AI Use in the Workplace. Some Legal Risks and Challenges

Dana VOLOSEVICI[1]

Abstract: As Artificial Intelligence (AI) advances, businesses benefit from its ability to exponentially enhance process effectiveness and efficiency, while also facing risks related to personal data protection, human dignity, and ultimately, human identity. This article aims to investigate two domains where AI is frequently employed in labor relations: recruitment and employee monitoring. In these areas, the article seeks to discuss aspects that could help clarify the conditions for the legitimate use of AI. A potential application of the ECJ's SHUFA case solution in recruitment is proposed, while the case of Amazon France Logistique is analysed concerning AI-based employee monitoring.

Keywords: AI, monitoring, recruitment, GDPR, workplace

Introduction

AI's impact on the concept of labor and its content is profound, reshaping the nature of work, skill requirements, and employment dynamics. The integration of AI into various industries has led to automation of repetitive and routine tasks, enhancing efficiency and productivity. This shift often results in the reduction of manual jobs but simultaneously creates opportunities for new roles that focus on managing, developing, and improving AI technologies. Employees now need to adapt by acquiring new skills and competencies, particularly in digital literacy, data analysis, and AI-related fields[2]. AI also influences workplace dynamics by enhancing decision-making processes. Employees benefit from AI-driven insights and analytics, which help in making informed decisions quickly. This can lead to increased efficiency, job satisfaction and performance, as employees are empowered with tools that enhance their capabilities. However, this reliance on AI also raises concerns about data privacy, ethical considerations, and the potential for bias in AI algorithms, which employees and employers must manage carefully[3].

This article aims to analyze the use of AI for two important aspects of the employment relationship, namely recruitment and performance monitoring. Both processes are considered high-risk AI systems by the AI Act. As expressly provided

---

[1] Ploieşti Petrol-Gaze University, Romania, e-mail: dana.volosevici@vplaw.ro

[2] F. Butera, G. De Michelis, *Intelligenza artificiale e lavoro, una rivoluzione governabile*, Marsilio Editori, 2024, p. 25.

[3] M. Airoldi, *Machine Habitus. Sociologia degli algoritmi*, Luiss University Press, 2024, p. 71.

by recital (57), AI systems used in employment and workers management, in particular for the recruitment and selection of persons and for monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high- risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights. Moreover, these two processes have a transdisciplinary content, because they intersect with multiple fields of expertise, blending insights from human resources, psychology, law, data science, and organizational behavior. As a consequence, they require a comprehensive understanding of human behavior, technological tools, applicable legal and organizational needs. As will be discussed in the subsequent sections, the legal approach, which aims primarily to protect the data subject, specifically the employee, imposes limitations on the implementation of certain practices that the industry seeks to adopt to enhance process efficiency, cost savings, and customer service improvements.

In recruitment and selection, psychological principles help in understanding candidate behavior and predicting job performance[4], while data science techniques enable the analysis of large applicant pools and the identification of the best matches through algorithms and predictive analytics. Organizational behavior insights ensure that selected candidates fit well with the company's culture and values. Law is intricately related to the recruitment process by establishing the legal framework within which hiring practices must operate. It ensures fairness and equality, prohibiting discrimination based on race, gender, age, or other protected characteristics. Employment laws regulate the use of personal data during recruitment, ensuring privacy and consent. Legal standards also dictate the terms of job postings, interview processes, and employment contracts, protecting both employers and potential employees.

Performance monitoring similarly integrates various disciplines. Data science and analytics are essential for processing performance metrics and providing actionable insights. Psychological theories aid in understanding employee motivation and engagement, crucial for designing effective performance management systems. Organizational behavior principles help in creating feedback mechanisms and development plans that align with the overall goals of the company. Law is crucial to the performance monitoring process as it ensures that employee evaluations are conducted fairly and ethically. Legal frameworks protect employee rights, mandating that performance data is collected and used without discrimination or bias. Privacy laws regulate how employee information is gathered, stored, and shared, ensuring confidentiality and informed consent. Labor laws also outline acceptable practices for performance reviews, feedback, and disciplinary actions, preventing unjust treatment and fostering a transparent work environment.

---

[4] J. M. Conte, F.J. Landy, *Work in the 21st Century. An introduction to Industrial and Organizational Psychology* Sixth Edition, Wiley, 2018, p. 169.

The transdisciplinary nature of recruitment and performance monitoring processes can create complexities in applying legal provisions due to the interplay of the diverse fields. This integration demands a nuanced understanding of various disciplines, making it challenging to ensure legal compliance uniformly. For instance, psychological assessments used in recruitment must be designed to avoid biases and adhere to anti-discrimination laws. However, integrating these assessments with data-driven tools like AI algorithms introduces additional layers of complexity. Ensuring that these algorithms are free from bias and do not inadvertently discriminate against protected groups requires continuous monitoring and legal oversight, which can be technically challenging and resource-intensive. Similarly, in performance monitoring, the use of advanced analytics and data science techniques must comply with privacy laws, ensuring that employee data is collected and processed transparently and with consent. Balancing the need for detailed performance insights with legal requirements for data protection can be difficult, especially as technologies evolve rapidly.

1. Some legal considerations regarding the use of AI in recruitment

The use of AI in recruitment has garnered significant academic attention, particularly concerning the legal implications. The literature also points to the necessity of interdisciplinary approaches, as legal scholars collaborate with data scientists and ethicists to develop comprehensive regulatory frameworks that address the multifaceted challenges posed by AI in recruitment. Moreover, the research papers underscore the importance of stringent legal oversight and the development of transparent, fair, and accountable AI systems to ensure that the benefits of AI in recruitment are realized without compromising legal and ethical standards.

Scholars such as Binns[5] and Leicht-Deobald et al.[6] emphasize the necessity for transparent AI systems to prevent discrimination and ensure fairness in hiring practices. These studies highlight the potential for AI to perpetuate biases if not properly monitored, raising significant legal challenges under employment discrimination laws. Barocas and Selbst[7] argue that the opacity of AI algorithms can obscure biased decision-making processes, making it difficult to identify and

---

[5] R. Binns, *Fairness in Machine Learning: Lessons from Political Philosophy*, Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency, pp. 149-159. https://doi.org/10.1145/3287560.3287581.

[6] U. Leicht-Deobald, T. Busch, C. Schank, A. Weibel, S.D. Schafheitle, I. Wildhaber, G. Kasper, *The Challenges of Algorithm-Based HR Decision-Making for Personal Integrity*, Journal of Business Ethics, no. 160, 2019, pp. 377-392, https://doi.org/10.1007/s10551-019-04204-w.

[7] S. Barocas, A.D. Selbst, A. D., *Big Data's Disparate Impact*, California Law Review, no. 104**,** 2016, pp. 671-732, https://doi.org/10.15779/Z38BG31.

address discriminatory practices. Dastin[8] underscores the need for compliance with data protection regulations, particularly with regard to the General Data Protection Regulation (GDPR). Thus, the data subject has the right to be informed in a „concise, transparent, intelligible and easily accessible form, using clear and plain language" (Article 12 (1), about how his data is collected, processed, and used, including about „the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" (Article 13 (2) f). Employees and candidates can request access to their personal data and obtain details about the logic behind AI-driven decisions that significantly affect them (Article 15 (1) h). They also have the right to rectify inaccuracies in their data (Article 16) and to object to automated decisions, demanding human intervention in certain cases (Article 18).

Further, Raghavan *et al.*[9] explore the impact of AI on privacy rights, emphasizing the importance of consent and transparency in data collection. Their research suggests that AI tools often collect extensive personal data, necessitating robust legal frameworks to protect candidates' privacy. The work of Kim[10] delves into the ethical and legal ramifications of using predictive analytics in recruitment, arguing that the predictive nature of AI can lead to preemptive discrimination against certain demographic groups, challenging existing anti-discrimination laws. Ajunwa, Crawford, and Schultz[11] discuss the implications of the Americans with Disabilities Act (ADA) in the context of AI, noting that automated systems must be designed to accommodate individuals with disabilities, ensuring accessibility and fairness. Additionally, scholars like Edwards and Veale[12] highlight the need for accountability in AI systems, suggesting that the lack of clear responsibility can complicate legal recourse for affected individuals.

Another aspect worth analyzing is the legal applicability in recruitment of the Article 22 of the GDPR, which states that „the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly

---

[8] J. Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, Reuters, 2018 [online] at https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G, accessed on 10.06.2024.

[9] M. Raghavan, S. Barocas, J. Kleinberg, K. Levy, *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices*. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 2020, pp. 469-481, https://doi.org/10.1145/3287 560.3287587.

[10] P.T. Kim, *Data-Driven Discrimination at Work*, William & Mary Law Review, no. 58, 2017, pp. 857-936, https://scholarship.law.wm.edu/wmlr/vol58/iss3/5.

[11] I. Ajunwa, K. Crawford, J. Schultz, *Limitless Worker Surveillance*, California Law Review, no. 105**,** 2017, pp. 735-776. https://doi.org/10.15779/Z38BR8MF94.

[12] L. Edwards, M. Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For*, Duke Law & Technology Review, no. 16, 2017, pp. 18-84, https://doi.org/10.2139/ssrn.2972855.

significantly affects him or her." In this context, we aim to examine how SCHUFA ECJ ruling[13] on automated processing, particularly in relation to a credit scoring system, could provide guidelines for data processing in the recruitment process.

SCHUFA, a private German company, provides its contractual partners with information on the creditworthiness of third parties, especially consumers. It creates a „score" predicting future behavior, like loan repayment, based on certain personal characteristics using mathematical and statistical methods. The scoring process assumes that by grouping individuals with similar characteristics, future behavior can be predicted. OQ was denied a loan by a third party due to negative information from SCHUFA. She requested SCHUFA to provide her personal data and to erase allegedly incorrect data. SCHUFA informed OQ of her score and generally described the scoring methods but, citing trade secrecy, refused to disclose specific elements and their weightings used in the calculation. SCHUFA maintained that it only provides information to its partners, who make the actual contractual decisions. OQ filed a complaint with HBDI, the competent supervisory authority, on October 18, 2018, requesting that SCHUFA grant her access to information and erase the incorrect data. On June 3, 2020, HBDI rejected her complaint, stating that it was not proven that SCHUFA failed to comply with Article 31 of the BDSG regarding its activities. OQ appealed this decision to the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany).

In response to Verwaltungsgericht Wiesbaden question, the ECJ ruled that „Article 22(1) of GDPR „must be interpreted as meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes 'automated individual decision-making' within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person."

In its reasoning, the ECJ clarified that for Article 22(1) to be applicable, three cumulative conditions must be met., Firstly, there must be a 'decision.' Secondly, that decision must be 'based solely on automated processing, including profiling'. Thirdly, that it must produce 'legal effects concerning [the interested party]' or 'similarly significantly [affect] him or her'[14].

Regarding the concept of a decision, the Court clarified that this refers not only to acts that produce legal effects concerning the individual but also to acts that similarly significantly affect him or her. To support this interpretation, reference was made to recital 71 of the GDPR, which explicitly mentions the „automatic refusal of an online credit application or e-recruiting practices without any human intervention." According to Advocate General Pikamäe, in the case under consideration, the decision process included several phases, such as

---

[13] ECJ, Judgment of 7 December 2023, Case C-634/21, SCHUFA Holding, ECLI:EU:C:2023:957.

[14] *Ibidem*, 43.

profiling, the establishment of the score, and the actual decision on the grant of credit[15].

Additionally, the Advocate General noted that the possibility of assigning certain powers to an external service provider does not seem to play a crucial role in the analysis regarding the application of the rules under Article 22(1). What is important is that the result of the analysis conducted by SCHUFA was almost automatically adopted by the credit institution. Thus, according to the referring court, even though human intervention was still possible at that stage of the decision-making process, the decision to enter into a contractual relationship with the data subject was practically determined by the score transmitted by credit agencies to such a considerable extent that the score heavily influenced the third-party controller's decision. Consequently, the score itself must be regarded as having the status of a 'decision' within the meaning of Article 22(1) of the GDPR.

Returning to the issue of recruitment, it is a common practice for companies to collaborate with external recruitment providers to leverage specialized expertise, access a broader talent pool, and streamline the hiring process. External contractors possess deep industry knowledge, extensive networks, and advanced tools for candidate sourcing and evaluation, which can result in higher quality hires and reduced time-to-fill positions. When external recruitment contractors use AI for candidate profiling, they use advanced algorithms to analyze vast amounts of data to predict candidate suitability for specific roles. This technology can analyze various factors, such as work history, education, skills, and even social media activity, to create comprehensive candidate profiles. As long as the GDPR provisions regarding data minimization, candidate notification, and the granting of legally recognized rights are adhered to, the use of algorithms cannot be considered inherently unlawful. The issue arises when the data subject, specifically the candidate, believes they have been harmed by how their profile was established, either through a discretionary action of the algorithmic analysis or by the omission of relevant information. In such instances, similar to the SCHUFA case, it must be determined whether the external consultant can be required to provide the candidate with information about the various elements considered in the calculation and their respective weightings.

Given that the matter concerns the conclusion or non-conclusion of an employment contract, it is evident that the outcome of the analysis produces "legal effects concerning him or her" or "similarly significantly affects him or her." The impact of the score determined by the recruitment firm through AI technology is more significant with the prominence of the recruitment firm. Although the company requesting the recruitment services could theoretically disregard the score provided by the recruiter, it will most likely be significantly influenced by it. As highlighted by the ECJ, it is the responsibility of national courts to determine,

---

[15] ECJ, Opinion Of Advocate General Pikamäe, delivered on 16 March 2023, Case C-634/21, SCHUFA Holding, ECLI:EU:C:2023:220.

in each case, the contextual framework and the extent of the recruitment firm's influence on the hiring company.

Consequently, recruitment contractors utilizing AI must ensure transparency in their data handling practices and provide candidates with the opportunity to understand and challenge decisions made by AI systems. To substantiate this right, candidates must be informed about how their data is being used, that the data will be processed not by the prospective employer but by a third party, including through the use of AI and that this process involves generating profiles and scores that will be transmitted to the prospective employer.

2. Legal risk related to the use of AI in monitoring the employee activity

The use of AI in monitoring employee activity involves sophisticated algorithms that analyze vast amounts of data to evaluate performance, productivity, and compliance with company policies. AI systems can track various aspects such as computer usage, communication patterns, and even biometric data to provide detailed insights into employee behavior. Monitoring methods are multiple and continuously developing. Some of the tools help employers monitor real-time activity. For example, Toggl and RescueTime use AI to automatically track the time employees spend on different tasks and applications, providing detailed productivity reports. Platforms such as Hubstaff and Teramind offer extensive features including screen capture, keystroke logging, and application usage tracking. Some other tools like ActivTrak use AI to analyze behavioral patterns, identifying trends and anomalies in employee performance. Devices like smartwatches and fitness trackers can monitor physical activity, stress levels, and overall well-being, providing employers with insights into employee health and productivity. Platforms like Microsoft Teams and Slack have integrated analytics that track communication patterns and collaboration metrics, helping managers understand team dynamics and efficiency. With the rise of remote work, tools like Time Doctor and Hubstaff offer features specifically designed to monitor remote employees, including GPS tracking, activity levels, and project management integration.

While enhancing the ability to monitor and improve employee productivity, these tools raise significant privacy and ethical considerations, as they constitute continuous monitoring. As noted in WP 29 Opinion on data protection at work, if there are no limits to the processing, and if it is not transparent, there is a high risk that the legitimate interest of employers in the improvement of efficiency and the protection of company assets turns into unjustifiable and intrusive monitoring"[16].

One recent example of exceeding the limits of an employer's right to monitor employee activity is the case of Amazon Logistique France, which received

---

[16] Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, p. 9.

a fine of 32 million euros from the French Supervisory Authority, the CNIL. Amazon France manages extensive warehouses in France, handling the reception, storage, and preparation of items for customer delivery. Employees in these warehouses are equipped with scanners to document the real-time performance of tasks such as shelving or packing items. Each scan generates data recorded and used to calculate indicators on the quality, productivity, and periods of inactivity of each employee. Following media reports on the company's practices, the French Supervisory Authority (SA) conducted multiple investigations and received several complaints from employees.

The analysis of data obtained from employees aimed to align with research in industrial practices. Access to such data allows managers to identify and address issues as they arise. Moreover, real-time performance monitoring provides immediate feedback, motivating employees to improve their productivity and efficiency. In „The Second Machine Age," MIT's Erik Brynjolfsson and Andrew McAfee[17] demonstrate that data-driven decision-making can lead to substantial productivity gains by enabling companies to adapt swiftly to changing conditions. The issue, therefore, is determining whether there are limits to such monitoring and, if so, what elements must be considered to establish those limits.

The CNIL did not question the need for ensuring a company's competitiveness, which justified Amazon's scanner system to manage its operations. Thus, the practice of electronically monitoring employees and using the obtained data for industrial purposes was validated. However, the French Supervisory Authority noted that the retention of all this data and the resulting statistical indicators was disproportionate. The system for measuring the speed at which items were scanned was found excessive. This system operated on the principle that items scanned very quickly increased the risk of error, leading to the establishment of an indicator to measure whether an item had been scanned in less than 1.25 seconds after the previous one. Consequently, employee behaviour was monitored every 1.25 seconds.

Such monitoring, which involved the use of scanners, differed from traditional activity monitoring methods due to its scale, exhaustiveness, and permanence, leading to very close and detailed scrutiny of employees' work. The permanent monitoring of employees, encompassing the entire spectrum of their activities throughout the workday, was considered abusive because it placed employees under continuous pressure. The Article 29 Working Party (WP29) noted as early as 2017 that monitoring communications and behavior pressures employees to conform to prevent the detection of perceived anomalies, similar to how intensive CCTV use has influenced citizen behavior in public spaces[18]. The CNIL further deemed it excessive to retain all data collected by the system and the resulting statistical indicators for all employees and temporary workers for 31 days.

---

[17] E. Brynjolfsson, A. McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies, 2014,* W.W. Norton & Company.

[18] Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, Adopted on 8 June 2017.

Amazon France responded[19] that the use of warehouse management systems is a common practice in the industry, being necessary to ensure the safety, quality, and efficiency of operations, as well as to track inventory and process parcels in a timely manner and in accordance with customer expectations. The three indicators either signal a risk of error when an employee scans an item in less than 1.25 seconds after scanning a previous item (the "Stow Machine Gun" indicator), periods of scanner inactivity of ten minutes or more (the "idle time" indicator), or scanner interruptions between one and ten minutes (the "latency under ten minutes" indicator). It is proven[20] that, by integrating various functions such as inventory control, order fulfilment, and shipping logistics, warehouse management systems enhance operational efficiency and reduce errors. They provide real-time visibility into inventory levels, locations, and movement, enabling better decision-making and resource allocation. However, industrial practices, even if proven to be efficient, must pass the test of legality, including those related to data minimization (Art. 5(1)(c)) and lawful processing (Art. 6 of GDPR).

The considerations of the CNIL's decision can contribute to shaping industrial practices that avoid abuses, even when these practices are based on seemingly neutral technical aspects, such as the need for data analysis to optimize production. Thus, without denying the potential importance of providing assistance to an employee or reassigning them in real time within the industrial process, the CNIL ruled that this does not necessitate access to every detail of the employee's quality and productivity indicators collected over the last month using scanners. The supervisory authority expressed the opinion that, in addition to real-time data, a selection of aggregated data, on a weekly basis, for example, would be sufficient.

We are therefore at a juncture where a just balance must be found between the industry's tendency to generate safety and progress through the use of AI and the employees' right to perform their work in conditions that do not constitute continuous pressure on them. The trend of measuring employees' activity down to the smallest gesture could hinder the natural development of human personality and the specific axiological characteristics of human beings.

3. Employee involvement for a legitimate AI use

The employment contract is characterized by an inherent imbalance of power between the parties, with the employee performing their duties under the authority of the employer. According to Article 40(1)(a) and (d) of the Labor Code,

---

[19] Déclaration d'Amazon à propos de la décision de la CNIL, https://www. aboutamazon.fr/actualites/politiques-publiques/declaration-damazon-a-propos-de-la-decision-de-la-cnil.

[20] L. N. Tikwayo, T. N. D. Mathaba, *Applications of Industry 4.0 Technologies in Warehouse Management: A Systematic Literature Review*, Logistics 2023, no. 7, 24. https://doi.org/10.3390/ logistics7020024.

the employer is granted the right to determine the organization and functioning of the unit and to exercise control over how job responsibilities are fulfilled. Even prior to the formalization of an employment contract, employers possess the authority to conduct comprehensive analyses of prospective employees' personal data. This practice involves the use of automated data processing techniques, including profiling, either directly by the employer or through an authorized agent. The exercise of such powers is subject to stringent legal and ethical scrutiny, given the potential for significant intrusion into personal privacy. Throughout the tenure of the employment relationship, employers may implement various monitoring mechanisms to oversee employee performance and compliance with job responsibilities. The degree of intrusiveness associated with these monitoring activities can vary significantly. Key factors influencing this include the specific technological tools employed, the scope and nature of these instruments, and the extent of data processed. Advanced technologies such as artificial intelligence and video surveillance can offer detailed insights into employee activities, raising important considerations regarding data protection and privacy rights under applicable legal frameworks. Employers must balance the legitimate business interests in monitoring and maintaining workplace efficiency with the necessity of safeguarding employees' privacy and personal data. Compliance with data protection regulations, such as the GDPR, is imperative to ensure that monitoring practices do not disproportionately infringe on employees' rights.

Beyond the actions of employers, employees, through unions or employee representatives, must play a proactive role in promoting their own rights. For instance, Romanian law[21] stipulates that when electronic communication systems or video surveillance are used in the workplace for monitoring purposes, the processing of employees' personal data to achieve the legitimate interests pursued by the employer is permitted only if the following cumulative conditions are met. First, the employer's legitimate interests must be thoroughly justified and outweigh the interests, rights, or freedoms of the individuals concerned. Additionally, the employer must provide mandatory, complete, and explicit prior information to the employees. Before introducing monitoring systems, the employer must consult with the union or, where applicable, employee representatives. It is also necessary that other less intrusive means and methods to achieve the employer's intended purpose have previously proven ineffective. Lastly, the duration of personal data storage must be proportional to the purpose of the processing and not exceed 30 days, unless expressly regulated by law or justified by specific situations.

---

[21] Law no. 190/2018 on measures to implement Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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), published in the Official Gazette no. 651 of 26 July 2018.

According to the Social Dialogue Law[22], consultation entails the exchange of opinions and information and the establishment of a dialogue between social partners (article 1, 2. b). This process ensures that both parties - employers and trade unions or employee representatives - can contribute to decision-making processes, particularly those affecting working conditions and employee rights. Therefore, unions or, where applicable, employee representatives are entitled to access the information and studies that formed the basis for implementing monitoring measures. They have the right to request further details and to articulate their stance on the introduction of such measures. This involvement ensures transparency and accountability in the decision-making process, allowing employees' interests to be considered and safeguarded. If individual employees and candidates might find it challenging to protect their rights[23], unions can play a crucial role in this regard. Through the consultation procedure and collective bargaining[24], unions can help establish a framework that ensures real protection of employees' rights, particularly concerning the use of AI in employment relationships. Unions can advocate and bargain for transparency, fairness, and accountability in AI-driven processes[25], ensuring that these technologies are used in ways that respect and uphold workers' rights. This collective approach is essential in balancing technological advancements with the need for equitable treatment in the workplace. In this regard, trade unions in several European countries have begun incorporating AI-related issues into collective bargaining agreements. For instance, under a recent agreement concluded by the government and the social partners in Spain, „digital platforms will have to make available to trade unions an algorithm, or any artificial intelligence of sorts, which may have an impact on such conditions – including individuals' access to, and maintenance of, employment and their profiling. This right to information is granted to everyone working through a platform [...] and thus the transparency requirement applies to all digital platforms equally"[26]. At European level, the European social partners agreed on a programme on European social dialogue which addresses the challenges of the extensive increase in the use of digital tools at the workplace and decided to „create the space for exchanging views on these trends and the relevance

---

[22] Law. no. 367/2022 on Social Dialogue, published in the Official Gazette no. 1238 of 26 December 2022.

[23] A. Aloisi, V. De Stefano, *Your Boss is an Algorithm. Artificial Intelligence, Platform Work and Labour*, Oxford Hart Publishing, 2022.

[24] A. Aloisi, E. Gramano, *Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context*, Comparative Labor Law & Policy Journal no. 41(1), 2019, pp. 95–122.

[25] V. De Stefano, '*Masters and servers': Collective labour rights and private government in the contemporary world of work*, International Journal of Comparative Labour Law and Industrial Relations no. 36(4), 2020, pp. 435–443.

[26] A. Aranguiz, *Spain's platform workers win algorithm transparency*, Social Europe, 2021, [Online] at https:// www.socialeurope.eu/spains-platform-workers-win-algorithm-transparency, accessed on 10.06.2024.

this has for social partners and collective bargaining at all appropriate levels across Europe"[27]. Moreover, in the matter of employment, the Article 88 of GDPR itself recognizes the role of collective bargaining, alongside that of the law to provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including [...] management and planning and organization of work.

Conclusion

The utilization of AI in society, particularly within the realm of labour relations, presents not only a legal challenge but also a significant moral dilemma in the current stage of societal development. While technological advancements captivate by breaking barriers in critical life domains, they simultaneously compel us to identify and preserve those quintessential human attributes that should remain beyond the reach of non-human entities. In labour relations, sophisticated tools have already been implemented to deeply measure various aspects of human behaviour and performance. This includes both the profiling of job candidates and the ongoing, comprehensive monitoring of employees. Such practices place workers under continuous scrutiny, thereby eroding their privacy and encroaching upon their private behavioural and even physiological traits. To mitigate potential abuses, a synergistic approach is essential, involving legal frameworks, judicial oversight, supervisory authorities, unions, and professional organizations. The objective is not to resist technological progress but to shape the future in accordance with values that universally define human dignity and integrity. By addressing these challenges through a concerted effort, we can ensure that the integration of AI into the workplace enhances rather than diminishes the human experience, safeguarding fundamental rights while embracing technological innovation.

References

Airoldi M., *Machine Habitus. Socilogia degli algoritmi*, Luiss University Press, 2024, p. 71.

Ajunwa I., Crawford K., Schultz J., *Limitless Worker Surveillance*, California Law Review, no. 105**,** 2017, pp. 735-776. https://doi.org/10.15779/Z38BR8MF94.

Aloisi A., De Stefano V., *Your Boss is an Algorithm. Artificial Intelligence, Platform Work and Labour*, Oxford Hart Publishing, 2022.

Aloisi A., Gramano E., *Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context*, Comparative Labor Law & Policy Journal no. 41(1), 2019, pp. 95–122.

Aranguiz A., *Spain's platform workers win algorithm transparency*, Social Europe, 2021, [online]

Barocas S., Selbst, A. D., *Big Data's Disparate Impact*, California Law Review, no. 104**,** 2016, pp. 671-732, https://doi.org/10.15779/Z38BG31.

---

[27] European Social Dialogue, Work Programme 2022-2024, [Online] at https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/2022-06-28_european_social_dialogue_programme_22-24_0.pdf, accessed on 10.06.2024.

Binns R., *Fairness in Machine Learning: Lessons from Political Philosophy*, Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency, pp. 149-159. https://doi.org/10.1145/3287560.3287581.

Brynjolfsson E., McAfee A., *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies, 2014,* W.W. Norton & Company.

Butera F., De Michelis G., *Intelligenza artificiale e lavoro, una rivoluzione governabile*, Marsilio Editori, 2024, p.25.

Conte J. M., Landy F.J., *Work in the 21st Century. An introduction to Industrial and Organizational Psychology* Sixth Edition, Wiley, 2018, p. 169.

Dastin J., *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, Reuters, 2018 [online]

Edwards L., Veale M., *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For*, Duke Law & Technology Review, no. 16, 2017, pp. 18-84, https://doi.org/10.2139/ssrn.2972855.

European Social Dialogue, Work Programme 2022-2024, [online]

Kim P.T., *Data-Driven Discrimination at Work*, William & Mary Law Review, no. 58, 2017, pp. 857-936.

Leicht-Deobald U., Busch T., Schank C., Weibel A., Schafheitle S. D., Wildhaber I., Kasper G., *The Challenges of Algorithm-Based HR Decision-Making for Personal Integrity*, Journal of Business Ethics, no. 160, 2019, pp. 377-392, https://doi.org/10.1007/s10551-019-04204-w.

Raghavan M., Barocas S., Kleinberg J., Levy K., *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices.* Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 2020, pp. 469-481, https://doi.org/10.1145/3287560.3287587.

De Stefano V., '*Masters and servers': Collective labour rights and private government in the contemporary world of work,* International Journal of Comparative Labour Law and Industrial Relations no. 36(4), 2020, pp. 435–443.

Tikwayo, L. N., Mathaba T. N. D., *Applications of Industry 4.0 Technologies in Warehouse Management: A Systematic Literature Review*, Logistics 2023, no. 7, 24. https://doi.org/10.3390/ logistics7020024.