

PROTECTION OF WORKERS IN RELATION TO THE USE OF ARTIFICIAL INTELLIGENCE IN THE WORKPLACE

Accepted

22. 4. 2025

Revised

23. 6. 2025

Published

30. 6. 2025

ASJA LEŠNIK

University of Maribor, Faculty of Law, Maribor, Slovenia, asja.lesnik@student.um.si

CORRESPONDING AUTHOR

asja.lesnik@student.um.si**Keywords**

artificial intelligence,
algorithmic management,
automation of work
processes,
discrimination,
data protection,
privacy protection,
occupational safety and
health,
liability,
worker protection,
legal framework

Abstract This article examines the impact of artificial intelligence (AI) on all stages of the employment relationship and analyses whether the current legal framework adequately protects workers from the risks posed by the use of AI in the workplace. The focus is on Slovenian labour law, while also considering relevant international and EU legal sources such as the AI Act, the Directive on Improving Working Conditions in Platform Work, the GDPR, and the EU Charter of Fundamental Rights. The author addresses legal challenges including discrimination, data protection, privacy, occupational safety and health, and liability for damages. The article finds that while some protective mechanisms already exist, none of the analysed legal sources comprehensively regulate AI use in employment relationships. To ensure effective worker protection, the author argues for either the amendment of current laws or the adoption of dedicated legislation. Since AI will play an even more significant role in Labour Law in the future, it is crucial for the law to adapt in a timely manner to the new challenges posed by AI.



1 Introduction

The integration of artificial intelligence (hereinafter also: AI) into the world of work is no longer a futuristic projection but a present-day reality. Employers are increasingly making use of AI systems in various phases of the employment relationship. As highlighted in recent research, the role of the employer can be automated and digitalised from the beginning of the employment relationship until its termination (Bagari, 2024: 1173; Adams-Prassl, 2019: 13).

In the hiring phase, employers can use AI to streamline and accelerate the recruitment process. Algorithms can handle job postings, screen and rank applications, and select suitable candidates (Šerbec & Polajžar, 2022: 13; Bagari, 2022: 43). During the course of employment, employers can delegate one of the fundamental aspects of employment — issuing instructions to workers and overseeing task performance — to AI. AI can also monitor job tasks and make decisions about employee performance and advancement (Šerbec & Polajžar, 2022: 13; Bagari, 2022: 43). Furthermore, AI plays an important role in the termination of employment. Algorithms can analyse various factors such as goal achievement and task performance, helping employers to make decisions about terminating employment relationships.

Although the use of algorithmic tools in employment relationships has been widely discussed in international literature, particularly in the context of platform work and increasingly also in traditional employment contexts, the legal implications of such practices have so far received limited attention in relation to the Slovenian legal system. This paper seeks to address that gap by critically examining the legal implications of AI deployment in employment relationships from the perspective of Slovenian labour law.

The key research question of this article is whether the increasing use of AI in employment relationships requires the adoption of new, specific legal rules aimed at strengthening worker protection. The paper does not aim to address broader issues related to automation or job displacement but rather focuses on the normative-dogmatic analysis of existing labour law and data protection frameworks, especially in light of the recently adopted Artificial Intelligence Act at the EU level.

Methodologically, the paper adopts a normative-dogmatic approach and is structured as follows: the first section provides an overview of the most relevant legal sources, with an emphasis on the provisions of the Artificial Intelligence Act that are or ought to be relevant in the context of introducing artificial intelligence

systems into work environments. The second section presents several concrete examples of the use of artificial intelligence in different phases of the employment relationship. The third section addresses legal risks and the existing legal framework for the protection of workers. The fourth section assesses whether the current Slovenian labour legislation provides adequate protection for workers in light of AI-driven management practices, and whether specific new legal provisions might be needed. The conclusion summarises the findings and outlines potential directions for future regulation.

2 Legal Sources and Terminology

2.1 Terminology

In practice, the term »artificial intelligence« is often used to describe a wide range of digital tools, but not all of them should be considered AI. Particularly in legal contexts, it is important not to equate AI with any advanced software, computer program, or electronic device. A clear distinction must be made between what qualifies as AI and what does not.

The AI Act¹, in Article 3, defines an AI system as a system based on hardware, designed to operate with varying levels of autonomy and capable, after deployment, of adapting and inferring how to generate outputs — such as predictions, content, recommendations, or decisions — from received input data, which may affect physical or virtual environments.

On February 6, 2025, the European Commission published Guidelines for interpreting the definition of an AI system under Article 3 of the AI Act. It explained that, according to this definition, a system must meet seven key elements to be classified as an AI system:

1. It is based on hardware;
2. It is designed to operate with varying levels of autonomy;
3. It can demonstrate adaptability after deployment;
4. It functions to achieve explicit or implicit goals;
5. It infers how to produce results from received input data;

¹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).

6. The results may include predictions, content, recommendations, or decisions;
7. These results can influence physical or virtual environments (European Commission, 2025: 2).

While definitions of AI systems vary in theory², they share several core characteristics:

- they process data,
- learn from experience,
- make (autonomous) decisions,
- adapt their behaviour based on past outcomes,
- and operate with varying levels of autonomy.

Examples of AI systems include:

- *FAMA*, used in recruitment processes; it evaluates candidate compatibility with company values and identifies potential risks such as inappropriate behaviour or controversial views (Adams-Prassl, 2024: 190–191);
- *Preactor*, used to give instructions to workers; it plans and schedules production work, specifying what and how many products must be manufactured daily (Bri  ne, 2017: 17);
- *Cogito*, used to monitor workers; it tracks and records productivity, with features such as displaying a speedometer icon if a worker speaks too quickly, or a heart icon when greater empathy is needed (Wood, 2021: 6);
- Amazon’s video surveillance system, installed in delivery vehicles, used for disciplinary purposes, including decisions to terminate employment (Wood, 2021: 9).

In theory, the practice of using algorithms to assign tasks, issue instructions, monitor work, and evaluate performance is referred to as »algorithmic management«. The term was first introduced by *Lee* in 2015, who defined it as »software algorithms assuming managerial functions, and the institutional mechanisms that support their implementation in practice«. According to his definition, algorithmic management includes the allocation, optimisation, and evaluation of work through algorithms (Lee et al., 2015: 1603). A similar definition was provided by *Mateescu and Nguyen*, who described algorithmic management as »a set of technological tools and techniques for remotely managing workers, based on data collection and worker

² See eg. Boden, 2016: 1-7; Zuiderveen, 2018: 8.

monitoring, enabling automated or semi-automated decision-making» (Mateescu and Nguyen, 2019: 1).

2.2 International Legal Sources (UN, ILO, Council of Europe)

At the international level, no binding legal instruments have yet been adopted to specifically regulate the field of artificial intelligence (AI). However, AI is already the subject of discussions within the United Nations (UN), the International Labour Organisation (ILO), and the Council of Europe, particularly in the context of various conferences.

So far, the ILO has not adopted any conventions or recommendations concerning AI. However, in May 2024, the Council of Europe adopted the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (hereinafter: Framework Convention), which aligns with the AI Act and incorporates many of its key concepts.

2.2.1 Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law

The purpose of the Framework Convention is to ensure that activities throughout the lifecycle of AI systems are fully consistent with human rights, democracy, and the rule of law. Each signatory to the Framework Convention is obliged to adopt appropriate legislative, administrative, and other measures to implement the provisions of the Convention. These measures must be proportionate to the severity and likelihood of adverse impacts on human rights, democracy, and the rule of law throughout the AI system's lifecycle (Article 1 of the Framework Convention).

The Framework Convention sets out:

- General obligations for signatories (Articles 4 and 5),
- Measures that must be adopted or maintained by the signatories (Article 14).

The remaining provisions largely overlap with the AI Act and include obligations for a risk-based approach, key principles for trustworthy AI, risk management obligations, documentation requirements, and oversight mechanisms for AI-related activities.

2.3 EU Legal Sources

AI and its impact on the labour market are also widely discussed at the EU level. With regard to the application of AI in the labour context, EU secondary legislation is particularly relevant (Bagari, 2023: 232). Key instruments include:

- Regulation (EU) 2024/1689 of the European Parliament and of the Council (the AI Act);
- Directive (EU) 2024/2831 of the European Parliament and of the Council (Directive on Improving Working Conditions in Platform Work)³;
- Directive (EU) 2019/1152 (Directive on Transparent and Predictable Working Conditions)⁴; and
- Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)⁵.

The influence of EU primary law should not be overlooked, especially the Charter of Fundamental Rights of the European Union⁶ (Articles 8, 21, 23, 27, and 31).

2.3.1 The AI Act

The AI Act establishes a unified and comprehensive framework for a so-called "European" approach to AI (Šerbec and Polajžar, 2022: 11). Its purpose is to improve the functioning of the internal market, promote the adoption of human-centric and trustworthy AI, and ensure a high level of protection for health, safety, and fundamental rights under the EU Charter of Fundamental Rights—including democracy, the rule of law, and environmental protection—while also supporting innovation (Article 1(1) of the AI Act).

In addition to general concepts relevant to the use of AI in employment relationships, the AI Act contains specific provisions related to labour.

Chapter III of the AI Act defines "high-risk AI systems"—those with significant adverse effects on health, safety, or fundamental rights. Special attention is given to

³ Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on Improving Working Conditions in Platform Work.

⁴ 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.

⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

⁶ OJ C 202, 7.6.2016, p. 389–405 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV).

the extent of these systems' impact on fundamental rights protected by the EU Charter (Recital 48 of the AI Act).

Article 6(1) provides that an AI system is considered high-risk if both of the following conditions are met:

- (a) The AI system is intended to be used as a safety component of a product or is itself a product covered by EU harmonisation legislation listed in Annex I;
- (b) The product or AI system must undergo third-party conformity assessment under the harmonised legislation before being placed on the market or put into service.

Article 6(2) further identifies other high-risk AI systems as listed in Annex III, including:

4. Employment, worker management, and access to self-employment:

- (a) AI systems for recruitment or selection of natural persons, particularly for targeted job advertising, application screening, and candidate evaluation;
- (b) AI systems used to make decisions about working conditions, promotion, or termination of employment contracts; task allocation based on behaviour, personality traits, or characteristics; or monitoring and evaluating performance and conduct in employment contexts.

This means the AI Act classifies AI systems used for recruitment, worker management, and self-employment access as high-risk, especially when used to make decisions regarding employment conditions, advancement, contract termination, or worker evaluation. Such systems can perpetuate historical patterns of discrimination, for example, against women, certain age groups, persons with disabilities, or individuals of specific racial or ethnic origin or sexual orientation. Additionally, AI systems used to monitor performance or behaviour may infringe on individuals' rights to data protection and privacy (see also Recital 57 of the AI Act).

Beyond classification, the AI Act imposes obligations on providers of high-risk AI systems, including employers⁷ using these systems. Article 26(7) states:

7. Deployers who are employers shall, prior to putting into service or using a high-risk AI system in the workplace, inform workers and their representatives that such

⁷ According to the first paragraph of Article 25 of the Artificial Intelligence Act, under certain conditions, each distributor, importer, installer, or other third party should be considered a provider of a high-risk AI system and, as such, should assume all relevant obligations. The same is stated in point 84 of the preamble of the Artificial Intelligence Act. See also Popa and Pascariu, 2024: 98.

a system will be used in relation to them. This information shall be provided in accordance with EU and national law and practice concerning worker information and consultation.

Thus, employers' primary duty is to inform workers and their representatives about the use of high-risk AI systems.

Furthermore, Article 27 requires deployers (with exceptions not applicable to employers) to carry out a fundamental rights impact assessment before using high-risk AI systems, detailing its required elements.

Recital 44 of the AI Act highlights serious concerns about the scientific reliability of AI systems used to detect or infer emotions, due to cultural, contextual, and individual variation. Such systems may yield unreliable, non-specific, and biased results, leading to discriminatory outcomes and the exclusion of certain groups. They may infringe on dignity, non-discrimination, and principles of equality and fairness. Accordingly, Article 5 of the AI Act prohibits AI practices such as placing on the market or using AI systems to infer emotions of natural persons in the workplace, except when used for health-related purposes.⁸

The term »emotion recognition system« is defined in Recital 18 as systems designed to detect or infer emotions or intentions based on biometric data, such as happiness, sadness, anger, surprise, or embarrassment. The definition excludes physical states like pain or fatigue unless used for accident prevention in pilots or drivers. For example, AI making assumptions about an employee's dissatisfaction based on facial expressions would fall under prohibited use, whereas fatigue detection for safety would not (see Commission Guidelines on Prohibited AI Practices: 83).

Regarding personal data protection, Recital 10 of the AI Act emphasises that the right to data protection is safeguarded by the GDPR, Regulation (EU) 2018/1724, and Directive 2016/680. The AI Act's goal is to support—not undermine—these frameworks.

2.3.1.1 Validity of the AI Act

⁸ For example, emotion recognition can be used for health-related reasons to assist employees with autism and to improve accessibility for blind or deaf individuals. Such use would fall under the exception for health-related reasons. On the other hand, emotion recognition for assessing well-being, motivation levels, and employee job satisfaction does not meet the conditions for 'health-related use' and would be prohibited (Commission Guidelines on Prohibited AI Practices as Defined in the Artificial Intelligence Act, C(2025) 884 final, dated February 4, 2025, p. 88).

From the perspective of the use of artificial intelligence in employment relationships, it should be noted that as of February 2, 2025, the first restrictions on placing certain AI systems on the market and their use will apply. Specifically, Article 5 of the AI Act, which regulates prohibited practices, will come into effect. Among other things, it prohibits the use and marketing of AI systems intended for evaluating or inferring individuals' emotions in the workplace.

To ensure consistent, effective, and uniform application of the AI Act within the European Union, the European Commission published Guidelines on Prohibited AI Practices on February 4, 2025.⁹ These guidelines include a detailed explanation of all prohibited practices along with practical examples to help obligated parties ensure compliance with the AI Act (European Commission, 2025).

Articles 26 and 27 of the AI Act, which set out obligations for providers of high-risk AI systems and also bind employers, will begin to apply on August 2, 2025. This is also when the provisions on penalties for violations of the AI Act will take effect (Information Commissioner of the Republic of Slovenia, 2025).

Article 111 of the AI Act lays down rules for AI systems that have already been placed on the market or put into use:

- for AI systems that are components of large-scale IT systems and were placed on the market or put into use before February 2, 2027, it stipulates that these systems must comply with the requirements of the AI Act by December 31, 2030;
- for AI systems that are components of large-scale IT systems and were placed on the market or put into use before February 2, 2026, and whose design has not undergone substantial change since then, these systems must comply with the AI Act requirements by August 2, 2030;
- for general-purpose AI systems placed on the market before August 2, 2025, providers must take the necessary steps to fulfil the obligations under this regulation by August 2, 2027.

The provision in Article 111 of the AI Act means that employers who are already using AI in employment contexts will be required to gradually ensure their systems comply with the new regulation, with different deadlines depending on the type and use of the systems.

⁹ European Commission, Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act).

2.3.2 Directive on Improving Working Conditions in Platform Work

The Directive on Improving Working Conditions in Platform Work represents the first direct legal regulation of algorithmic management (Bagari, 2024: 1176). Its purpose is to improve working conditions and the protection of personal data in platform work. The minimum rights set out in the Directive apply to every person performing platform work in the EU who has an employment contract or is in an employment relationship.

The Directive also sets out rules to improve the protection of individuals in relation to the processing of their personal data, by ensuring measures for algorithmic management that are applied to people performing platform work in the EU, including those who do not have an employment contract or are not in an employment relationship (Article 1 of the Directive on Improving Working Conditions in Platform Work).

This Directive applies only to digital labour platforms that organise platform work (Article 1 of the Directive), which means that the provisions on algorithmic management do not apply to traditional employment relationships. Nevertheless, some provisions could be meaningfully applied to the use of artificial intelligence in traditional work environments as well, as I will explain in the discussion. These are found in Chapter III and relate to personal data protection, transparency, the obligation to include human oversight and review, occupational safety and health, and the right to information and consultation.

2.3.3 Directive on Transparent and Predictable Working Conditions

The purpose of the Directive on Transparent and Predictable Working Conditions is to improve working conditions by promoting more transparent and predictable employment while ensuring labour market flexibility (first paragraph of Article 1 of Directive (EU) 2019/1152).

Although this Directive does not directly address the use of artificial intelligence in employment relationships, some of its provisions may offer an important legal basis for addressing risks associated with the use of AI in the workplace (Bagari, 2023: 232).¹⁰

¹⁰ See for example Article 3, Article 4 and Article 13.

2.3.4 GDPR

GDPR sets out comprehensive rules for the protection of individuals with regard to the processing of personal data and the free movement of such data. It safeguards the fundamental rights and freedoms of individuals, particularly their right to the protection of personal data (first and second paragraphs of Article 1 of the GDPR). In the context of the topic under discussion, the following provisions are particularly relevant:

- Article 6 of the GDPR, which lays down the conditions for lawful processing of personal data,
- Article 9, which regulates the processing of special categories of data,
- Article 22, which governs automated individual decision-making, including profiling.

2.4 National Legal Sources

Within the framework of national legal sources, the following are particularly relevant to the issues discussed:

- The Constitution of the Republic of Slovenia (hereinafter: URS)¹¹ – Articles 14, 34, 35, 37 and 38,
- The Employment Relationships Act (hereinafter: ZDR-1)¹² – Articles 6, 22, 25, 27, 28, 36, 45, 47, 48, 77, 83, 87 and 170,
- The Occupational Health and Safety Act (hereinafter: ZVZD-1)¹³ – Articles 5, 7, 9, 11, 17, 18, 19, 37 and 38,

The Personal Data Protection Act (hereinafter: ZVOP-2)¹⁴ – Articles 2, 6 and 22.

3 Use of Artificial Intelligence in Different Stages of the Employment Relationship

3.1 Use of Artificial Intelligence in Recruitment

¹¹ Ustava Republike Slovenije, Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a in 92/21 – UZ62a.

¹² Zakon o delovnih razmerjih (ZDR-1), Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS, 81/19, 203/20 – ZIUPOPVDVE, 119/21 – ZČmIS-A, 202/21 – odl. US, 15/22, 54/22 – ZUPŠ-1, 114/23 in 136/23 – ZIUZDS.

¹³ Zakon o varnosti in zdravju pri delu (ZVZD-1), Uradni list RS, št. 43/11.

¹⁴ Zakon o varstvu osebnih podatkov (ZVOP-2), Uradni list RS, št. 163/22.

Artificial intelligence is already part of the recruitment process in many companies, and it is expected to play a key role in hiring in the coming years. HR professionals see the main advantage of AI primarily in its ability to quickly identify suitable candidates and significantly reduce the time spent reviewing applications (Fritts and Cabrera, 2021: 1-3).

Employers use algorithms either to assist in identifying suitable candidates or to completely entrust the selection process to the algorithm (Bagari, 2022: 44). AI can be used in various stages of the recruitment process (Fritts and Cabrera, 2021: 2-3):

1. Sourcing candidates.
2. Pre-selection and application screening.
3. Conducting interviews.
4. Selection and hiring decision.

One example of AI usage during the screening phase is FAMA, a software provider offering tools to thoroughly analyse candidates' online presence. With the help of AI, it assesses candidates' alignment with company values and detects potential risks, such as inappropriate behaviour or controversial opinions (Adams-Prassl, 2024: 190-191).

A 2019 study by *Raghavan et al.* examined 18 AI-based recruitment service providers in the screening phase. The providers used various methods to evaluate candidates, including personality tests, situational judgment tests, puzzle-solving tasks, and video interview analysis. For instance, HR departments can supply employee data to an AI vendor and request a report predicting expected sales performance. Algorithms then analyse a short video of a candidate to detect personality traits linked to success, such as »openness«, »excitement« and »warmth«. *Raghavan et al.* note that such video analyses are particularly common. In the U.S., these practices attracted the attention of lawmakers, leading to the 2019 enactment of the Illinois Artificial Intelligence Video Interview Act. This law requires employers to notify and obtain consent from candidates if their video interviews are to be analysed using AI tools (Raghavan et al., 2019: 6-12).

3.2 Performing Work Under the Instructions of AI

Performing work under the employer's instructions is one of the fundamental characteristics of the employment relationship, as defined in the first paragraph of

Article 4 of the Employment Relationships Act (ZDR-1). This definition necessarily places the employer in an active role, ensuring that workers receive clear work instructions.

Work is often assigned and organised through algorithms without human intervention (European Economic and Social Committee, 2017: 3.23). Instead of the employer, an algorithm may provide workers with instructions on what needs to be done, in what order and timeframe, manage shifts, assign tasks, and even determine rewards (Bagari, 2022: 44). A typical example is platform work, where tasks are assigned via smartphones and computers, directing workers to specific locations and instructing them on routes and time expectations. However, algorithmic task assignment is increasingly used in traditional work environments as well (Wood, 2021: 2-5).

Algorithmic management is common in retail, where systems allocate workers based on predicted customer demand. For instance, U.S. retailers Forever 21 and Century 21 implemented *Kronos*, a system that combines employee data with customer traffic and weather data to automatically schedule workers. In times of lower demand, the system notifies workers of temporary reductions in working hours, resulting in highly unstable working conditions (Wood, 2021: 4).

Advanced manufacturing plants also use algorithmic scheduling. *Briône* highlights the use of algorithmic management at the Siemens Congleton electronic components factory in the UK. They use *Preactor* software for real-time production scheduling, specifying daily production targets and detailed step-by-step instructions for workers (Briône, 2017: 17).

AI-based task assignment is not limited to physical labour and is increasingly present in office settings. For example, Canadian healthcare consulting firm Klick Health uses *Genome*, a tool that calculates average completion times for tasks and alerts team leads about project delays and unmet deadlines. The company also uses *RescueTime*, a tool designed to reduce distractions that might affect worker productivity (Wood, 2021: 5).

Fully autonomous systems assigning tasks to workers are still relatively rare. Even platforms like Deliveroo and Foodora maintain supervisory teams to monitor work and resolve issues. Completely removing human oversight would, in practice, reduce the effectiveness of algorithmic management (Wood, 2021: 5).

3.3 Performing Work Under the Supervision of AI

Another key characteristic of the employment relationship under Article 4 of ZDR-1 is performing work under the employer's supervision. This means the employer is responsible for organizing work, including monitoring compliance with work instructions.¹⁵

Employer supervision includes the right to monitor task execution and to sanction workers who do not perform assigned tasks or fail to follow instructions (Polajžar, 2023b: 244).

Algorithms can be used for such supervision, not only on online platforms but also in traditional workplaces. Adams-Prassl notes that platform work served as an »early lab« for developing algorithmic management tools, which are now used across various sectors (Adams-Prassl, 2024: 190). Employers use smart devices, cameras, and algorithms to collect and process large amounts of employee personal data (Polajžar, 2023b: 244).

A frequently discussed example is Humanyze, which developed badges worn by employees during working hours to collect workplace data. Though the company claims the badges do not record conversations, web activity, or personal behaviour outside the office, they include sensors that track movement, proximity to others, speaking patterns, and the frequency and duration of interactions. The collected data is analysed to uncover informal communication networks vital for understanding team and organisational dynamics. This eliminates the need for surveys or direct observation, providing quantitative metrics for previously unmeasurable success factors like collaboration and communication—key elements of productivity (Adams-Prassl, 2024: 191).

Amazon has also patented wristbands that track warehouse workers' locations and hand movements. When storing an item, workers follow standard procedures and scan the location. This allows Amazon's software to track item placement in real time and assign tasks based on the most efficient options considering worker location and movement paths. The wristband communicates these assignments and provides time estimates to complete each task. Amazon also uses algorithms for health and safety purposes, such as warning workers when they get too close to each other (Bagari, 2022: 45).

Aloisi and De Stefano list other employee surveillance systems. *Activtrack* alerts supervisors if a worker is distracted or browsing social media. *OccupEye* tracks absence duration. *TimeDoctor* and *Teramind* monitor all online tasks. *Interguard* builds

¹⁵ Sodba VIII Ips 392/2009, ECLI:SI:VSRS:2011:VIII.IPS.392.2009.

timelines of browsing history and bandwidth usage, notifying managers of suspicious activity. *HubStaff* and *Sneek* regularly take webcam snapshots of employees, about every five minutes (Aloisi and De Stefano, 2022).

3.4 Use of AI in Terminating Employment Relationships

An employment relationship can end in one of the legally defined ways provided in Article 77 of the Employment Relationships Act (ZDR-1).

AI can play an important or even decisive role in employment termination decisions. For example, on online platforms, workers with low customer ratings may be blocked from further work. Based on collected data (customer ratings, completed tasks, etc.), algorithms identify underperforming workers and apply sanctions (such as removal from the platform) (Bagari, 2022: 44-46; Polajžar, 2023b: 245).

Algorithmic management is also used in traditional workplaces for dismissal decisions. As discussed earlier, AI plays a significant role in employer oversight, but management goes beyond supervision. AI also enables decisions regarding disciplinary action. Data collected by AI systems can be combined with other online information (such as social media data) to support or initiate decisions about employee rights, disciplinary measures, and termination (Bagari, 2024: 1175).

Outside of platform work, algorithm-based dismissals are relatively rare. Some examples come from warehousing and logistics, where wearable devices monitor every aspect of worker activity. Supervisors then rely on this data instead of personal judgment when deciding on termination (Wood, 2021: 8).

A particularly well-known case involves Amazon. At an Amazon warehouse in Italy, algorithmic management was extensively used in the dismissal process. Employee performance data was used to generate individualised reports informing workers that they failed to meet targets, leading to dismissals. In some U.S. warehouses, the process was even stricter: dismissals based on low productivity—assessed entirely by an algorithm—occurred automatically, without human intervention. If a worker received six written warnings within 12 months, the system automatically issued a termination notice (Rosenblat and Stark, 2016: 3758-3766). According to Amazon, warehouse managers had no influence, control, or insight into how the algorithm worked (Wood, 2021: 9; Adams-Prassl, 2024: 192).

Gent observes that Amazon's algorithmic processes resemble those used by digital platforms like Deliveroo, Foodora, and Uber Eats, where access to work is automatically restricted due to poor performance. In Amazon warehouses, workers

receive automated notifications each morning confirming or cancelling their shifts based on the previous day's productivity metrics (Wood, 2021: 9).

4 Legal Risks and Existing Legal Framework

The legal risks associated with the use of AI in the workplace mainly relate to five key areas:

- prevention of discrimination;
- protection of workers' privacy;
- protection of workers' personal data;
- occupational health and safety;
- liability for damages.

Solutions for some areas can be found in existing legislation, but this legislation focuses only on certain aspects or risks posed by the use of artificial intelligence, without providing a comprehensive legal framework for algorithmic governance (Bagari, 2024: 1175).

4.1 Prohibition of Discrimination

One of the most common criticisms of the use of algorithms in hiring and firing, or algorithmic decision-making in general, is their potential bias, which can lead to discriminatory patterns (Fritts and Cabrera, 2021: 1). Although we initially think that subjectivity is excluded when using artificial intelligence in hiring and firing processes, there is a risk that algorithms reflect the biases of their programmers, whose main goal is generally to increase productivity and work performance (Bagari, 2022: 48). It is important to mention, as noted by the European Economic and Social Committee, that artificial intelligence develops in a homogeneous environment, mostly consisting of young white individuals, which means that (whether intentionally or unintentionally) cultural and gender differences are incorporated into artificial intelligence, especially since AI systems learn through training data. Therefore, it is crucial that these data are accurate, as well as high-quality, diverse, sufficiently detailed, and objective. In general, data are considered objective, but this is not always true. Data can be easily manipulated, and they can also be biased, reflecting cultural, gender, or other preferences or prejudices, and may even be incorrect (European Economic and Social Committee, 2017: 3.5).

Artificial intelligence models are usually designed to predict or make inferences, such as drawing conclusions about individuals who differ from those whose data were used to train the model (European Data Protection Board, 2024a: 13).

Barocas and Selbst have listed several examples where the use of artificial intelligence in the workplace can lead to discrimination. If employers wish to use AI, for example, to select the best candidates for employment, they must define the criteria for what makes »a good employee«. If the employer defines the criterion »rarely late« as a measure of a good employee, artificial intelligence will automatically rank lower those who live farther from the workplace compared to those who live closer (Barocas and Selbst, 2016: 678).

Slovenian legislation regarding labour relations already contains provisions prohibiting discrimination (Article 21 of the Charter, Article 10 of the Act on Artificial Intelligence, Article 6 of the ZDR-1, Article 2 of the ZVOP-2). Furthermore, more specific provisions ZDR-1 regarding hiring and firing procedures provide certain safeguards against discrimination.

The employer's contractual freedom in selecting candidates for employment is limited by the relevant provisions of ZDR-1:

- Article 6 of ZDR-1, which stipulates that the employer must provide equal treatment to job seekers regardless of nationality, race, or ethnic origin, national and social origin, gender, skin colour, health condition, disability, religion or belief, age, sexual orientation, family status, union membership, property status, or other personal circumstances;
- Article 9 of ZDR-1, which stipulates that when concluding an employment contract, both parties must comply with the provisions of ZDR-1 and other laws, ratified and published international agreements, other regulations, collective agreements, and the employer's general acts¹⁶;
- Article 22 of ZDR-1, which stipulates that an employee entering into an employment contract must meet the prescribed, collectively agreed, or employer-required conditions for performing work;
- Article 25 of ZDR-1, which stipulates that an employer hiring new employees must publicly announce the job vacancy;
- Article 27 of ZDR-1, which stipulates that an employer must not announce a job vacancy exclusively for men or women unless a particular gender is an

¹⁶ Despite the fact that the employer makes the final decision in the selection process, unsuccessful candidates must not be subjected to discrimination (VDSS sodba in sklep Pdp 896/2013, ECLI:SI:VDSS:2014:PDP.896.2013).

essential and determining condition for the job, and such a requirement is proportional and justified by a legitimate objective.

In the process of terminating an employment relationship, it is necessary to highlight the provision of the second paragraph of Article 83 of ZDR-1, which states that an employer may terminate an employment contract for a valid reason. This legal requirement is in line with Article 4 of ILO Convention No. 158 on the termination of employment at the initiative of the employer¹⁷, which states that an employee's employment cannot be terminated without a serious reason. Furthermore, Recommendation No. 166 to this Convention specifies that all parties (primarily employers) must, as much as possible, prevent or minimise dismissals.¹⁸ An employer may terminate the employment contract for reasons specified in the first paragraph of Article 110 of ZDR-1 (third paragraph of Article 83 of ZDR-1), and regularly for reasons specified in the first paragraph of Article 89 of ZDR-1. Additionally, according to the second paragraph of Article 87 of ZDR-1, the employer must provide written justification for the termination of the employment contract.¹⁹

Problems arise in enforcing rights, as workers are often left to prove discrimination on their own, which can limit the effectiveness of legal protection. The burden of proof that the prohibition of discrimination has not been violated, according to the sixth paragraph of Article 6 of ZDR-1, lies with the employer, but this burden arises only when the employee provides facts that justify the presumption of a violation of the prohibition of discrimination. This provision implies that the burden of proof regarding the existence of discrimination lies with the employee. The employee must not only claim unequal treatment but also show that the reason for the unequal treatment was one of the conditions listed in the law or another personal circumstance. The reversed burden of proof (as with proving the reason for termination or the legality of termination) does not mean that the employee is free from the burden of proof.²⁰

Discrimination in algorithmic management is difficult to detect, as certain requirements (e.g., conditions for the job) are usually not discriminatory in themselves. However, algorithms may draw additional information about candidates during the selection process, which could lead to discriminatory outcomes in the

¹⁷ International Labour Organization, Termination of Employment Convention No. 158.

¹⁸ E.g. VDSS Sodba Pdp 483/2020, ECLI:SI:VDSS:2021:PDP.483.2020.

¹⁹ E.g. VDSS Sodba Pdp 279/2021, ECLI:SI:VDSS:2021:PDP.279.2021.

²⁰ VDSS Sodba Pdp 611/2019, ECLI:SI:VDSS:2020:PDP.611.2019.

decision-making process regarding the selection of the appropriate candidate (Bagari, 2023: 228).

4.2 Protection of Workers' Personal Data

The collection and processing of personal data in employment relationships is not a new concept. However, in the past, the collection of personal data was limited by the accessibility of such data and the human capacity to process it (Bagari, 2023: 224). Artificial intelligence enables employers to gather previously unimaginable amounts of data about their employees from various sources (Adams-Prassl, 2024: 192).

4.2.1 Legal Grounds for the Processing of Workers' Personal Data

Article 48 of the Employment Relationship Act (ZDR-1) already states that workers' personal data can only be collected, processed, used, and shared with third parties if specified by this or another law or if necessary for the exercise of rights and obligations arising from the employment relationship or in connection with it. Personal data of workers may only be collected, processed, used, and shared with third parties by the employer or by an employee specifically authorised by the employer. Personal data of workers for which there is no longer a legal basis for collection must be immediately erased and no longer used.

Regarding the processing of personal data and the protection of workers from the risks associated with such processing, the General Data Protection Regulation (GDPR) and the Personal Data Protection Act (ZVOP-2) are also important, particularly the fundamental provision that personal data may only be processed when there is a legal basis for such processing (one of the conditions from Articles 6 or 9 of the GDPR).²¹

For the processing of personal data within the framework of employment relationships, three legal grounds are relevant (Polajžar, 2021b: 277-278):

- **execution of an employment contract** (Article 6(1)(b) GDPR), which is applicable, for instance, when the employer processes personal data

²¹ See Article 6 ZVOP-2 and Article 6 GDPR. The GDPR already clarifies in Recital 4 that the processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right – in accordance with the principle of proportionality, it must be considered in relation to its function in society and balanced against other fundamental rights.

necessary for payroll processing, but generally not for employee monitoring using ICT tools (internet, email, phone, etc.),

- **consent of the worker** (Article 6(1)(a) GDPR), which can be problematic due to the subordinate position of the worker, so it is important that consent is given voluntarily and reflects the genuine will of the worker,
- **legitimate interest of the employer, unless the interests or fundamental rights of the worker override the employer's interest** (Article 6(1)(f) GDPR), where such a legitimate interest could be, for example, the employer's monitoring of employees to protect their legal, economic, and other interests. The employer's interest must be lawful (according to national law and EU law), specific, and genuine (not merely speculative).

There is no hierarchy among the different legal grounds in Article 6(1) of the GDPR (European Data Protection Board, 2024: 19). The selection of the appropriate legal ground for each processing activity is the responsibility of the data controller (in this case, the employer), who must consider the specific circumstances and the purpose of the processing. Given that there is no specific regulation governing the use of artificial intelligence in employment relationships, its use can only be justified if a legal basis is demonstrated according to the first paragraph of Article 6 of the GDPR (Information Commissioner of the Republic of Slovenia, Opinion of the Information Commissioner of the Republic of Slovenia No. 07121-1/20250230, 24 February 2025).

The Information Commissioner also highlighted the principle of data minimisation, which states that only as much personal data of workers should be processed as is strictly necessary for the specific purpose (Information Commissioner of the Republic of Slovenia, Opinion of the Information Commissioner of the Republic of Slovenia No. 07121-1/20250230, 24 February 2025). This principle stems from the first paragraph of Article 5 of the GDPR, which sets out principles for personal data processing. In point (c), it specifies that personal data should be limited to what is necessary for the purposes for which they are processed. The European Data Protection Board stated that assessing necessity involves evaluating two questions: (1) whether processing personal data will achieve the purpose, and (2) whether there is a less intrusive way to achieve that purpose. The scope of personal data used by an AI model should be assessed against less intrusive alternatives that could achieve the same legal interest. If the goal can be achieved without processing personal data

using AI, the processing of personal data is not considered necessary (European Data Protection Board, 2024a: 22-23).

The European Data Protection Board further emphasises that when processing the personal data of workers, their subordinate position in the employment relationship must also be taken into account. Due to the specifics of the relationship between the worker and the employer, the assessment of the scope of personal data processing in the employment relationship will differ from, for example, the relationship between a service provider and a customer (European Data Protection Board, 2024c: 15).

Carter, however, explains that some principles, such as purpose limitation and data minimisation, are difficult to reconcile with AI-based monitoring, which relies on large data sets and the reuse of data for new purposes (Carter, 2024: 5-6).

4.2.2 Right to Information for Workers

The GDPR also grants the right to information to workers. One of the primary objectives of the GDPR is to give individuals – in this case, workers – control over their personal data. This goal cannot be achieved if workers are not informed that their personal data is being processed by their employers and do not have access to this data. Workers must be aware of the risks, rules, protection, and rights related to algorithmic management, and how they can exercise these rights concerning such processing. The right to information is a prerequisite for balancing the asymmetry in the employment relationship and for exercising other data rights, including rectification, erasure, and data portability. The GDPR in Articles 12, 13, and 14 specifies what, how, and when workers must be informed about the processing of their personal data. This requirement for transparency has three key components (Abraha, 2023: 175-176):

1. the content of the information,
2. the time frame within which the information must be provided,
3. the manner in which the information must be provided to the worker.

The European Data Protection Board has clarified that employers must, regardless of the legal basis for transferring personal data within the group, ensure that they meet their obligation to provide workers with the required information about processing activities affecting their personal data, in accordance with Articles 12, 13, and 14 of the GDPR. Therefore, employees must be provided with appropriate

information about the processing of their personal data within the group, including the legal basis for such processing (European Data Protection Board, 2024c: 34).

4.2.3 Right of Access

In addition to the right to be informed, the GDPR also establishes the right of access, which allows workers to exercise control over their data. Article 15(1)(h) specifically applies to the context of automated decision-making and provides workers with the right to understand how algorithmic management is used. Unlike the obligation to inform, which requires that information be provided at a certain time and in an appropriate manner, Article 15 grants a right of access that applies only when the worker explicitly requests it. Workers may exercise this right at any time (Abraha, 2023: 177).

Abraha highlights three main shortcomings of this article:

- the ambiguity regarding how much information employers must disclose about the functioning of algorithms,
- the fact that employers may deny access to data in order to protect trade secrets or the rights of others,

the limited scope of application, as the right of access applies only to fully automated decisions with significant effects (Abraha, 2023: 177–180).

4.2.4 Prohibition of Automated Decision-Making

As previously mentioned, the most important safeguard against the risks of algorithmic management is Article 22 of the GDPR, which states in its first paragraph that the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. In the context of algorithmic hiring, this could be understood either as an enforceable right of a candidate not to be subject to automated decision-making, or as a general prohibition for employers to use such automated decision-making—making the chosen interpretation key to determining employers' ability to use automated hiring systems and to ensure protection for candidates against such decisions (Parviainen, 2022: 229).

The first interpretation views Article 22(1) as a right of the candidate not to be subjected to automated decisions. This means that employers may generally use algorithmic hiring systems but must provide an opt-out for candidates who assert

this right. If none of the exceptions under Article 22(2) apply, human decision-makers must evaluate those candidates. The second interpretation understands Article 22(1) as a general prohibition on automated decision-making in employment unless the conditions under Article 22(2) are met and the safeguards from Article 22(3) are implemented. This interpretation provides a higher level of protection for candidates and is more consistent with the GDPR's goals, as it prevents potential negative impacts of automated decisions. The debate on the correct interpretation is still unresolved, as the Court of Justice of the EU has not yet provided a clear position. However, the European Commission has endorsed the second interpretation, stating that processing based on Article 22(1) is generally not permitted (European Commission, 2017: 20). Parviainen also supports the second interpretation as the safer one, as it offers better protection for candidates and clearer legal frameworks for employers (Parviainen, 2022: 229–234).

Exceptions to the prohibition of automated decision-making are outlined in Article 22(2) of the GDPR, which permits such decisions if:

- they are necessary for the conclusion or performance of a contract²²,
- they are authorised by Union or Member State law²³ or
- they are based on the explicit consent of the data subject.

In its guidelines on automated decision-making, the European Commission illustrated the necessity exception from Article 22(2) with an example of a company receiving tens of thousands of applications for a job posting. In such a case, the Commission considers automated decision-making potentially necessary to compile a shortlist of candidates for the purpose of concluding a contract with an individual (European Commission, 2017: 23).

Regarding the exception based on the candidate's or employee's consent, the main issue is whether candidates are truly in a position to give freely given consent. Recital 43 of the GDPR states that consent is not valid if there is a clear imbalance between the data subject and the controller. Such an imbalance is clearly present between

²² These exceptions are not further elaborated upon in either the preparatory materials or the preamble of the GDPR, leaving it unclear how they should be interpreted and whether, in certain circumstances, automated decision-making is truly necessary for the conclusion of an employment contract. According to Sartor and Lagioia, automated decision-making could be necessary in cases where there is an overwhelming number of job applications that exceed the employer's processing capacity—for example, in the case of a start-up company that needs to hire 500 workers for a logistics center within one month and expects thousands of applications. In such a scenario, manually reviewing all applications would be nearly impossible, making automated preliminary filtering potentially justified. However, other parts of the process, such as interviews, could still be conducted without automated decision-making (Sartor and Lagioia, 2020: 59–60).

²³ According to *Parviainen* there is no legislation at the EU level that allows for automated decision-making in employment.

employers and candidates, especially in mass hiring for lower-level positions. Another concern is the question of informed consent. Candidates must be transparently informed of all essential aspects of automated decision-making, including its consequences. However, due to the technical complexity of algorithms, candidates may not fully understand what they are consenting to, even when informed (Parviainen, 2022: 242–245).

4.2.5 Other Legal Mechanisms

In addition to the core principles, several other mechanisms regulated by the GDPR are also important from the perspective of employee protection. These include the data protection impact assessment, which must be conducted before introducing surveillance technologies into the work environment (Article 35 GDPR). The European Data Protection Board stresses that conducting a data protection impact assessment is especially crucial in cases where data processing through AI systems poses a high risk to individuals' rights, which undoubtedly applies in the context of processing employees' personal data (European Data Protection Board, 2024a: 10). It is also important to mention the employer's obligation, as the data controller, to consult the supervisory authority if the results of the assessment indicate that sufficient risk mitigation measures cannot be implemented (Article 36 GDPR), the obligation to appoint a data protection officer (Article 39 GDPR) and the right of employees to lodge a direct complaint with the Information Commissioner if they believe that the processing of their data violates the GDPR (Article 77 GDPR) (Polajžar, 2021b: 279-281).

An important feature of GDPR are also the extremely high administrative fines that the GDPR prescribes for violations of the fundamental rules on personal data processing, which in themselves have a deterrent effect on potential infringers (Polajžar, 2023c: 34).

More broadly, both the GDPR and the Slovenian Data Protection Act (ZVOP-2) establish rather flexible principles and criteria for processing employees' personal data, which complicates their consistent application in employment relationships. As a result, significant gaps remain in the legal protection of employees' personal data. Some authors have therefore pointed out the inadequacy of the GDPR as a general instrument for data protection in the field of labour (Bagari, 2024: 1175–1176; Abraha, 2023: 184–187).

4.3 Protection of Workers' Privacy

Respect for privacy in the use of artificial intelligence systems is undoubtedly one of the issues that justifiably raises concerns. AI systems can monitor and control workers in increasingly sophisticated ways, potentially infringing on their right to privacy (European Economic and Social Committee, 2017: 3.13, 3.23).

The use of advanced algorithms creates new opportunities for employers to exercise (in some cases excessive) control over employees. Algorithms can, for instance, track the location of workers at the workplace, monitor whether they are moving or stationary, speaking or silent, and even record the duration of their personal interactions (Bagari, 2024: 1174).

All this presents a significant risk to workers' fundamental rights. In relation to the use of AI for surveillance, the intrusion into workers' privacy is particularly alarming. Employers are not entitled to unlimited surveillance, as they are bound by the employee's right to privacy.²⁴ It is therefore essential that labour law protection limits employer surveillance to ensure that the right to monitor does not endanger fundamental human rights (De Stefano, 2018: 13).

Employers may only restrict workers' right to privacy under certain conditions, some of which are precisely defined by law for specific types of surveillance (Brajnik and Langeršek, 2019: 19). For those types of surveillance that interfere with privacy rights and are not specifically regulated by law, it is crucial that employers adhere to existing legal standards. The right to privacy is protected as a fundamental human right under Article 35 of the Constitution of the Republic of Slovenia. Additionally, the Employment Relationships Act (ZDR-1) in Article 46 stipulates that employers must respect and protect the personality and privacy of workers.

Before implementing a specific technology, the data controller (employer) must assess the legitimacy and justification of the purpose for which the technology is to be introduced. Furthermore, all procedures and measures must be carried out in accordance with the principle of proportionality. This means evaluating whether the same purpose could be adequately achieved by less intrusive measures and always choosing the option that interferes least with the worker's privacy while pursuing a legitimate aim. Measures should not be adopted if comparable outcomes can be achieved with milder alternatives. If a measure is deemed necessary, appropriate, and effective at the level of a particular organisation (in this case, the employer), it must

²⁴ VDSS sodba Pdp 264/2005, ECLI:SI:VDSS:2006:VDS.PDP.264.2005.

be carried out in a way that minimises intrusion into the individual's privacy (Information Commissioner of the Republic of Slovenia, Opinion of the Information Commissioner of the Republic of Slovenia No. 07121-1/20250230 of 24 February 2025).

4.4 Occupational Safety and Health

The use of AI in the workplace also raises issues regarding the occupational safety and health of workers subject to these systems (Cafaliello, 2023: 193).

One of the main concerns linked to AI deployment is its impact on workers' psychosocial well-being. Algorithms used for monitoring and optimising work processes often lead to higher levels of stress and uncertainty, especially when AI replaces human oversight and decision-making. Employees may be constantly monitored and have their performance analysed by algorithms, which can create a sense of lost control over their work environment (Nazareno and Shiff, 2021: 3).

Main risks include:

- increased pressure on workers, as AI systems may drive them toward higher productivity, potentially causing stress, exhaustion, and a greater risk of workplace accidents,
- reduced control over their work, leading to stress due to excessive micromanagement,
- AI systems monitoring employee performance may result in excessive competition and a decrease in teamwork,
- emphasis on productivity may reduce communication among workers, leading to isolation and a negative impact on mental health,
- invasive monitoring and the collection of sensitive personal data may generate anxiety and mistrust toward employers due to fear of data misuse (European Agency for Safety and Health at Work, 2025: 2).

Tomprou and Lee studied the effects of AI use in the workplace on the relationship between employees and employers (Tomprou and Lee, 2022). They found that employees reported lower trust in their working relationships when they noticed that decision-making authority had shifted from humans to algorithmic systems. This reduction in trust can increase psychosocial risks.

The use of AI can lead to psychological issues such as anxiety, depression, stress, and burnout. Workers often feel under constant pressure to meet targets set by AI systems, without always knowing how those decisions are made. This may create

feelings of uncertainty, as employees may not understand why certain goals were set, how the criteria affected their work, or whether they can influence any changes. Additionally, when AI monitors worker productivity and efficiency, it can lead to a sense of dehumanisation. Employees may feel like mere numbers or data points rather than individuals with unique needs, experiences, and emotions (Nazareno and Shiff, 2021: 4–5).

Article 19 of the ZVZD-1 requires employers to inform workers about the introduction of new technologies and tools. However, experts already question the effectiveness of this provision and whether it is actually implemented in practice. The duty to inform and consult on decisions that may cause significant changes to work organisation or contractual relationships also arises from Directive 2002/14/EC, which establishes a general framework for informing and consulting workers in the European Community. However, the implementation of this right depends in part on how domestic legislation and courts apply the directive (Bagari, 2024: 1176).

The provisions on occupational health and safety are also included in the Framework Directive on the introduction of measures to encourage improvements in the safety and health of workers at work²⁵. Its aim is to promote measures that improve worker safety and health (Article 1). It sets out employer obligations regarding worker safety and health (Articles 5–12) and employee obligations (Article 13). Although the directive also applies to the use of AI in the workplace, it does not address the specific characteristics of AI in a way that would effectively mitigate its associated risks (Cafaliello et al., 2023: 200).

A key shortcoming of existing regulations on the safety of information systems is their reliance on the »safety by design« approach. This method focuses on one phase of the technology lifecycle – the design phase – and assumes that technology can be made safe through decisions made during its invention, design, and early testing. This approach is used, for example, in the automotive and medical industries. However, it is inadequate for AI because the safety of AI depends not only on how it is designed but also (and perhaps more importantly) on how it is used and the decisions it makes. This is especially important for systems that »learn« — those whose outputs change in response to input data without human intervention, such as AI systems. Therefore, it is necessary to establish minimum standards and

²⁵ Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work.

procedural requirements concerning the risks AI poses to workplace safety and health, not just during design but also during implementation and all subsequent stages of use (Cefaliello et al., 2023: 194).

There are also considerable gaps in the current legal framework regarding AI's impact on worker health. Risks such as discrimination and privacy violations fall under the category of psychosocial risks. Although these are psychosocial, their impact on workers is material, as workers depend on their income for survival. For these reasons, Cefaliello and others argue that it is essential to adopt specific legislation addressing occupational safety and health in the context of AI use in the workplace (Cafaliello et al., 2023: 200).

4.5 Liability and Labour Law Responsibility for the Use of Artificial Intelligence in the Workplace

The use of AI in the workplace also raises questions regarding liability — both compensation and employment law liability — for its use.

There are two types of liability:

- employer's liability for damages and
- employer's employment law liability.

4.5.1 Employer's Liability for Damages

Article 179 of the Employment Relationships Act (ZDR-1) governs an employer's liability for damages to an employee. The first paragraph states that if an employee suffers damage at or in connection with work, the employer must compensate the employee under general civil law principles. The second paragraph specifies that this liability also applies to damage caused by the employer through violations of employment rights.

Regarding violations of anti-discrimination and anti-bullying rules in the workplace, Article 8 of ZDR-1 further provides that in cases of such violations, the employer is liable for damages under general civil law. Non-pecuniary damage includes mental distress due to unequal treatment or discriminatory conduct by the employer or due to failure to ensure protection against sexual or other harassment or bullying in the workplace under Article 47 of ZDR-1. The amount of compensation must be effective, proportionate to the harm suffered, and serve as a deterrent against repeat violations by the employer.

This raises the question: who is liable for damages suffered by a worker due to fundamental rights violations caused by AI (as discussed in previous sections) — the employer, or can the liability be shifted to the AI developer or provider (Adams-Prassl, 2024: 195)?

4.5.2 Employer's Employment Law Liability

A key aspect is the employer's employment law responsibility toward the employee. The use of AI may breach fundamental obligations, including the duty to ensure safe working conditions (Article 45 of ZDR-1), the obligation to respect and protect the worker's personality and privacy (Article 46 of ZDR-1), and the protection of personal data (Article 48 of ZDR-1). Violations of workplace safety obligations or the prohibition of discrimination are legitimate grounds for an employee to terminate the employment contract extraordinarily (first paragraph of Article 111 of ZDR-1).

5 Discussion on the Possibilities of Additional Protection for Workers Against Risks Associated with the Use of Artificial Intelligence in the Workplace

5.1 Employer's Duty to Explain and the Use of the Reversed Burden of Proof in Cases of Discrimination

Discrimination is one of the major concerns related to the use of algorithms in the workplace. The greatest issue arises in the enforcement of rights, as the burden of proof regarding the existence of discrimination lies with the worker. However, proving discrimination in algorithmic decision-making is extremely difficult.

The burden of proof that no discrimination occurred lies with the employer (sixth paragraph of Article 6 of the Employment Relationship Act – ZDR-1), yet this only applies once the worker provides facts that justify a presumption of discrimination.²⁶ Thus, the burden of assertion regarding the existence of discrimination is on the worker. To successfully claim compensation under Article 8 of ZDR-1, the worker must allege and demonstrate unlawful conduct by the employer, material and/or non-material damage, and a causal link, while the employer's fault is presumed

²⁶ VDSS Sodba Pdp 611/2019, ECLI:SI:VDSS:2020:PDP.611.2019.

(Mežnar, 2024: 86). Due to the opacity of algorithms, this burden of assertion is very difficult to meet in practice. On the other hand, the employer, by complying with legal documentation requirements, is in a better position to prove that the use of an AI system did not breach the prohibition of discrimination.

Primarily, in cases where employers use algorithms in hiring and dismissal processes, there should be a duty to explain. Upon request, the employer should be obliged to explain to the worker or candidate the criteria on which the decision was based, which criterion was decisive, and how the candidate or worker was evaluated. This would allow workers to obtain enough information to assert their rights in court. If the employer fails to fulfil this duty, the burden of proof and assertion that the automated decision was non-discriminatory and based on objective criteria should lie with the employer.

Aloisi and De Stefano propose a similar solution, suggesting that the burden of proof should be shifted to AI system providers used in work environments. These providers would need to demonstrate the »harmlessness« of such systems before their deployment, involving affected workers and their representatives in the discussion. Failure to do so would render such systems automatically unlawful (Aloisi & De Stefano, 2023: 305).

5.2 Adoption of Specific Regulations Governing the Prohibition of Discrimination Related to AI Use in the Workplace

The prohibition of discrimination is protected by binding legal sources at both the international and national levels. With regard to AI-related discrimination, the fundamental principles are quite clear – discrimination is and should not be acceptable in our society.

However, *Zuiderveen* warns that current legislation contains technologically neutral legal provisions based on broad principles, which are hard to apply in specific cases.²⁷ Therefore, he proposes adopting specific regulations or, alternatively, guidelines that supplement existing regulations and are tailored to the use of AI in the workplace, which would need to be regularly updated in line with technological developments (Zuiderveen, 2018: 33–38).

²⁷ E.g. GDPR.

Such specific regulations or guidelines should explicitly address the employer's duty to explain and the use of reversed burden of proof, as outlined in the previous section.

5.3 Protection of Personal Data

In areas such as data protection, privacy, and occupational health and safety, solutions for further protecting workers could be found in the Platform Work Directive, even though it currently applies only to digital labour platforms. Abraha suggests that the EU should either adopt a specific directive addressing algorithmic management risks or extend the scope of the Platform Work Directive (Abraha, 2023: 187). *Aloisi and De Stefano* also emphasise the need for a comprehensive EU legal framework regulating AI in the workplace, including a dedicated legislative instrument (Aloisi & De Stefano, 2022: 305–307).

Polajžar outssets that the Court of Justice of the European Union also plays an important role in the protection of worker's rights in this area through its interpretation of EU law. CJEU ensures that GDPR (secondary EU law) is compatible with primary EU law (e.g. Charter of Fundamental Rights) (Polajžar, 2023c: 33).

Carter, however, notes that the provisions of the GDPR alone are insufficient for the protection of personal data and privacy. He advocates for considering a broader rights framework under Articles 7 and 8 of the EU Charter of Fundamental Rights and Article 8 of the ECHR, recognising that privacy must be dynamically implemented. This is especially important given the rapidly advancing and increasingly invasive nature of AI surveillance technologies. Thus, a holistic, innovative, and adaptive approach to privacy is necessary (Carter, 2024: 13–14).

Similar to platform work, employers in traditional workplaces should be prohibited from processing specific types of workers' personal data, such as emotional or psychological states, private communications, personal data collected outside working hours, predictions regarding the exercise of fundamental rights, and sensitive data (ethnicity, political beliefs, etc.). Biometric identification methods should also be fully banned (Article 7 of the Platform Work Directive).

Employers using algorithmic management should be required to conduct data protection impact assessments (DPIAs), as such processing can pose significant risks to workers' rights. DPIAs should include an assessment of potential discriminatory effects and impacts on working conditions (Article 8 of the Platform Work

Directive), involve workers and their representatives (e.g. unions, works councils), and ensure all employees have access to these assessments.²⁸ Furthermore, employers should regularly inform workers, their representatives, and relevant authorities about the use and functioning of automated systems (Articles 8 and 9 of the Platform Work Directive).²⁹

Abraha also stresses the importance of involving workers' representatives, noting that collective bargaining is the most effective tool for protecting against rapid technological changes in algorithmic management (Abraha, 2023: 188–189).

There should also be a mandatory provision ensuring human oversight of automated monitoring and decision-making systems. Supervisors must have the necessary competence and authority to override automated decisions. Crucially, decisions regarding employment relationships – such as contract termination – must be made by a human (Article 10 of the Platform Work Directive).

In exceptional cases, automated decision-making may be allowed, such as when there is a large volume of job applications. In such cases, automation could be used for creating a shortlist of potential candidates. However, workers should always have the right to an explanation of the decision and be able to request a review. Employers should be obligated to provide an explanation or amend the decision if it violates the candidate's or employee's rights (Article 11 of the Platform Work Directive).

The European Data Protection Board (EDPB) has also emphasized the need for a national supervisory authority to oversee data protection in the context of AI, which should cooperate with national data protection authorities (EDPB, 2024b: 2). Moreover, due to the multilayered nature of data protection regulations, the EDPB calls for cooperation among all stakeholders addressing data protection and AI issues (EDPB, 2024b: 4–5).

5.4 Protection of Workers' Privacy

With regard to broader privacy protection for workers, further protective measures could be drawn from the Platform Work Directive.

²⁸ Under the current legal framework, neither trade unions nor workers' councils have specific competences regarding the processing of employees' personal data. Only the general regulation on the adoption of internal acts by the employer, as set out in Article 10 of the Employment Relationships Act (ZDR-1), indicates that the employer must submit a draft internal act to the trade union for its opinion prior to its adoption. If the union provides an opinion, the employer is obliged to consider it and respond to it accordingly (Senčur Peček and Polajžar, 2023: 476).

²⁹ For more on collective rights and the protection of privacy in the workspace see Polajžar, 2024b: 31–47.

As with platform work, in traditional workplaces where algorithmic management is used to monitor employees, employers should be prohibited from processing data related to workers' private communication (Article 7 of the Platform Work Directive).

Where there are justified reasons for such intrusion, human oversight should be guaranteed, and those responsible must have adequate competencies. Workers and their representatives must be informed of any (automated) intrusion into their privacy, with clear information on the reasons, scope, duration, and their right to object if they believe it is disproportionate. The employer must provide a well-founded decision when addressing such objections (Articles 10 and 11 of the Platform Work Directive).³⁰

5.5 Occupational Safety and Health

In terms of occupational health and safety, it is essential to ensure that AI is not used in ways that cause psychosocial strain. Some solutions can be found in the Platform Work Directive. Employers should assess the risks related to automated systems and take preventive measures to protect employees. Systems that exert undue pressure or endanger the physical or mental health of workers should not be used (Article 12 of the Platform Work Directive).

The use of AI should be included in the risk assessment (Article 17 of the Health and Safety at Work Act – ZVZD-1), and the safety declaration with the risk assessment should be published and made available to employees whenever it is updated (Article 18 of ZVZD-1). This obligation must be enforced in practice, as employers are unlikely to independently assess the impact of AI on occupational safety and health, especially its psychosocial effects (Bagari, 2023: 230).

In addition, employers are required under Article 37 of ZVZD-1 to inform workers about workplace hazards, safety measures, and procedures, including those related to the use of AI (Bagari, 2023: 229).

5.6 The Role of Workers' Representatives in Introducing AI into the Workplace

³⁰ See also Polajžar, 2024a: 195-212.

Labour law increasingly relies on collective rights and the role of workers' representatives to protect employees from AI-related risks (Polajžar, 2023b: 246). Workers' representatives can exercise their role through the employer's general act adoption procedure under Article 10 of ZDR-1, collective bargaining agreements, and participation in management under the Worker Participation in Management Act (hereinafter: ZSDU)³¹ and Articles 45–48 of ZVZD-1.

Directive 2002/14/EC on establishing a general framework for informing and consulting employees in the EU³² emphasises that timely information and consultation are key to successful company restructuring and adaptation to new conditions brought by globalisation, especially the development of new work organisation forms. Article 4 of the Directive specifies informing workers about the recent and likely development of the company's activities and economic situation, and informing and consulting about decisions that may cause substantial changes in work organization or contractual relationships (Bagari, 2022: 50). The European Economic and Social Committee has also called for full involvement and information sharing with workers and social partners in decisions about AI use in the workplace (EESC, 2021: 4.17).

The importance of involving workers' representatives is also highlighted in several EU legal sources, including Article 27 of the Charter of Fundamental Rights, Article 26 of the AI Act, Articles 13 and 14 of the Platform Work Directive³³, and Article 4 of the Directive on Transparent and Predictable Working Conditions.

Therefore, active involvement of workers' representatives in the introduction of AI in the workplace is crucial. In addition, it is essential to establish clear rules on the use and functioning of algorithms to ensure greater transparency and protection of workers' rights (Bagari, 2023: 230). Polajžar proposed that the legislator grant stronger powers to workers' representatives through the ZSDU, and that workers' councils, being closely familiar with company conditions, should play a key role in AI decision-making. He also suggested amending Articles 61 and/or 65 of ZSDU to allow the workers' council to obtain an expert opinion when assessing the impact of AI deployment in the company, with such opinion being treated as a necessary cost for the council's functioning (Polajžar, 2021a: 4). In addition, he proposed that

³¹ Zakon o sodelovanju delavcev pri upravljanju (ZSDU), Uradni list RS, št. 42/07 – uradno prečiščeno besedilo in 45/08 – Zarbit.

³² Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community - Joint declaration of the European Parliament, the Council and the Commission on employee representation.

³³ For more on the collective rights of platform workers see Polajžar, 2024a: 195-212 in Polajžar, 2023a: 277-306.

Articles 61 and/or 65 of the Worker Participation in Management Act (ZSDU) could be amended to allow the works council to obtain an expert opinion when it is required to assess the effects of the implementation and use of artificial intelligence in the company as part of its duties. Such an expert opinion would be considered a necessary expense for the functioning of the works council, which, in accordance with Article 65 of the ZSDU, must be covered by the employer. This would facilitate the works council's access to expert opinions (Polajžar, 2023b: 251).

Wood also believes that a collective approach to regulating algorithmic management is a key mechanism for protecting workers' rights and ensuring fairness in the use of artificial intelligence in the workplace. It is important that workers, through their representatives, participate in the implementation of AI systems. Such an approach reduces risks, as decisions are also subject to collective bargaining, which is becoming one of the key challenges of modern social dialogue. This dialogue no longer addresses only wages and working hours, but also the use of artificial intelligence in work processes (Wood, 2021: 14).

5.7 Regulation in Employers' General Acts and Collective Agreements

One of the possible ways to provide additional protection to workers regarding the use of AI in the workplace would be to include this topic in the employer's general acts. Article 10 of the Employment Relationships Act (ZDR-1) allows an employer to adopt a general act that regulates work organisation or defines obligations that employees must be aware of to fulfil their contractual and other duties.

Experts emphasise the importance of adopting general acts to define the limits of permissible surveillance and the use of ICT work equipment in the workplace. They point out that all forms of monitoring work tools must be regulated in advance through general acts, which must transparently describe how surveillance is carried out, its duration, etc. This is particularly important for respecting workers' right to privacy. However, the mere adoption of a general act by the employer does not make every form of surveillance permissible, as the employer must still respect constitutional and legal limitations when conducting surveillance (Polajžar, 2021b: 285–286).

Regarding this issue, Polajžar notes that general acts represent a problematic unilateral intrusion into workers' right to privacy, as these acts not only specify work obligations but also prescribe procedures through which the employer intrudes into workers' privacy. Therefore, it would be more appropriate to regulate such

intrusions through collective agreements. There are no obstacles to adopting collective agreements governing workers' rights concerning the use of AI in the workplace, although both workers' and employers' representatives must voluntarily agree to conclude such agreements (Polajžar, 2021b: 286).

5.8 Worker Education and Training

Article 170 of ZDR-1 establishes the right (and duty) of employees to education, training, and upskilling in accordance with the needs of the work process, with the aim of maintaining or expanding the ability to perform work under the employment contract, maintaining employment, and increasing employability.

Given the innovations and specific characteristics that the introduction of AI brings to certain or all jobs, the employer not only has the option but an explicit obligation to ensure adequate training for employees who will use AI in their work. Employees must be trained to work with new technologies and supported in understanding AI and its impact on employment relationships (Bagari, 2023: 230).

6 Conclusion

This article has explored the question of whether the use of artificial intelligence in employment relationships calls for the adoption of additional, specific legal regulations to ensure better protection of workers. It has demonstrated that AI can influence every phase of the employment relationship — from recruitment, through day-to-day task management, to performance evaluation and even employment termination — raising new and complex legal challenges that the existing labour framework does not comprehensively address.

Some mechanisms that address certain risks related to the use of AI in employment relationships can already be found within the existing legal framework, both at the EU level (such as the EU Charter of Fundamental Rights, the AI Act, the Directive on Improving Working Conditions in Platform Work, the Directive on Transparent and Predictable Working Conditions in the EU, and the GDPR) and at the national level (including the Slovenian Constitution, the Employment Relationships Act – ZDR-1, the Health and Safety at Work Act – ZVZD-1, and the Personal Data Protection Act – ZVOP-2). However, none of these legal sources provide a comprehensive regulation of the use of AI in the workplace.

To ensure that the core function of labour law — the protection of workers — is upheld, several areas require urgent attention. These include the employer's duty to explain algorithmic decisions, the right of workers to access and contest automated decisions, the obligation of human oversight in crucial employment decisions and stronger involvement of worker representatives in the implementation of AI systems. The role of regulatory bodies and the importance of education and awareness-raising among both employers and employees have also been emphasised as necessary elements of a preventive strategy.

This article suggests that certain measures must be adopted to ensure adequate worker protection. However, it will ultimately depend on each individual country whether these measures are incorporated into labour legislation or addressed within another legal framework. Regardless of the approach, the key goal must remain the same: to ensure the core function of labour law—protecting those who need protection. It is a simple formula, but unfortunately, one that is extremely difficult to implement and achieve in practice (Tičar, 2017: 253).

References

- Abraha, H. (2023) Regulating algorithmic employment decisions through data protection law. In: *European Labour Law Journal* 14(2), p. 175-187.
- Adams-Prassl, J. (2024) Law and (R)evolution at Work. In: Acceto, M., Škrubelj K. and Weiler J. H. H., (ed.). *Law and Revolution: Past Experiences, Future Challenges* (Routledge), p. 184-195.
- Adams-Prassl J. (2019) What If Your Boss Was an Algorithm? In: *Comparative Labor Law&Policy Journal* 41, p. 4-30.
- Aloisi, A., De Stefano, V. (2023) Between risk mitigation and labour rights enforcement: Assessing the transatlantic race to govern AI-driven decision-making through a comparative lens. In: *European Labour Law Journal* 14 (2), p. 305-307.
- Aloisi, A., De Stefano, V. (2022) *Your Boss Is an Algorithm. Artificial Intelligence, Platform Work and Labour*, Hart Publishing (Hart publishing, 2022).
- Bagari, S. (2023) Tveganja pri uvajanju umetne inteligence v delovna razmerja in možne pravne rešitve. In: *Delavci in delodajalci* 23 (2/3), p. 224-237.
- Bagari, S. (2022) Uporaba algoritmov na področju delovnih razmerij in socialne varnosti. In: *Delavci in delodajalci* 22 (1), p. 43-52.
- Bagari, S. (2024) Vpliv umetne inteligence na delovna razmerja. In: *Podjetje in delo* 50, p. 1168-1179.
- Barocas, S. and Selbst, A. D. (2016) Big Data's Disparate Impact. In: *104 California Law Review* 671, p. 678.
- Brionne P. (2017) *Mind Over Machines: New technology and employment relations*. Research Paper 02/17, p. 17.

- Cafaliello, A. et al. (2023) Making algorithmic management safe and healthy for workers: Addressing psychosocial risks in new legal provisions. In: *European Labour Law Journal* 14 (2), p. 193-209.
- Carter, C. (2024) AI surveillance: Reclaiming privacy through informational control. In: *European Labour Law Journal* 16 (2), p. 5-14.
- De Stefano, V. (2018) Negotiating the algorithm: Automation, artificial intelligence and labour protection. In: *Employment, Working Paper 246*, International Labour Office, p. 13.
- European Agency for Safety and Health at Work, Towards AI-based and algorithmic worker management systems for more productive, safer and healthier workplaces. In: *Safe and healthy work in the digital age 2023-2025*, 2025, p. 2.
- European Data Protection Board, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 2024a, <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en> (available on March 18 2025).
- European Data Protection Board, Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework, 2024b, <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en> (available on March 19 2025).
- European Data Protection Board, Opinion 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, 2024c, <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en> (available on March 18 2025).
- Eurobarometer, Artificial Intelligence and the future of work, 2025, <<https://europa.eu/eurobarometer/surveys/detail/3222>> (available on March 19 2025).
- Eurostat, Uporaba umetne inteligence v podjetjih, <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises&action=stats-explained&lang=sl> (available on March 19 2025).
- European Commission, Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act).
- European Commission, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2017, <<https://ec.europa.eu/newsroom/article29/items/612053>> (available on March 20 2025).
- Fritts, M. and Cabrera, F. (2021) AI recruitment algorithms and the dehumanization problem. In: *Ethics and Information Technology* 23 (4), p. 1-3.
- Information Commissioner of the Republic of Slovenia, Od 2. februarja je treba upoštevati prepovedi Akta o umetni inteligenci glede določenih UI sistemov, 2025, <<https://www.ip-rs.si/novice/od-2-februarja-2025-je-treba-upo%C5%A1tevati-prepovedi-akta-o-umetni-inteligenci-glede-dolo%C4%8Denih-ui-sistemov-1738746030>> (available on March 25 2025).

- Information Commissioner of the Republic of Slovenia, Opinion of the Information Commissioner of the Republic of Slovenia No. 07121-1/20250230, 24 February 2025.
- Lee, M. K. et al. (2015) Working with machines: the impact of algorithmic, data-driven management on human workers. In: Proceedings of the 33rd Annual ACM SIGCHI Conference, Seoul, South Korea, 18-23 April, New York: ACM Press, p. 1603.
- Maynard Keynes, J. (2010) Economic Possibilities for Our Grandchildren. In: Essays in Persuasion (Palgrave Macmillan), p. 321.
- Mateescu, A. and Nguyen, A. (2019) Explainer: algorithmic Management in the Workplace. https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf (available on March 25 2025), p. 1.
- Nazareno, L. and Schiff, D. (2021) The impact of automation and artificial intelligence on worker well-being. In: Technology in Society, Elsevier 67 (C), p. 3-5.
- Owlikowski, W. J. and Scott, S. V. (2014) What Happens When Evaluation Goes Online? Exploring Apparat-uses of Valuation in the Travel Sector. In: Organization Science 25 (3), p. 868.
- Pahor, M. and Langeršek, E. (2019) Nadzor zaposlenih na delovnem mestu. In: Delo + varnost 63 [64] (2), p. 19.
- Parviainen, H. (2022) Can algorithmic recruitment systems lawfully utilise automated decision-making in the EU? In: European Labour Law Journal 13 (2), p. 225-245.
- Polajžar, A. (2024a) Access of platform workers to collective rights – the fall of the binary divide? In: Časopis pro právní vědu a praxi, p. 195-212.
- Polajžar, A. (2024b) Collective labour rights of platform workers and the protection of privacy at work – based on the example of the European legal framework and selected EU countries. In: Wielec Marcin, Oreziak Barłomiej (ed.), The right to privacy: the view of young researchers (Wydawnictwo Instytutu Wymiaru Sprawiedliwości), p. 31-47.
- Polajžar, A. (2023c) Covert Surveillance at the Workplace and the ECtHR Approach: Possible Risks of Breaching GDPR Rules. In: E-Journal of International and Comparative Labour Studies 12 (3), p. 20-46.
- Polajžar, A. (2021a) Čas je za posodobitev zakonskega okvirja za močnejšo vlogo svetov delavcev v dobi digitalizacije in umetne inteligence (II. del), Razmišljanje o mogočih spremembah slovenske zakonodaje. In: Ekonomska demokracija 125 (4), p. 4.
- Polajžar, A. (2023a) Dostop platformnih delavcev v dejavnosti oglaševanja do kolektivnega dogovarjanja. In: Repas Martina (ur.), Dileme sodobnega oglaševanja: izbrane teme, (Univerzitetna založba), p. 277-306.
- Polajžar, A. (2021b) Varstvo zasebnosti delavca v dobi digitalizacije: GDPR in vloga delavskih predstavnikov. In: Delavci in delodajalci 21 (2/3), p. 277-286.
- Polajžar, A. (2023b) Vloga predstavnikov delavcev in delodajalcev pri uvajanju umetne inteligence v delovna razmerja ter primeri dobrih praks. In: Delavci in delodajalci 23 (2/3), p. 244-251.
- Popa, A. and Pascariu, L. (2024) Impact of EU's Artificial Intelligence Regulation on Workers. In: European Journal of Law and Public Administration 11(2), p. 98.
- Raghavan, M. et al. (2019) Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices. In: Proceedings of the 2020 Conference on Fairness, Accountability and Transparency (Association for Computing Machinery), p. 6-12.

- Rosenblat, A. and Stark, L. (2016) Algorithmic labour and information asymmetries: a case study of Uber's drivers. In: *International Journal of Communication* 10, p. 3758-3766.
- Sartor, G. and Lagioia, F. (2020) The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (Scientific Foresight Unit), p. 59-60.
- Senčur Peček, D. (2021) Pravica do odklopa in druga pravna vprašanja upravljanja delovnega časa v dobi digitalizacije. In: *Delavci in delodajalci* 21 (2/3), p. 298.
- Senčur Peček, D. (2017) Vpliv informacijske tehnologije na delovna razmerja. In: *Podjetje in delo* 6-7, p. 1171-1173.
- Senčur Peček, D. and Polajžar, A. (2023) Privacy at work in Slovenia. In: Hendrickx Frank, Mangan David, Gramano Elena (ur.), *Privacy@work:a European and comparative perspective* (Kluwer Law International B.V.), p. 476.
- SiStat, Število podjetij po izvoru uporabe tehnologije umetne inteligence in velikostnem razredu v Sloveniji, <<https://pxweb.stat.si/SiStatData/pxweb/sl/Data/-/2984709S.px>> (available on March 18 2025).
- Šerbec, H. and Polajžar, A. (2022) Predlog Akta o umetni inteligenci in vpliv na delovna razmerja. In: *Pravna praksa* 41 (15), p. 11-13.
- Tičar, L. (2016) Vpliv digitalizacije na pojav novih oblik dela. In: *Delavci in delodajalci* 16 (2/3) p. 253.
- Tomprou, M. and Lee Min, K. (2022) Employment Relationships in Algorithmic Management: A Psychological Contract Perspective. In: *Computers in Human Behaviour* 126.
- Wood, A. J. (2021) Algorithmic Management Consequences for Work Organisation and Working Conditions. In: *JRC Working Papers Series on Labour, Education and Technology* 2021/07, p. 1-14.
- Zuiderveen, B. F. (2018) Discrimination, artificial intelligence and algorithmic decision-making (Directorate General of Democracy), p. 8-38.

Legal Sources

- Charter of Fundamental Rights of the European Union, OJ C 202, 7.6.2016, p. 389–405 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV).
- Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work.
- Council of Europe, The Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law.
- Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community - Joint declaration of the European Parliament, the Council and the Commission on employee representation.
- 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.
- Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on Improving Working Conditions in Platform Work.
- International Labour Organization, Termination of Employment Convention No. 158.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

- and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).
- Ustava Republike Slovenije (URS), Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a in 92/21 – UZ62a.
- Zakon o delovnih razmerjih (ZDR-1), Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS, 81/19, 203/20 – ZIUPOPDVE, 119/21 – ZČmIS-A, 202/21 – odl. US, 15/22, 54/22 – ZUPŠ-1, 114/23 in 136/23 – ZIUZDS.
- Zakon o inšpekciji dela (ZID-1), Uradni list RS, št. 19/14 in 55/17.
- Zakon o sodelovanju delavcev pri upravljanju (ZSDU), Uradni list RS, št. 42/07 – uradno prečiščeno besedilo in 45/08 – Zarbit.
- Zakon o varnosti in zdravju pri delu (ZVZD-1), Uradni list RS, št. 43/11.
- Zakon o varstvu osebnih podatkov (ZVOP-2), Uradni list RS, št. 163/22.
- VDSS sodba in sklep Pdp 896/2013, ECLI:SI:VDSS:2014:PDP.896.2013
- VDSS sodba Pdp 264/2005, ECLI:SI:VDSS:2006:VDS.PDP.264.2005.
- VDSS Sodba Pdp 279/2021; ECLI:SI:VDSS:2021:PDP.279.2021.
- VDSS Sodba Pdp 483/2020, ECLI:SI:VDSS:2021:PDP.483.2020.
- VDSS Sodba Pdp 611/2019, ECLI:SI:VDSS:2020:PDP.611.2019.

Povzetek članka v slovenskem jeziku (abstract in Slovene language):

Ta članek obravnava vpliv umetne inteligence na vse faze delovnega razmerja ter analizira, ali obstoječi pravni okvir ustrezno varuje delavce pred tveganji, ki jih prinaša uporaba umetne inteligence v delovnem okolju. Članek se osredotoča na slovensko delovno pravo, pri čemer upošteva in analizira mednarodne in pravne vire EU, kot so Akt o umetni inteligenci, Direktiva o izboljšanju delovnih pogojev pri delu prek spletnih platform, Splošna uredba o varstvu podatkov (GDPR) in Listina EU o temeljnih pravicah. Avtorica obravnava pravne izzive uporabe umetne inteligence v delovnem okolju, kot so diskriminacija, varstvo podatkov, zasebnost, varnost in zdravje pri delu ter odgovornost za povzročeno škodo. Ugotavlja, da čeprav že obstajajo nekateri zaščitni mehanizmi, nobeden izmed analiziranih pravnih virov ne ureja uporabe umetne inteligence v delovnih razmerjih celovito. Za zagotovitev učinkovite zaščite delavcev avtorica zagovarja bodisi spremembo obstoječe zakonodaje bodisi sprejetje posebne zakonodaje. Ker bo umetna

inteligenca v prihodnosti igrala še pomembnejšo vlogo na področju delovnega prava, je ključno, da se pravo pravočasno prilagodi novim izzivom, ki jih prinaša umetna inteligenca.