbild: The Conception of the Employee as a Person," *Western Law* 23, no. 2 (2002): 577; Mark Freedland and Nicola Kontouris, *The Legal Construction of Personal Work Relation* (Oxford: Oxford University Press, 2011), 73. Also, importance of the dignity can be seen in the Charter of Fundamental Rights of the European Union in art. 31 "every employee has the right to working conditions which respect his or her health, safety and dignity."

5 Raymond Wacks, *Privacy and the Law* (Oxford: Clarendon Press, 1989), 11-12.

3 PANOPTICON METAPHOR IN CONTEMPORARY EMPLOYMENT RELATIONSHIP

The extent to which management can these days monitor employees' behaviours- both on site and remotely using advanced surveillance technologies has increased dramatically. Over the past several decades, we have witnessed a growing use of digital technologies by the employers in the workplace to capture and analyse employee data, monitor them electronically, and manage them using algorithms.[6] Employers are deploying so-called "bossware" to track employee productivity, predict workplace behaviours and future health conditions, assess intentions to join a trade union, and even infer private plans such as starting a family. In that context, workplaces are increasingly adopting Emotion AI,[7] corporate wellness programs and even genetic testing of employees. Also, there is potential for the introduction of neurosurveillance, namely, through alleged capabilities of Emotion AI to automatically infer, analyse, and/or respond to workers' affective phenomena at scale. By influencing employees' emotions and related constructs, these technologies aim to optimize organizational outcomes.[8]

Many companies have introduced practices or programs which focus on encouraging healthy lifestyles and preventing harmful behaviours. They tend to offer a wide variety of practices by which to deal with employees' emotional, intellectual, physical and social issues.[9] Furthermore, workplace genetic testing (wGT) programs screen for high-risk, actionable genetic diseases, such as cancer. These programmes aim to control workforce healthcare costs, increase employee retention, and boost productivity. However, they also pose risks,[10] such as intrusion into privacy of employees.

With the help of neurosurveillance technologies, employers can analyse employees' brain data to assess cognitive functions (e.g., mental capacity

6 Katherine C. Kellogg, Melissa A. Valentine and Angèle Christin, "Algorithms at Work: The New Contested Terrain of Control," *Academy of Management Annals* 14, no. 1 (2020): 366-410; Diane E. Bailey, "Emerging Technologies at Work: Policy Ideas to Address Negative Consequences for Work, Employees, and Society," *ILR Review* 75, no. 3 (2022): 527-551.

7 Joni Roy Piispanen and Rebekah Rousi, "Emotion AI in Workplace Environments: A Case Study," 2024, accessed February 12, 2025, https://arxiv.org/pdf/2412.09251.

8 Carolyn Holton, "Identifying Disgruntled Employee Systems Fraud Risk through Text Mining: A Simple Solution for a Multi-Billion-Dollar Problem," *Decision Support Systems* 46, no. 4 (2009): 853-864.

9 Isidro Peña et al., "Wellness Programs, Perceived Organizational Support, and Their Influence on Organizational Performance: An Analysis Within the Framework of Sustainable Human Resource Management," *Sage Open* 14, no. 1 (2024); Matke Soeren et al., "Workplace Wellness Programs Study: Final Report," *Rand Health Q* (2013); Maria Marin-Farrona et al., "Effectiveness of Worksite Wellness Programs Based on Physical Activity to Improve Workers' Health and Productivity: A Systematic Review," *Systematic Reviews* 12, article no. 87 (2023).

10 Lizabeth A. Barclay and Karen S. Markel, "Discrimination and Stigmatization in Work Organizations: A Multiple Level Framework for Research on Genetic Testing," *Human Relations* 60, no. 6 (2023): 953-980.

and efficiency), cognitive patterns (e.g., stress responses) and even detect neuropathologies.[11] Data obtained may be used for decisions related to promotion, hiring, or dismissal, as well for improving well-being, productivity,[12] workplace safety and personalized work environment.[13] Namely, by gathering data on cognitive load, stress levels and overall mental health employers enable a more supportive work environment. Neurotechnological tools which are utilised in workplace surveillance include EEG devices,[14] wearable devices[15] and neurofeedback systems.[16] Despite their potential benefits, neurosurveillance raises serious concerns about privacy threats,[17] data misinterpretation, questionable consent[18] and a risk of neurodiscrimination.

Given the extensive monitoring capabilities now available to management, the metaphor of "panoptic power" is useful for describing the modern employment relationship. Namely, this metaphor has often been the starting point for examination of the effects of the surveillance in the workplace, as well for describing the type of employer-employee dynamics it creates. With so much information on employees that employers collected due to the use of electronic systems information panopticon is formed; liberating employers from the constraints of time and space. [19] However, the panoptic power management has extended beyond workplace; it increasingly encroaches upon employees' private lives, posing significant risks to their privacy.[20]

11 Ekatarina Muhl and Roberto Andorno, "Neurosurveillance in the Workplace: Do Employers Have the Right to Monitor Employees' Minds?," *Frontiers in Human Dynamics* 5 (2023); Ekatarina Muhl, "The Challenge of Wearable Neurodevices for Workplace Monitoring: An EU Legal Perspective," *Frontiers in Human Dynamics* 6 (2024).

12 Francesca Bonetti and Giorgio Casoni, "Brain Training, Mindfulness, and Wearables: Empowering Employee Wellbeing Through Neurotechnologies," *Diid Disegno Industriale Industrial Design* (2023).

13 Janaina Lemos et al., "Enhancing Workplace Safety through Personalized Environmental Risk Assessment: An AI-Driven Approach in Industry 5.0," *Computers* 13, no. 5 (2024): 120.

14 Stephen Mujeye and Yair Levy, "Complex Passwords: How Far is Too Far? The Role of Cognitive Load on Employee Productivity," *Online Journal of Applied Knowledge Management* 1, no. 1 (2013): 122-132.

15 Josh Henniger, "Wearable Technology and Employer Wellness Programs: Gaps and Solutions," *Ohio State Business Law Journal* 12, no. 2 (2017): 197.

16 Beomjun Min et al., "The Effectiveness of a Neurofeedback-Assisted Mindfulness Training Program Using a Mobile App on Stress Reduction in Employees: Randomized Controlled Trial," *Journal of Medical Internet Research mHealth and uHealth* 3, no. 11 (2023).

17 Wendy Martinez et al., "Understanding the Ethical Concerns for Neurotechnology in the Future of Work," in *CHIWORK '22: Proceedings of the 1st Annual Meeting of the Symposium on Human-Computer Interaction for Work*, eds. Andrew L. Kun et al. (New York: Association for Computing Machinery, 2022), 1-19.

18 Muhl and Andorno, "Neurosurveillance in the Workplace," 5.

19 More in details: Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

20 These can include: physical harms, economic harms, reputational and other social-psychological harms, direct psychological harms, individual 'autonomy harms' such as coercion and manipulation, collective harms such as 'chilling effects,' and the erosion of work/non-work boundaries and work-life balance. See: Daniel J. Solove and Danielle Keats, "Privacy Harms," *Boston University Law Review* 102 (2022): 793-863.

Monitored employees often experience a lack of privacy and, in some cases, feel their dignity is under threat. Surveillance allows employers to access personal information, which - if misused - can serve as a basis for illegal practices such as invasion of privacy, discrimination, or unjustified dismissal. Awareness of constant supervision can lead to fear, stress,[21] stress-related illnesses, and paranoia among employees. Surveillance may undermine mutual trust, foster suspicion and tension, and trigger resistance within the workplace. These effects often result in decreased employee satisfaction, increased labour disputes, reduced productivity, diminished work quality,[22] and blurred boundaries between work and personal life - ironically, counteracting the intended purposes of workplace monitoring and control.

It is not difficult to conclude that the revolution in big data and artificial intelligence has introduced an array of tools that employers now use to control their workforce - tools with the potential to profoundly influence employee outcomes.[23] Doesn't this evoke the dystopian vision in George Orwell's *1984*, where the emotional and psychological states of individuals are laid bare in public spaces? What can be done to prevent this fiction from becoming reality?

Currently, the ways in which employers deploy these technologies are often opaque - not only to employees but also to policymakers. Many practices operate under regulatory frameworks that reinforce managerial prerogatives or reflect a lack of trust in employees. Although international and European legal frameworks recognize privacy as a fundamental right, their current structure remains insufficient to address the realities of data-driven and algorithmically managed work. Namely, international standards lack binding enforcement, while European regulations do not fully mitigate power asymmetries in employment or regulate emerging surveillance technologies. This regulatory gap creates strong incentives for employers to use digital technologies at will, often in ways that directly or indirectly harm employees. While some of these harms stem from the design of the technologies themselves, more often they result from poor managerial decisions regarding when, why, where, and how to use such tools. At this point, it is critical to explore the strengths and limitations (gaps) of the existing legal framework for protecting employee privacy in the workplace.

21 Mika Kivimäki et al., "Long Working Hours and Risk of Coronary Heart Disease and Stroke: A Systematic Review and Meta-Analysis of Published and Unpublished Data for 603,838 Individuals," *The Lancet* 386, no. 10005 (2015): 1739-1746.

22 Jitendra M. Mishra and Suzanne M. Crampton, "Employee Monitoring: Privacy in the Workplace?," *S.A.M. Advanced Management Journal* 63, no. 3 (1998): 4-14; Delbert M. Nebeker and Charles B. Tatum, "The Effects of Computer Monitoring, Standards and Rewards on Work Performance, Job Satisfaction and Stress," *Journal of Applied Social Psychology*, no. 23 (1993): 508.

23 Zuboff, *The Age of Surveillance Capitalism.*

4 EXISTING FRAMEWORKS FOR THE PROTECTION OF EMPLOYEE PRIVACY AT THE WORKPLACE

Given that employee privacy is at risk throughout the entire data lifecycle,[24] it is essential to highlight the potential of both legal and technological solutions for privacy protection. Employee privacy can be compromised during data collection, analysis, use, and erasure. Risks may arise from a lack of transparency and awareness about data collection, knowledge asymmetries, group or individual discrimination, limited employee autonomy over data usage, and insufficient transparency and accountability regarding data erasure. [25]

Employer accountability for privacy infringements in the workplace is typically governed by national labour and data protection laws. However, in modern workplaces, data-driven employee monitoring often transcends national borders - particularly in the case of multinational companies operating across multiple jurisdictions. Therefore, it is important to focus on both European and international regulatory frameworks for the protection of employee privacy.

4.1 Legal Framework for Employee's Privacy Protection

Several distinct yet overlapping and closely intertwined legal regimes in Europe aim to protect various aspects of employee privacy. These include the European Convention on Human Rights (1953),[26] the EU Charter of Fundamental Rights (2012),[27] the EU General Data Protection Regulation (hereinafter: GDPR) (2016),[28] EU Directive (EU) 2019/1152,[29] Recommendation CM/Rec (2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment,[30] as well as Opinion 8/2001 on the processing of personal data in the employment context (WP48),[31] the Working Document on the

24 Recitals 71a-71b, Art. 23 para. 1, Art. 33 para. 3. European Parliament Position on the General Data Protection Regulation, 2014, accessed June 10, 2025, https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_EN.html.

25 Isabel Ebert, Isabelle Wildhaber and Jeremias Adams-Prassl, "Big Data in the Workplace: Privacy Due Diligence as a Human Rights-Based Approach to Employee Privacy Protection," *Big Data & Society* 8, no. 1 (2021): 3.

26 Council of Europe, European Convention on Human Rights, ETS No. 5 of November 4, 1950, entered into force September 3, 1953.

27 Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391-407.

28 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), OJ L 119, 4.5.2016, pp. 1-88.

29 Directive (EU) 2019/1152 of the European Parliament and of the Council of 20 June 2019 on transparent and predictable working conditions in the European Union, OJ L 186, 11.7.2019., pp. 105-121.

30 Recommendation of the Committee of Ministers to Member States on the processing of personal data in the context of employment, CM/Rec (2015)5 of April 1, 2015.

31 Working Party 29, Opinion 08/2001 on the Processing of Personal Data in the Employment Context, WP 48 of 13 September 2001.

surveillance of electronic communications in the workplace (WP55),[32] and Opinion 2/2017 on data processing at work[33] (adopted on 8 June 2017). National employment law regimes also play a significant role.

The European Court of Human Rights (hereinafter: ECtHR), in the case *Barbulescu v Romania,*[34] outlined relevant factors that national courts should consider when assessing the compatibility of employee monitoring with Article 8 of the Convention on Human Rights. These principles have been confirmed in many other cases.

The right to privacy in the workplace has also been recognized concretely by the International Labour Organization (ILO). In its *Code of Practice on the Protection of Workers' Personal Data* (1997),[35] the ILO called for the extension of responsibility to private companies, obliging them to ensure compliance with international human rights norms. This emphasis on human rights responsibilities is becoming more visible at the international level. However, it is important to note that no legal regime to date has established comprehensive protective standards internationally.

The limitation of fundamental rights and freedoms, such as the right to privacy, should be the exception and must be carried out in a reasonable manner. While this topic will be further explored in authors' another article, it is important to highlight the general principles of privacy protection in the workplace that are derived from the aforementioned legal sources and ECtHR case law. These principles should be respected to ensure that any intrusion into an employee's privacy is justified. These principles include reasonable expectation of privacy, the principle of necessity and proportionality, the principle of legitimacy, the principle of transparency, the principle of finality and the principle of information and consultation.

Although there is an established international and European legal framework, for privacy protection which recognize privacy as a fundamental right, their current structure remains insufficient to address the realities of data-driven and algorithmically managed work (industry 4.0 and 5.0). Namely, international standards lack binding enforcement, while European regulations do not fully mitigate power asymmetries in employment or regulate emerging surveillance technologies, its operationalization lacks sector-specific guidance and robust enforcement mechanisms, especially related to behavioural analytics, biometric systems, and AI-enabled productivity surveillance. Furthermore, challenges persist in ensuring transparency of decision-making systems, protection from indirect discrimination, and access to effective remedies for workers subjected to opaque performance scoring or automated

32 Data Protection Working Party, Working Document on the Surveillance of Electronic Communications in the Workplace, 5401/01/EN/Final, WP 55 of May 29, 2002.

33 Data Protection Working Party, Opinion 2/2017 on Data Processing at Work, WP 249 of June 8, 2017.

34 ECtHR, Bărbulescu v. Romania, App. no. 61496/08, Judgment of September 5, 2017.

35 International Labour Organization, "Code of Practice on the Protection of Workers' Personal Data, 1997," accessed June 16, 2025, https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40ed_protect/%40protrav/%40safework/documents/normativeinstrument/wcms_107797.pdf.

disciplinary actions.[36] This is evident in ongoing national and European privacy litigations. While legal frameworks are in place to protect employee privacy, their effectiveness can be limited by variability in legislation, enforcement, compliance, and the rapid pace of technological change. Continuous evaluation and adaptation of laws are necessary to enhance employee privacy protection.

Given that legislative changes are often slow, it is crucial to find ways to bridge the legal gaps that arise due to technological advancements. In this context, several technology-based solutions have been proposed to complement existing legal frameworks, particularly in the deployment of people analytics software. One such approach is *Privacy by Design* (PbD), which aims to enhance privacy protection across borders by embedding design specifications into information technologies, promoting accountable business practices, and ensuring that networked infrastructures support privacy rights.[37]

4.2 Privacy by Design at the Workplace: A Proactive Approach to Employee Data Protection

Privacy by Design (PbD) is a framework developed by Ann Cavoukian that emphasizes the proactive incorporation of privacy measures into the design and operation of systems, processes, and technologies. Implementing Privacy by Design principles in the workplace is essential for safeguarding employee privacy in an increasingly digital environment. By adopting proactive measures that prioritize privacy, organizations can build trust with their employees, comply with legal requirements, and mitigate risks associated with data breaches.

Privacy by Design is a holistic approach to privacy that encompasses seven foundational principles: [38]

- Proactive, not reactive; Preventative, not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – Positive-sum, not Zero-sum
- End-to-end security – Lifecycle protection
- Visibility and transparency – Keep it open
- Respect for user privacy – Keep it user-centric.

Indeed, design-based approaches are not only popular in the tech industry[39] but have increasingly found their way into legal frameworks[40] and ECtHR case

36 Judgement of October 6, 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, EU:C:2015:650 and Judgement of July 16, 2020, Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schrems, C-311/18, EU:C:2020:559.

37 Ebert, Wildhaber and Prassl „Big Data in the Workplace", 5.

38 Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles," Information and Privacy Commissioner of Ontario, 2010, accessed June, 17, 2025, https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.

39 E.g. Microsoft, Apple, Google, IBM, Salesforce, Cisco, Adobe, SAP, Facebook.

40 Protection by design is an 'appropriate measure' to comply with data protection law (Art. 25 para. 1 GDPR).

law.[41] However, several potential shortcomings in design-based approaches have been identified, particularly regarding the adequate protection of privacy in the contemporary workplace.

First, the design-based approach struggles to adequately incorporate the principle of proportionality. This is because algorithms are limited in their ability to perceive and process the environment in the same way humans do when assessing the legality of privacy intrusions. Furthermore, these approaches cannot *ex ante* balance the competing interests at the moment of decision-making. With the potential use of newer, more sophisticated technologies, a different weight may be given to the competing interests involved, depending on the extent of intrusions into workers' private lives.

Another shortcoming is the ambiguous legal terminology that must be translated into code. The concept of Privacy by Design consists of two legal terms - privacy and design - that lack consensus on their meanings. This ambiguity makes it difficult for computer programmers to translate legal concepts into code if the corresponding legal rules rely on vague or unclear terminology.[42]

Technological evolution also presents a challenge. Rapid advancements in technology can outpace design-based approaches, making it difficult for organizations to keep their systems updated with the latest privacy protections.[43] As a result, gaps in protection are ubiquitous.

Additionally, Privacy by Design, with its tech-based solutions, is not a panacea due to its implementation complexity and inconsistent application.[44] Organizations may struggle to balance privacy features with functionality, leading to complications during implementation. Without clear guidelines and standards, design-based approaches may be applied inconsistently across different departments or systems within an organization, resulting in varying levels of privacy protection.

Furthermore, developing privacy-centric systems can require significant upfront investments in technology, training, and ongoing maintenance. Smaller organizations, in particular, may find it challenging to allocate the necessary resources due to cost implications. Employees and management may also resist changes to established workflows or systems that prioritize privacy, especially if they perceive these changes as hindrances to productivity.

Another obstacle is the superficial implementation of privacy measures. Design-based approaches may sometimes prioritize compliance with legal requirements rather than fostering a culture of privacy within the organization. Privacy-focused designs can also inadvertently compromise user experience, organizational policies, training, and employee engagement. Human factors - such as employee awareness and behaviour - are essential for effective privacy protection and the development

41 ECtHR, I v. Finland, App. no. 20511/03, Judgment of July 17, 2008, § 1 et seq.

42 Inga Kroener and David Wright, "A Strategy for Operationalizing PbD," *The Information Society* 30, no. 5 (2014): 355-365.

43 Yves Alexande et al., "Unique in the Crowd: The Privacy Bounds of Human Mobility," *Scientific Reports* 3, article no. 1376 (2013).

44 Alexander Dix, "Built-in Privacy– No Panacea, but a Necessary Condition for Effective Privacy Protection," *Identity in the Information Society* 3 (2010): 257-265.

of intuitive, user-friendly systems. Additionally, once a system is designed, there is a risk that it may not be regularly updated to adapt to new threats or changes in the regulatory landscape, leading to outdated privacy protections.

In summary, while design-based approaches can enhance employee privacy protection, they also face several challenges. In order to be effective, these approaches must be integrated within broader organizational practices, ongoing training, and a commitment to fostering a culture of privacy. Furthermore, data-driven models that weight human behaviour are not immune to errors or false conclusions about human interaction.[45] So, a broader privacy approach is of utmost importance - one that also incorporates ethical expectations by management in decisions about workplace monitoring measures. Representatives from all affected stakeholder groups should be strategically involved. All of this brings us to the potential need for the implementation of corporate sustainability due diligence and corporate liability in the legal framework on employee privacy protection.

5 THE NEED FOR THE LEGAL IMPLEMENTATION OF CORPORATE SUSTAINABILITY DUE DILIGENCE AND CORPORATE LIABILITY IN THE EMPLOYEES' PRIVACY PROTECTION

Due diligence has traditionally been used in national legal frameworks as a standard of care in tort law and comparable concepts in civil law. However, it was not until the last decade that it began to be applied in relation to human rights impacts and business activities. Human rights due diligence (hereinafter: HRDD) has since emerged as a key mechanism for addressing human rights abuses by businesses. Fundamental labour standards (FLSs) are an essential component of these human rights.

In this context, the notion of prevention is critical, relating to efforts to prevent businesses from causing, contributing to, or being linked to adverse human rights impacts globally.[46] HRDD is defined as a comprehensive, proactive effort to identify both actual and potential human rights risks over the entire life cycle of a project or business activity, with the aim of avoiding and mitigating those risks.[47] HRDD is

45 Peter Nagy and Gina Neff, "Imagined Affordance: Reconstructing a Keyword for Communication Theory," *Social Media + Society* 1, no. 2 (2015).

46 UN Human Rights Council, "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework," accessed May 15, 2025, https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. Guiding Principle 13.

47 UN Human Rights Council, Business and Human Rights: Towards Operationalizing the "Protect, Respect and Remedy" Framework, A/HRC/11/13 of April 22, 2009, para. 71. See also the UN Working Group on Business and Human Rights, The Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises', A/73/163 of July 16, 2018, para. 10, and OECD, "OECD-Due-Diligence Guidance for Responsible Business Conduct," 2018, accessed June 10, 2025, https://www.oecd.org/en/publications/2018/02/oecd-due-diligence-guidance-for-responsible-business-

proactive and continuous, based on the principle that businesses must anticipate risks rather than merely respond to violations once they occur. [48]

Companies need a thorough due diligence process to identify the risks of breaching employees' human rights, to assess whether an ongoing breach exists, and to evaluate how the company's systems would respond in the event of a breach. However, the knowledge gained during the due diligence process must be implemented at all appropriate stages. Integrating HRDD into boardroom decision-making fosters long-term value creation, risk mitigation, and stakeholder trust. [49]

5.1 Legal Framework for Corporate Sustainability Human Rights Due Diligence

While initially introduced as a voluntary standard, HRDD is increasingly being incorporated into binding national legislation[50] and supranational regulations. These developments mark a shift toward mandatory HRDD, transforming corporate accountability from a model of soft governance into one of enforceable legal obligations. [51] At this point, we shall provide an analysis of the non-binding United Nations Guiding Principles on Business and Human Rights, alongside the binding Directive (EU) 2024/1760 (Corporate Sustainability Due Diligence Directive – CSDDD) of the European Parliament and of the Council of June 13, 2024 on corporate sustainability due diligence.[52]

5.1.1 United Nations Guiding Principles on Business and Human Rights

The globalization of business has led to significant human rights implications and has underscored the need for international frameworks to regulate corporate behaviour. The United Nations Guiding Principles on Business and Human Rights (2011) (hereinafter: UNGPs)[53] represent the key international - and the first - document on business and human rights to incorporate the concept of Human Rights Due Diligence (HRDD) within its framework.

These Guiding Principles of the UNGPs rest on three foundational pillars:

conduct_c669bd57.html, para. 16.

48 Surya Deva, *Regulating Corporate Human Rights Violations: Humanizing Business* (London: Routledge, 2012).

49 Justine Nolan, "The Corporate Responsibility to Respect Human Rights: Soft Law or Not Law?", in *Law and Society*, eds. Surya Deva and David Bilchitz (Edward Elgar Publishing, 2021), 138-161.

50 French Duty of Vigilance Law (2017) mandates large companies to implement vigilance plans to prevent human rights and environmental violations and German Supply Chain Due Diligence Act (2021) requires companies to conduct due diligence on human rights and environmental risks across their supply chains.

51 Claire Bright et al., "Towards a Corporate Duty for Lead Companies to Respect Human Rights in Their Global Value Chains?," *Business and Politics* 22, no. 4 (2020): 667-697.

52 Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859, OJ L 2024/1760, 5.7.2024.

53 "Guiding Principles on Business and Human Rights."

a) The state's existing obligations to respect, protect, and fulfill human rights and fundamental freedoms;
b) The role of business enterprises as specialized organs of society performing distinct functions, required to comply with all applicable laws and to respect human rights;
c) The need for rights and obligations to be matched with appropriate and effective remedies when breaches occur.

These Guiding Principles apply to all states and all business enterprises - whether transnational or otherwise - regardless of their size, sector, location, ownership, or structure. They are intended to be understood as a coherent whole and should be read, individually and collectively, in light of their overarching objective: to enhance standards and practices related to business and human rights, thereby achieving tangible benefits for affected individuals and communities, and contributing to a socially sustainable globalization.

Although the UNGPs are not legally binding and suffer from weak accountability and enforcement mechanisms,[54] inconsistent implementation,[55] and a limited focus on power asymmetries, they are nonetheless regarded as the "global authoritative standard on business and human rights."[56] Their strength lies in their normative clarity and structure,[57] global legitimacy and endorsement,[58] its function of catalysing legal and policy reform[59] and soft law flexibility.[60]

Owing to these strengths, the UNGPs have influenced the incorporation of HRDD into other international standards, national legislation,[61] and domestic court

54 Florian Wettstein, "Normativity, Ethics, and the UN Guiding Principles on Business and Human Rights: A Critical Assessment," *Journal of Human Rights* 14, no. 2 (2015): 162-182.

55 Jette Steen Knudsen and Jeremy Moon, "Visible Hands: Government Regulation and International Business Responsibility," *Cambridge Journal of Economics* 41, no. 2 (2017): 383-409.

56 International Bar Association, "IBA Practical Guide on Business and Human Rights for Business Lawyers," 13, accessed May 28, 2025, https://www.ibanet.org/MediaHandler?id=d6306c84-e2f8-4c82-a86f-93940d6736c4.

57 John Gerard Ruggie, *Just Business: Multinational Corporations and Human Right* (W. W. Norton & Company, 2013).

58 Surya Deva and David Bilchitz, eds., *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect?* (Cambridge: Cambridge University Press, 2013.).

59 Christian Scheper, "From Naming and Shaming to Knowing and Showing: Human Rights and the Power of Corporate Practice," *The International Journal of Human Rights* 19, no. 6 (2015): 737-756.

60 Stephen J. Kobrin, "Private Political Authority and Public Responsibility: Transnational Politics, Transnational Firms, and Human Rights," *Business Ethics Quarterly* 19, no. 3 (2009): 349-374.

61 These are: *LOI n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre* [French Duty of Vigilance Law], Legifrance, accessed June 10, 2025, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034290632; *Wet zorgplicht kinderarbeid* [Dutch Child Labour Due Diligence Act], Staatsblad, no. 401/2019 of October 24, 2019; *Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten* [German Corporate Due Diligence in Supply Chains Act], BGBl. no. 46 of July 22, 2021; *Lov om virksomhet, ers åpenhet og arbeid med grunnleggende menneskerettigheter og anstendige*

decisions.[62] They have also been adopted or referenced by subsequent international instruments in this domain, including: the OECD Guidelines for Multinational Enterprises (2011);[63] the International Labour Organization's Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy (2017);[64] the International Finance Corporation's Performance Standards (2012);[65] the 2030 Agenda for Sustainable Development; and most recently, CSDDD, which also amends Directive (EU) 2019/1937 and Regulation (EU) 2023/2859.[66]

5.1.2 Directive (EU) 2024/1760 (CSDDD)

Regarding the personal scope, the CSDDD applies to very large EU companies employing more than 1,000 employees and generating a net worldwide annual turnover of over EUR 450 million, regardless of the sector in which they operate.[67] The Directive also applies to non-EU companies that generate a net turnover of more than EUR 450 million within the EU. The provision on the personal scope of the Directive was highly debated and became one of its most significant limitations.[68] Regarding the material scope, companies falling within the scope of the CSDDD are expected to undertake due diligence in relation to their human rights and environmental impacts, with the objective of preventing adverse human rights impacts. The Directive defines an "adverse human rights impact" as one resulting from an abuse of selected human rights tailored specifically to corporate conduct,[69] as well as other rights enshrined in a list of international instruments.[70] These additional rights, derived from listed instruments, are deemed relevant if they are capable of being abused by a company,

arbeidsforhold (åpenhetsloven) [Norwegian Act Relating to Enterprises' Transparency and Work on Fundamental Human Rights and Decent Working Conditions], Lovedata, accessed June 10, 2025., https://lovdata.no/static/lovtidend/ltavd1/2021/nl-20210618-099.pdf.

62 District Court of The Hague, Milieudefensie v. Royal Dutch Shell, Judgment of May 26, 2021, NL:RBDHA:2021:5339, especially para. 4.4.11.

63 OECD, "OECD Guidelines for Multinational Enterprises (1976, amended 2011)", accessed May 15, 2025, https://www.oecd.org/investment/mne/48004323.pdf.

64 ILO, "Tripartite Declaration of Principles Concerning Multinational Enterprises and Social Policy" (2017), accessed May 15, 2025, https://www.ilo.org/empent/areas/mne-declaration/WCMS_570332/lang--en/index.htm. It applies to states, trade unions and businesses.

65 International Finance Corporation, "Environmental and Social Performance Standards" (2012), accessed June 30, 2025, https://www.ifc.org/wps/wcm/connect/Topics_Ext_Content/IFC_External_Corporate_Site/Sustainability-IFC/Policies-Standards/Performance-Standards.

66 Regulation (EU) 2023/2859 of the European Parliament and of the Council of 13 December 2023 establishing a European single access point providing centralised access to publicly available information of relevance to financial services, capital markets and sustainability, OJ L 2023/2859, 20.12.2023.

67 Art. 2(2) of the CSDDD.

68 Civil society organisations deplored that the current thresholds would cover only about 5,500 companies in the entire EU. See: European Coalition for Corporate Justice, "CSDDD Endorsement Brings Us 0.05% Closer to Corporate Justice," 15 March 2024, accessed April 2, 2025, https://corporatejustice.org/news/reaction-csddd-endorsement-brings-us-0-05-closer-to-corporate-justice/.

69 Art. 3(3) of the CSDDD.

70 Annex I, Part I, Section II. of the CSDDD.

impair a legal interest, and if the company could have reasonably foreseen that such rights might be affected.[71]

Although the Annex initially appears comprehensive, the decision to include only certain human rights and international instruments - excluding, notably, the Universal Declaration of Human Rights - marks a departure from the UNGPs' broader approach. In the context of our article, it is significant that Part I of the Annex lists the prohibition of arbitrary or unlawful interference with a person's privacy, family, home, or correspondence, as well as unlawful attacks on their honour or reputation. These rights are to be interpreted in line with Art. 17 of the International Covenant on Civil and Political Rights.[72]

Therefore, under the CSDDD, member states are obliged to ensure that relevant companies conduct due diligence.[73] In the context of privacy protection this means that those companies must integrate due diligence into their privacy policies in a way to:

- identify actual or potential adverse impacts on employees' privacy;
- prevent and mitigate potential adverse impacts on employees' privacy;
- bring actual adverse impacts on employees' privacy to an end, minimise their extent and remediate;
- establish and maintain a notification and complaints procedure;
- monitor the effectiveness of their due diligence policy and measures and
- publicly communicate on due diligence.

In this regard companies must take "appropriate measures" and consider specific factors when designing them.[74] Appropriate measures are defined as measures "capable of achieving the objectives of due diligence by effectively addressing adverse impacts in a manner commensurate to the degree of severity and the likelihood of the adverse impact."[75] Risk factors include geographic and contextual factors and factors specific to a product, service and business operations.[76]

The CSDDD also includes an obligation to conduct meaningful consultation with stakeholders at the different stages of the due diligence process.[77] Stakeholders are widely defined and include companies' employees, employees of its subsidiaries, trade unions and workers' representatives, consumers and other affected individuals, groups and communities but also national human rights and environmental institutions or civil society organisations whose purpose includes environmental protection.[78] The CSDDD requires that a company's due diligence covers not only a company's operations and the operations of its subsidiaries, but also that of its business partners in its so-called "chain of activities."[79]

---

71 Art. 3(c) of the CSDDD.
72 Annex, Part one, (4) of the CSDDD.
73 Art. 7 of the CSDDD.
74 Art. 8 of the CSDDD.
75 Art. 3(1)(q) of the CSDDD.
76 Art. 3(1)(q) of the CSDDD.
77 Art. 13(3) of the CSDDD.
78 Art. 3(1)(n) of the CSDDD.
79 Chain of activities' means: „activities of a company's upstream business partners related to

The CSDDD is the first mandatory due diligence instrument that introduces two complementary enforcement mechanisms.[80] The Directive establishes a mixed public and private enforcement regime, involving both public supervisory authorities and a civil liability provision. Under the public enforcement mechanism, Member States are required to designate a supervisory authority responsible for monitoring compliance. This authority is empowered to issue injunctions - such as orders to cease an infringement or provide appropriate remediation - adopt interim measures, and impose penalties, including pecuniary sanctions of up to 5% of the company's worldwide net turnover. [81]

In parallel, the CSDDD introduces a fault-based civil liability mechanism designed to provide access to justice for victims of adverse impacts. However, the conditions for liability are relatively restrictive: the claimant must prove that damage occurred to a person as a result of an adverse impact, that the company failed to prevent or end this impact either negligently or intentionally, and that a causal link exists between this failure and the damage. Notably, causation is excluded if the damage was caused solely by the company's business partners. All of these elements must be established by the claimant. To alleviate this burden of proof, domestic courts must be able to order the disclosure of evidence under the control of the company, in accordance with national procedural law.[82]

Although the CSDDD aims to promote corporate accountability and uphold human rights through due diligence assessments of corporate operations and supply chains, several shortcomings can be identified with regard to employee privacy protection:

- Lack of specific privacy guidelines, leading to inconsistent implementation;
- Limited scope, as the Directive may not cover all sectors or types of companies, resulting in regulatory gaps for certain industries and smaller businesses;
- Ambiguity in consent requirements;
- Insufficient enforcement mechanisms;
- Divergent national interpretations;

---

the production of goods or the provision of services by that company, including the design, extraction, sourcing, manufacture, transport, storage and supply of raw materials, products or parts of products and the development of the product or the service; and (ii) activities of a company's downstream business partners related to the distribution, transport and storage of a product of that company, where the business partners carry out those activities for the company or on behalf of the company, and excluding the distribution, transport and storage of a product that is subject to export controls under regulation (EU) 2021/821 or to the export controls relating to weapons, munitions or war materials, once the export of the product is authorised." (Art. 3(1)(g) of the CSDDD).

80 A 2017 report by the UN Working Group on Business and Human Rights, emphasised the need to ensure that rights holders are an integral part of any process that aims to provide an effective remedy for corporate human rights abuses. UN General Assembly, Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, A/72/162 of July 18, 2017.

81 Art. 24-27 of the CSDDD.

82 Art. 29(3)(e) of the CSDDD.

- Potential conflicts with other regulations;
- Risk of "tick-box compliance," whereby companies meet only the minimum legal requirements without meaningfully engaging in due diligence, thereby undermining the Directive's objectives.

As previously noted, due to the limited personal scope of the CSDDD, certain industries and smaller companies are not subject to its obligations and therefore are not required to adopt a human rights due diligence approach to privacy protection in the workplace. In such cases, it becomes essential for companies to adopt internal privacy protection policies that incorporate core data protection principles, such as purpose specification and limitation, prior informed consent, data minimization, use limitation, and, importantly, ethical considerations in order to avoid costly litigation processes.

Given that both the *privacy by design* and *human rights due diligence* frameworks exhibit shortcomings in protecting employee privacy, the next section will explore the potential for integrating these two approaches to bridge the existing gaps in this context.

6 COULD INTEGRATION OF HUMAN RIGHTS DUE DILIGENCE AND PRIVACY BY DESIGN FRAMEWORK MITIGATE DIGITAL PANOPTICISM IN THE WORKPLACE?

In the previous sections possibilities and shortcomings of human rights due diligence and privacy by design frameworks have been explained. The question is: could possibilities of human rights due diligence prevail (compensate) shortcomings of privacy by design framework and *vice versa*? In other words, could the integration of these two frameworks create new framework that has a power of mitigation of the panopticism in the modern workplace? First, we need to make distinction between these two frameworks in the context of the protection of workplace privacy.

6.1 Distinguishing Due Diligence and Privacy by Design in the Protection of Workplace Privacy

Human Rights Due Diligence and Privacy by Design are two widely recognized frameworks aim to protect privacy in the workplace. While both approaches mitigate risks to employee privacy, they differ in their conceptual foundations, focus and scope, implementation methods, and regulatory requirements. By analyzing those differences within the context of workplace privacy, we highlight their complementary roles and provide a framework for organizations seeking to integrate both approaches effectively.

Key differences between HRDD and PbD regarding their conceptual foundations include:

- HRDD has its foundation in human rights law and stress an organization's responsibility to protect fundamental human rights, including privacy, under international legal frameworks (e.g., the Universal declaration of human

rights and the International covenant on civil and political rights).

- PbD, on the other hand, has its source in data protection law and focuses on integrating privacy protections into systems and technologies in a manner that complies with data protection laws like the General Data Protection Regulation.
- Furthermore, the differences between these two frameworks regarding implementation and process are as follows:
- HRDD requires ongoing risk assessments and stakeholder engagement to prevent and mitigate human rights violations. [83] It involves a more extensive and continuous process of monitoring, assessing, and addressing risks related to employee privacy.
- PbD is implemented through system design and data handling practices, meaning that privacy is considered during the development phase. In this way, the organization ensures the creation of privacy-friendly systems and data minimization practices.
- Considering the regulatory basis, these two frameworks differ in the following ways:
    1. HRDD aligns with the *UN Guiding Principles on Business and Human Rights* and the legally binding *Corporate Sustainability Due Diligence Directive* (CSDDD).
    2. PbD has regulatory basis in data protection laws, notably the *General Data Protection Regulation* (GDPR), which is legally binding and requires organizations to demonstrate compliance with privacy principles.
- In terms of stakeholder responsibility, the frameworks differ as follows:

HRDD places responsibility on organizations to address the rights of workers by considering both the operational impact on employees and the interests of relevant stakeholders.

PbD assigns primary responsibility to technical and operational teams to design systems that ensure privacy protection throughout the lifecycle of personal data.

As we have seen, although HRDD and PbD share the common goals of protecting privacy and preventing harm, they operate in different yet complementary ways. HRDD offers a broad, human rights–oriented framework that requires companies to actively assess and manage the impact of their actions on workers' rights. It encourages proactive engagement and stakeholder involvement, which is especially important in workplaces where surveillance and data collection are pervasive. PbD, on the other hand, focuses specifically on data privacy and security at the system level. It requires organizations to embed privacy protections at every stage of data handling - from collection to processing, storage, and destruction.

By integrating both approaches, organizations can more effectively safeguard employee privacy, ensuring compliance with legal requirements and adherence

83 Lise Smit et al., "Human Rights Due Diligence in Global Supply Chains: Evidence of Corporate Practices to Inform a Legal Standard," *The International Journal of Human Rights* 25, no. 6 (2020): 945-973.

to ethical standards in increasingly digitalized workplaces. Real-world examples demonstrate that it is possible to build systems that not only comply with regulations but also uphold fundamental rights.[84]

In the subsequent section, we examine the Croatian legal framework governing the protection of privacy in the workplace and assess the degree to which the principles of Privacy by Design and Human Rights Due Diligence are integrated into the mitigation of digital panopticism in the employment context.

7 MITIGATING DIGITAL PANOPTICISM IN CROATIAN WORKPLACES: LEGAL FRAMEWORK FOR EMPLOYEE PRIVACY PROTECTION

In the Croatian legal system, the protection of employees' privacy and the regulation of monitoring activities are embedded within a complex normative framework consisting of the Labour Act,[85] the Occupational Safety and Health Act[86] and the Act on the Implementation of the General Data Protection Regulation.[87] These statutes, read in conjunction with the EU's General Data Protection Regulation

84 After criticism from privacy advocates and scholars, Microsoft faced scrutiny over its "Productivity Score" tool, initially released as part of Microsoft 365, which allowed employers to monitor individual employee activity. Microsoft revised the tool to align better with human rights and privacy by design principles. The result of the revision is Microsoft's Productivity Score: Privacy-Centric Redesign, tool that aggregate data at the organizational level, removing identifiable information about individual employees. "Microsoft 365 Removes Per-User Data in Productivity Monitoring Tool," The Guardian, accessed June 1, 2025, https://www.theguardian.com/technology/2020/dec/02/microsoft-apologises-productivity-score-critics-derided-workplace-surveillance. IBM's Transparent Remote Work Monitoring is software which IBM implemented during the pandemic for the monitoring of remote workers, which initially faced employee reactions over privacy concerns. In response IBM has incorporated transparent guidelines and employee feedback into the process, demonstrating a commitment to balancing organizational needs with employee privacy. Studies indicate that 54% of employees are more productive when they feel their privacy is respected. Vorecol, "How Do Workplace Surveillance Practices Differ Across States, and What Can Employers Learn from These Variations?," accessed June 1, 2025, https://vorecol.com/blogs/blog-how-do-workplace-surveillance-practices-differ-across-states-and-what-can-employers-learn-from-these-variations-206966. SAP's SuccessFactors is platform that offers workforce analytics designed with privacy considerations. The system emphasizes data minimization, transparency, and user consent, aligning with privacy by design principles. Cisco's Ethical Use of Collaboration Analytics - provides analytics tools within its collaboration platforms, such as Webex, to help organizations understand usage patterns. Cisco emphasizes ethical data use by aggregating data and avoiding intrusive monitoring. Their approach includes clear communication with users about what data is collected and how it is used, ensuring alignment with privacy by design principles. "SAP SuccessFactors: Cloud-Based HCM with Core HR, Talent, and Analytics," accessed June 1, 2025, https://learning.sap-press.com/sap-successfactors.

85 *Zakon o radu* [Labour Act], Official Gazette, no. 93/14, 127/17, 98/19, 151/22, 64/23.

86 *Zakon o zaštiti na radu* [Occupational Safety and Health Act], Official Gazette, no. 71/14, 118/14, 154/14, 92/15, 86/18, 115/18, 151/22.

87 *Zakon o provedbi Opće uredbe o zaštiti podataka* [Act on the Implementation of the General Data Protection Regulation], Official Gazette, no. 42/18.

(GDPR), form a layered structure of substantive and procedural guarantees which regulate the conditions under which management may lawfully monitor employees' behaviour.

Art. 28 of the Croatian Labour Act establishes the core legal framework for employee privacy protection in Croatia. Its purpose is to balance the legitimate interests of the employer (security, efficiency, and asset protection) with the fundamental right of employees to privacy and dignity. According to art. 28 employees' personal data may be collected, processed and delivered to third parties only if so specified by this or another act or if necessary for the exercise of rights and obligations from or relating to employment. The employer must specify in advance, in the work regulations, which data will be collected, processed, used, or disclosed to third parties for that purpose. Employers who employ at least twenty workers must appoint a person who enjoys workers' confidence and who is, apart from the employer himself, authorized to monitor if workers' personal data are processed and provided to third parties in accordance with the law. Incorrectly recorded personal data must be immediately rectified and the data for the retention of which there are no longer legal or actual reasons must be erased or otherwise removed. Also, we should point out here the relevancy of rules of Labour Act on employer's obligation to seek Workers' Council's approval before adopting a decision on the processing and transfer of employees' personal data and to consult the Council before adopting a decision relevant for employees' health and safety at work, and introduction of new technology and changes in the organization and mode of work, that can, *inter alia*, jeopardise employee's right to privacy.

Furthermore, Labour Act regulates protection of privacy and processing of personal data of employees engaged through digital labour platforms. Namely, to ensure the protection of workers' privacy a digital labour platform and an aggregator, shall not process data relating to private communications, data concerning a worker's emotional or psychological state, data concerning a worker's health, except in cases provided for under personal data protection legislation, nor collect personal data during periods when the worker is neither performing work nor making himself/herself available for work.[88]

Additionally, the Labour Act provides specific safeguards for remote workers, requiring employers to uphold the protection of their privacy and to ensure working conditions that do not compromise their safety or health. This obligation applies where such protection is feasible, taking into account the nature of the work and the level of risk to the worker's life and health, as assessed in accordance with occupational health and safety regulations governing remote work.[89]

These provisions limit the employer's ability to collect or monitor employees' personal data exclusively to cases permitted by law or necessary for exercising rights and obligations arising from employment reflecting several foundational GDPR principles: lawfulness, fairness, purpose limitation, and data minimization;[90] lawful

88 Art. 221 j of the Labour Act.
89 Art. 17b 5. and 6. of the Labour Act.
90 Art. 5 of the GDPR.

bases for processing,[91] transparency and accountability,[92] and special observations on data processing in the context of employment.[93]

Occupational Safety Act regulates video surveillance[94] for work safety and security purposes only for controlling entries into and exits from work premises and reducing exposure of workers to risk of robbery, burglary, violence, theft and similar events at work or in connection with work. Employers must notify the employees on the monitoring in writing at the time of hiring. Monitoring cannot cover areas intended for personal hygiene and changing rooms. Furthermore, employers may only use video surveillance upon prior consent of Workers' Council (or trade union representative if there is no Council) in case of continuous monitoring of all movements of employees during their work or if devices are placed so that the employees are in their field of vision at all times during work. The employer may not use recorded material for purposes other than those prescribed in the act, may not broadcast them in public or to persons who are not authorized to supervise general safety and health at work, and is obliged to ensure that the recordings are not made available to unauthorized persons.

According to the Act on Implementation of the General Data Protection, unless otherwise prescribed by another act, the processing of personal data by video surveillance is subject to this act. Monitoring through video surveillance refers to the collection and further processing of personal data that involves the making of recordings forming or intending to form part of the storage system. Such processing may only be carried out for a purpose that is necessary and justified for the protection of persons and property unless there are prevailing interests of data subjects contravening such processing. Monitoring may only cover rooms, parts of business premises, outer surface of the building as well as the interior of public transport vehicles.[95] The Act prescribes a retention period of up to six months for video recordings, unless other acts provide for a longer period or if they are used as evidence in court, administrative, arbitration or other equivalent proceedings. Competent state bodies may access personal data collected by video surveillance in the performance of their statutory duties.

The processing of employees' personal data through a video surveillance system may be carried out only if, in addition to the conditions laid down by this Act, the conditions established by regulations governing occupational safety are also fulfilled, and if employees have been properly informed in advance about such a measure, as well as if the employer has informed the employees before making the decision to install the video surveillance system. Video surveillance of work premises must not include rooms intended for rest, personal hygiene, or changing clothes.[96]

Furthermore, the Act provide for possibility to process biometric data of

91 Art. 6 of the GDPR.
92 Art. 13, 14 of the GDPR.
93 Art. 88 of the GDPR.
94 Art. 43 of the Occupational Safety and Health Act.
95 Art. 26 of the Act on the Implementation of the General Data Protection Regulation.
96 Art. 26 of the Act on the Implementation of the General Data Protection Regulation.

employees only for the purpose of recording working hours and for entry into and exit from official premises, if prescribed by law or if such processing is carried out as an alternative to another solution for recording working hours or entry into and exit from official premises, provided that the employee has given explicit consent for such processing of biometric data in accordance with the provisions of the GDPR.[97]

Despite Croatian's law alignment with EU privacy standards and relatively strong statutory basis for employee privacy protection that it provides, the Labour Act, Occupational Safety and Health Act, and Act on the Implementation of the GDPR demonstrate failure in their coordination, enforcement and remain insufficiently responsive to the challenges of the digital workplace.

These legislative gaps expose systemic failures to operationalize the principles of Privacy by Design (PbD) and Human Rights Due Diligence (HRDD) in the employment context. The resulting gap between formal compliance and substantive protection exposes employees to forms of digital panopticism and algorithmic control inconsistent with European human rights standards.

Namely, Croatian labour legislation still holds to reactive, not proactive approach to privacy protection in the workplace. Due to the fact that Croatia has not yet implemented CSDDD there is no legal obligation to carry out Data Protection Impact Assessment (DPIA) prior to implementing surveillance, biometric, or monitoring technologies. Also, the legislation does not set specific technical or organizational standards to ensure privacy-by-default settings, data minimization, or end-to-end security. Consequently, privacy risks in the workplace are assessed *post factum* after intrusion into employees' privacy is occurred. Furthermore, although there is legal obligation for employers to inform employees about monitoring measures, there is no legal requirement for consultation or participation of employees' representative bodies in the process of design or implementation of those monitoring systems.

In the context of the implementation of HRDD principle in the sphere of employee's privacy protection, it should be stressed that neither the Labour Act nor the Occupational Safety and Health Act require employers to conduct human rights impact assessments for workplace technologies that may affect privacy, dignity, or equality. This reactive approach conflicts with HRDD's preventive strategy, which requires continuous assessment and mitigation of human rights risks.

Also, HRDD prioritizes stakeholder engagement and grievance mechanisms. Croatian law does not mandate worker consultation before adopting monitoring systems, nor does it provide an effective remedy for privacy-related harms in employment. Complaints are dispersed between the Data Protection Agency (AZOP),[98] the Labour Inspectorate, and the courts, without a coordinated oversight mechanism. This institutional fragmentation leaves employees with limited access to justice and weakens accountability for corporate misuse of personal data.

97 Art. 23 of the Act on the Implementation of the General Data Protection Regulation.
98 Art. 4 of the Act on the Implementation of the General Data Protection Regulation.

8 CONCLUSION

After explaining the specific characteristics of the employment relationship - particularly the inequality of bargaining power that allows employers to dictate the terms of employment and control how work is performed - the issue of the *digital panopticon* and employee privacy protection in the contemporary workplace is dealt with. The aim of this article is to explore the potential of existing legal frameworks and privacy-by-design approaches to address the challenges of privacy protection. Having identified several shortcomings in legislative approaches, corporate practices, and the demands of workers and their representatives - shortcomings that hinder the effective balancing of managerial prerogatives and employee privacy - the potential of Human Rights Due Diligence (HRDD) is examined to help overcome these problems. It can be concluded that digital panopticism and corporate due diligence are not inherently incompatible. However, unchecked workplace surveillance conducted under the guise of compliance can undermine core ethical principles and erode corporate legitimacy. In this context, HRDD retains the potential to reshape preventative approaches to mitigating adverse human rights impacts. In particular, it is emphasized that HRDD must be a holistic and ongoing process - one that extends well beyond traditional workplace audits.

Furthermore, "mandatory privacy due diligence is essential to counteract the many failures of industry self-regulation."[99] At present, this issue is dealt with in the CSDDD. Also, a key aspect to be carried out in the future must be to provide incentives in order for companies to stay involved with new and progressing marketplaces instead of making careless abandonment of emerging markets. Achievement of Directive goals furthermore depends on linking implementation and relevant technical assistance and programs that expand the capacities of companies engaged earlier in processes, at the same time simultaneously supporting entities involved at the end of processes thereby providing incentives to enduring suppliers. Member states will have to integrate the Directive into their own national systems of law and to found responsible and just authorities at a national level.[100] "At the same time, it is imperative to reaffirm the ongoing relevance of the UN Guiding Principles on Business and Human Rights (UNGPs) for all companies - regardless of size, sector, or geographical reach - as well as the importance of promoting alternative verification mechanisms to social auditing and industry-led initiatives, such as community-based monitoring."[101] The principles outlined in the UNGPs are vital for protecting human rights, including privacy, especially in companies that fall outside the scope of the CSDDD.

When implemented, privacy protection due diligence (PPDD) must focus on outcomes, not just processes. It is essential that businesses understand PPDD not merely as a symbolic gesture but as a mechanism requiring substantive compliance

99 Jowita Mieszkowska, "The Unintended Consequences of the EU Corporate Sustainability Due Diligence Directive," *American Journal of International Law Unbound* 118 (2024): 291-296.

100 Mieszkowska, "The Unintended Consequences," 296.

101 Mieszkowska, "The Unintended Consequences," 296.

with human rights standards and a shift in decision-making approaches. Legislation mandating PPDD should both incentivize effective implementation and ensure accountability for non-compliance.

For PPDD to be effective, it must also include rights holders as key participants in the process.

In conclusion, employers seeking to foster effective workplace privacy protection should embed key insights from data protection, legal, and ethical frameworks into their existing corporate due diligence models, thereby establishing a Privacy Due Diligence approach. By incorporating a three-pillar framework - consisting of transparency, data minimization, and participatory governance - into their due diligence processes, companies can meet regulatory and risk management objectives without compromising individual autonomy. As we have seen, both, the privacy by design and human rights due diligence frameworks exhibits shortcomings in protecting employee privacy. For comprehensive privacy protection in the workplace, organizations should adopt a new privacy protection framework that incorporates both approaches. In that framework HRDD should play a guiding role in the creation of organizational policies and in conducting risk assessments, while PbD should shape the design and implementation of privacy-preserving technologies. Real-world examples demonstrate that it is possible to build systems that not only comply with regulations but also uphold fundamental rights.

In Croatia to bridge aforementioned gaps in legal framework for the employee privacy protection following policy and legal recommendations should be followed: amend the Labour Act and Occupational Safety and Health Act to require combined data protection and human rights impact assessments; introduce mandatory worker consultation prior to any surveillance implementation, aligning with HRDD principles; enhance coordination between Agency for the Protection of Personal Data and the Labour Inspectorate to ensure coherent enforcement and establish specialized units within those two bodies to monitor digital workplace surveillance,[102] remote work, and platform labor; replace consent-based processing with legitimate interest grounded in safeguards and proportionality and finally adopt sector-specific rules under Art. 88 GDPR to regulate workplace data processing explicitly within PbD and HRDD frameworks and include best practices for platform and remote work.

BIBLIOGRAPHY

Books and Articles:

1. Bailey, Dieane E. "Emerging Technologies at Work: Policy Ideas to Address Negative Consequences for Work, Employees, and Society." *ILR Review* 75, no. 3 (2022): 527-551.
2. Barclay, Lizabeth A., and Karen S. Markel. "Discrimination and Stigmatization in Work Organizations: A Multiple-Level Framework for Research on Genetic Testing." *Human Relations* 60, no. 6 (2023): 953-980.

102 Croatian Personal Data Protection Agency (AZOP), "Guidelines on Video Surveillance in the Workplace," 2021, accessed November 1, 2025., https://azop.hr/videonadzor-preporuka/.

3. Bonetti, Francesca, and Giorgio Casoni. "Brain Training, Mindfulness, and Wearables: Empowering Employee Wellbeing Through Neurotechnologies." *Diid Disegno Industriale Industrial Design* (2023). https://doi.org/10.30682/diiddsi23t3e.
4. Botan, Carl. "Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects." *Communication Monographs* 63, no. 4 (1996): 293-313.
5. Bright, Claire, Axel Marx, Nina Pineau, and Jan Wouters. "Towards a Corporate Duty for Lead Companies to Respect Human Rights in Their Global Value Chains?" *Business and Politics* 22, no. 4 (2020): 667-697.
6. De Montjoye, Yves-Alexandre, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. "Unique in the Crowd: The Privacy Bounds of Human Mobility." *Scientific Reports* 3, article no. 1376 (2013): 1-5.
7. Deva, Surya. *Regulating Corporate Human Rights Violations: Humanizing Business.* London: Routledge, 2012.
8. Deva, Surya, and David Bilchitz, eds. *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect?* Cambridge: Cambridge University Press, 2013.
9. Dix, Alexander. "Built-in Privacy - No Panacea, but a Necessary Condition for Effective Privacy Protection." *Identity in the Information Society* 3 (2010): 257-265.
10. Ebert, Isabel, Isabelle Wildhaber, and Jeremias Adams-Prassl. "Big Data in the Workplace: Privacy Due Diligence as a Human Rights-Based Approach to Employee Privacy Protection." *Big Data & Society* 8, no. 1 (2021): 1-13.
11. Finkin, Matthew W. "Menschenbild: The Conception of the Employee as a Person." *Western Law Review* 23, no. 2 (2002): 567-590.
12. Foucault, Michel. "'Panopticism' from 'Discipline & Punish: The Birth of the Prison'." *Race/Ethnicity: Multidisciplinary Global Contexts* 2, no. 1 (2008): 1-12.
13. Freedland, Mark, and Nicola Kontouris. *The Legal Construction of Personal Work Relation*. Oxford: Oxford University Press, 2011.
14. Hendrickx, Frank. "Employee Privacy." In *Comparative Labour Law and Industrial Relations in Industrialized Market Economies*, ed. Roger Blanpain, 399-422. Alphen aan den Rijn: Kluwer Law International, 2001.
15. Holton, Carolyn. "Identifying Disgruntled Employee Systems Fraud Risk Through Text Mining: A Simple Solution for a Multi-Billion-Dollar Problem." *Decision Support Systems* 46, no. 4 (2009): 853-864.
16. Kellogg, Katherine C., Melissa A. Valentine, and Angèle Christin. "Algorithms at Work: The New Contested Terrain of Control." *Academy of Management Annals* 14, no. 1 (2020): 366-410.
17. Kivimäki, Mika, et al. "Long Working Hours and Risk of Coronary Heart Disease and Stroke: A Systematic Review and Meta-Analysis of Published and Unpublished Data for 603,838 Individuals." *The Lancet* 386, no. 10005 (2015): 1739-1746.
18. Knudsen, Jette Steen, and Jeremy Moon. "Visible Hands: Government Regulation and International Business Responsibility." *Cambridge Journal of Economics* 41, no. 2 (2017): 383-409.
19. Kobrin, Stephen J. "Private Political Authority and Public Responsibility: Transnational Politics, Transnational Firms, and Human Rights." *Business Ethics Quarterly* 19, no. 3 (2009): 349-374.
20. Kroener, Inga, and David Wright. "A Strategy for Operationalizing PbD." *The Information Society* 30, no. 5 (2014): 355-365.
21. Lemos, Janaina, Vanessa Borba de Souza, Frederico Soares Falcetta, Fernando Kude de Almeida, Tânia M. Lima, and Pedro Dinis Gaspar. "Enhancing Workplace Safety through Personalized Environmental Risk Assessment: An AI-Driven Approach in Industry 5.0." *Computers* 13, no. 5 (2024): 1-21.

22. Marin-Farrona, Maria, Brad Wipfli, Saurabh S. Thosar, Enrique Colino, Jorge Garcia-Unanue, Leonor Gallardo, Jose Luis Felipe, and Jorge López-Fernández. "Effectiveness of Worksite Wellness Programs Based on Physical Activity to Improve Workers' Health and Productivity: A Systematic Review." *Systematic Reviews* 12, article no. 87 (2023): 1-13.
23. Martinez, Wendy, Johann Benerradi, Serena Midha, Horia A. Maior, and Max L. Wilson. "Understanding the Ethical Concerns for Neurotechnology in the Future of Work." In *CHIWORK '22: Proceedings of the 1st Annual Meeting of the Symposium on Human-Computer Interaction for Work*, eds. Andrew L. Kun et al., 1-19. New York: Association for Computing Machinery, 2022.
24. Mattke, Soeren, Hangsheng Liu, John Caloyeras, Christina Y. Huang, Kristin R. Van Busum, Dmitry Khodyakov, and Victoria Shier. "Workplace Wellness Programs Study: Final Report." *RAND Health Quarterly* 3, no. 2 (2013): 1-137.
25. Mieszkowska, Jowita. "The Unintended Consequences of the EU Corporate Sustainability Due Diligence Directive." *American Journal of International Law Unbound* 118 (2024): 291-296.
26. Min, Beomjun, et al. "The Effectiveness of a Neurofeedback-Assisted Mindfulness Training Program Using a Mobile App on Stress Reduction in Employees: Randomized Controlled Trial." *Journal of Medical Internet Research mHealth and uHealth* 3, no. 11 (2023). https://doi.org/10.2196/42851.
27. Mishra, Jitendra M., and Suzanne M. Crampton. "Employee Monitoring: Privacy in the Workplace?" *S.A.M. Advanced Management Journal* 63, no. 3 (1998): 4-14.
28. Muhl, Ekaterina. "The Challenge of Wearable Neurodevices for Workplace Monitoring: An EU Legal Perspective." *Frontiers in Human Dynamics* 6 (2024): 1-11.
29. Muhl, Ekatarina, and Roberto Andorno. "Neurosurveillance in the Workplace: Do Employers Have the Right to Monitor Employees' Minds?" *Frontiers in Human Dynamics* 5 (2023): 1-11.
30. Mujeye, Stephen, and Yair Levy. "Complex Passwords: How Far is Too Far? The Role of Cognitive Load on Employee Productivity." *Online Journal of Applied Knowledge Management* 1, no. 1 (2013): 122-132.
31. Nagy, Peter, and Gina Neff. "Imagined Affordance: Reconstructing a Keyword for Communication Theory." *Social Media + Society* 1, no. 2 (2015): 1-9.
32. Nebeker, Delbert M., and Charles B. Tatum. "The Effects of Computer Monitoring, Standards and Rewards on Work Performance, Job Satisfaction and Stress." *Journal of Applied Social Psychology* 23, no. 7 (1993): 508-536.
33. Nolan, Justine. "The Corporate Responsibility to Respect Human Rights: Soft Law or Not Law?" In *Law and Society,* ed. L. C. Backer. Edward Elgar Publishing, 2021.
34. Peña, Isidro, Silvia María Andrade, and Virginia Barba-Sánchez. "Wellness Programs, Perceived Organizational Support, and Their Influence on Organizational Performance: An Analysis Within the Framework of Sustainable Human Resource Management." *SAGE Open* 14, no. 1 (2024): 1-14.
35. Regan, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995.
36. Ruggie, John G. *Just Business: Multinational Corporations and Human Right.* W. W. Norton & Company, 2013.
37. Scheper, Christian. "From Naming and Shaming to Knowing and Showing: Human Rights and the Power of Corporate Practice." *The International Journal of Human Rights* 19, no. 6 (2015): 737-756.
38. Smit, Lise, et al. "Human Rights Due Diligence in Global Supply Chains: Evidence of Corporate Practices to Inform a Legal Standard." *The International Journal of Human Rights* 25, no. 6 (2020): 945-973.

39. Solove, Daniel J., and Danielle Keats. "Privacy Harms." *Boston University Law Review* 102 (2022): 793-863.
40. Vaught, Bobby C., Raymond E. Taylor, and Steven F. Vaught. "The Attitudes of Managers Regarding the Electronic Monitoring of Employee Behaviour: Procedural and Ethical Considerations." *American Business Review* 1, no. 1 (2000): 107-114.
41. Wacks, Raymond. *Privacy and the Law*. Oxford: Clarendon Press, 1989.
42. Weiss, Manfred. "Re- inventing Labour Law." In *The Idea of Labour Law*, ed. Langille Davidov. Oxford: Oxford University Press, 2011.
43. Wettstein, Florian. "Normativity, Ethics, and the UN Guiding Principles on Business and Human Rights: A Critical Assessment." *Journal of Human Rights* 14, no. 2 (2015): 162-182.
44. Zuboff, Shoshana. *In the Age of the Smart Machine: The Future of Work and Power*. New York: Basic Books, 1998.
45. Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs, 2019.

Legal Sources:

1. Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391-407.
2. Council of Europe, European Convention on Human Rights, ETS No. 5 of November 4, 1950, entered into force September 3, 1953.
3. Data Protection Working Party. Opinion 2/2017 on Data Processing at Work, WP 249 of June 8, 2017.
4. Data Protection Working Party. Working Document on the Surveillance of Electronic Communications in the Workplace, 5401/01/EN/Final, WP 55 of May 29, 2002.
5. Directive (EU) 2019/1152 of the European Parliament and of the Council of 20 June 2019 on transparent and predictable working conditions in the European Union, OJ L 186, 11.7.2019., pp. 105-121.
6. Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859, OJ L 2024/1760, 5.7.2024.
7. *Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten* [German Corporate Due Diligence in Supply Chains Act], BGBl, no. 46 of July 22, 202.
8. International Labour Organization. "Code of Practice on the Protection of Workers' Personal Data." 1997. Accessed May 2, 2025. https://www.ilo.org/public/libdoc/ilo/1997/97B09_118_engl.pdf.
9. International Labour Organisation. "Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy (2017)." Accessed May, 20, 2025. https://www.ilo.org/empent/areas/mne-declaration/WCMS_570332/lang--en/index.htm
10. *LOI n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre* [French Duty of Vigilance Law]. Legifrance. Accessed June 10, 2025. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034290632.
11. *Lov om virksomheters åpenhet og arbeid med grunnleggende menneskerettigheter og anstendige arbeidsforhold (åpenhetsloven)* [Act Relating to Enterprises' Transparency and Work on Fundamental Human Rights and Decent Working Conditions]. Lovedata. Accessed June 10, 2025. https://lovdata.no/static/lovtidend/ltavd1/2021/nl-20210618-099.pdf.
12. Recommendation of the Committee of Ministers to Member States on the processing of personal data in the context of employment, CM/Rec (2015)5 of April 1, 2015.

13. 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), OJ L 119, 4.5.2016, pp. 1-88.
14. Regulation (EU) 2023/2859 of the European Parliament and of the Council of 13 December 2023 establishing a European single access point providing centralised access to publicly available information of relevance to financial services, capital markets and sustainability, OJ L 2023/2859, 20.12.2023.
15. *Wet zorgplicht kinderarbeid* **[**Dutch Child Labour Due Diligence Act], Staatsblad, no. 401/2019 of October 24, 2019.
16. *Zakon o provedbi Opće uredbe o zaštiti podataka* [Act on the Implementation of the General Data Protection Regulation], Official Gazette, no. 42/18.
17. *Zakon o radu* [Labour Act], Official Gazette, no. 93/14, 127/17, 98/19, 151/22, 64/23.
18. *Zakon o zaštiti na radu* [Occupational Safety and Health Act], Official Gazette, no. 71/14, 118/14, 154/14, 92/15, 86/18, 115/18, 151/22.

Case Law:

1. District Court of The Hague, Milieudefensie v. Royal Dutch Shell*,* Judgment of May 26, 2021, NL:RBDHA:2021:5339.
2. ECtHR, Bărbulescu v. Romania*,* App. no. 61496/08, Judgment of September 5, 2017.
3. ECtHR, I v. Finland, App. no. 20511/03, Judgment of July 17, 2008.
4. Judgement of July 16, 2020, Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schrems, C-311/18, EU:C:2020:559.
5. Judgement of October 6, 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, EU:C:2015:650.

Internet Sources:

1. Cavoukian, Ann. "Privacy by Design: The 7 Foundational Principles, 2010." Information and Privacy Commissioner of Ontario. Accessed May, 20, 2025. https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.
2. Croatian Personal Data Protection Agency (AZOP). "Guidelines on Video Surveillance in the Workplace." 2021. Accessed November 1, 2025. https://azop.hr/videonadzor-preporuka/.
3. European Coalition for Corporate Justice. "CSDDD Endorsement Brings Us 0.05% Closer to Corporate Justice." 15 March 2024. Accessed April 2, 2025. https://corporatejustice.org/news/reaction-csddd-endorsement-brings-us-0-05-closer-to-corporate-justice/.
4. Human Rights Council. "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework." Accessed May 15, 2025. https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
5. International Bar Association. "IBA Practical Guide on Business and Human Rights for Business Lawyers." Accessed May 28, 2025. https://www.ibanet.org/MediaHandler?id=d6306c84-e2f8-4c82-a86f-93940d6736c4.
6. International Finance Organisation. "Environmental and Social Performance Standards, 2012." Accessed April 14, 2025. https://www.ifc.org/wps/wcm/connect/Topics_Ext_Content/IFC_External_Corporate_Site/SustainabilityIFC/Policies-Standards/Performance-Standards.
7. "Microsoft 365 Removes Per-User Data in Productivity Monitoring Tool." The Guardian. Accessed June 1, 2025. https://www.theguardian.com/technology/2020/dec/02/microsoft-apologises-productivity-score-critics-derided-workplace-surveillance.

8. OECD. "Due-Diligence Guidance for Responsible Business Conduct, 2018." Accessed June 10, 2025. https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/02/oecd-due-diligence-guidance-for-responsible-business-conduct_c669bd57/15f5f4b3-en.pdf.
9. OECD. "OECD Guidelines for Multinational Enterprises (1976, amended 2011)." Accessed May 15, 2025. https://www.oecd.org/investment/mne/48004323.pdf.
10. Piispanen, Joni Roy, and Rebekah Rousi. "Emotion AI in Workplace Environments: A Case Study." 2024. Accessed February 12, 2025. https://arxiv.org/pdf/2412.09251.
11. "SAP SuccessFactors: Cloud-Based HCM with Core HR, Talent, and Analytics." Accessed June 1, 2025. https://learning.sap-press.com/sap-successfactors.
12. Vorecol. "How Do Workplace Surveillance Practices Differ Across States, and What Can Employers Learn from These Variations?" Accessed June 1, 2025. https://vorecol.com/blogs/blog-how-do-workplace-surveillance-practices-differ-across-states-and-what-can-employers-learn-from-these-variations-206966.

Other:

1. UN Human Rights Council. Business and Human Rights: Towards Operationalizing the "Protect, Respect and Remedy" Framework, A/HRC/11/13 of April 22, 2009.
2. UN Working Group on Business and Human Rights. The report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, A/73/163 of July 16, 2018.

Andrijana Bilić*

Sažetak

INTEGRIRANI PRISTUP ZAŠTITI PRIVATNOSTI RADNIKA U DIGITALNOM OKRUŽENJU: DUŽNA PAŽNJA U POGLEDU LJUDSKIH PRAVA I PRIVATNOSTI PO DIZAJNU

Sveprisutnost digitalnih nadzornih tehnologija na radnom mjestu značajno je preoblikovala suvremene radne odnose, ali je istodobno otvorila brojna pravna i etička pitanja vezana uz privatnost radnika i njihovu autonomiju. Ovaj fenomen se sve češće opisuje pojmom „digitalni panopticizam". U ovome se radu istražuje u kojoj mjeri postojeći pravni okvir, u kombinaciji s pristupom zaštiti privatnosti po dizajnu (PbD), može doprinijeti učinkovitijem odgovoru na izazove zaštite privatnosti radnika. Nakon što se ukazalo na ključne slabosti zakonodavnih rješenja i poslovne prakse, kao i na zahtjeve koje postavljaju radnici i njihovi predstavnici – čimbenike koji narušavaju ravnotežu između upravljačkih ovlasti i prava na privatnost – razmatra se potencijal okvira dužne pažnje u pogledu ljudskih prava (HRDD) za prevladavanje tih izazova. Budući da ni sam HRDD okvir nije bez nedostataka, dodatno se argumentira kako integrirani, sveobuhvatni pristup koji spaja HRDD i načela privatnosti po dizajnu (PbD) može predstavljati učinkovit sustav zaštite prava radnika. Takav pristup, osim što ublažava štetne posljedice digitalnog nadzora, promiče radno okruženje utemeljeno na povjerenju, poštivanju ljudskih prava i većoj organizacijskoj učinkovitosti.

Ključne riječi: *digitalni nadzor; privatnost radnika; privatnost po dizajnu; dužna pažnja u pogledu ljudskih prava; hrvatski pravni okvir za zaštitu privatnosti.*

* Dr. sc. Andrijana Bilić, redovita profesorica, Sveučilište u Splitu, Pravni fakultet; andrijana.bilic@pravst.hr. ORCID: https://orcid.org/0000-0002-1272-4749.