

Olena Ye. Lutsenko

Yaroslav Mudryi National Law University, Ukraine

o.lutsenko8267-2@edu-knu.com

ORCID ID: 0000-0001-9357-8546

Olena H. Sereda

Yaroslav Mudryi National Law University, Ukraine

osereda3@gmail.com

ORCID ID: 0000-0002-8252-1963

Georgii Zhelef

Interregional Academy of Personnel Management, Ukraine

georgiy.zhelef@gmail.com

ORCID ID: 0009-0000-1460-1446

Nataliia Stepanenko

KROK University, Ukraine

nataliasv@krok.edu.ua

ORCID ID: 0000-0002-9421-6827

Maxim O. Tymoshenko

Private Higher Education Establishment “European University”, Ukraine

maxim.tymoshenko@e-u.edu.ua

ORCID ID: 0000-0003-2584-5731

Artificial Intelligence in Labour Relations: Is Ukrainian Labour Law Ready for European Standards?

Abstract: This article aims to carry out a comparative analysis of the regulation of AI use in labour relations in Ukraine and the EU, with a view to identifying common trends and differences and formulating recommendations for enhancing Ukrainian legislation in the context of digitalization. The study uses methods of comparative analysis and formal legal and functional approaches. It analyses the main aspects of AI application in labour relations, in particular in recruitment, personnel management, management decision-making, and the protection of employees' personal data. The authors examine the

main international and EU regulations (GDPR and AI Act) that set requirements for processing the personal information of employees using AI. Thus it is determined that Ukraine does not have a specialized legal framework for regulating such processes, while the EU is developing relevant standards which guarantee the transparency of algorithms, the protection of employees' rights, and the ethical use of digital technologies. Consequently, the authors suggest a conceptual model of the regulation of AI application in the labour sphere, which covers the basic principles, stages of interaction, risk classification, subject-object relations, and institutional control mechanisms. The presented model may serve as a basis for developing a Ukrainian law on AI use in labour relations.

Keywords: personal data, labour relations, artificial intelligence, digital ethics, GDPR, e-commerce workforce regulation

Introduction

Modern labour markets and administrative decision-making now incorporate AI as a structural component. Its use in hiring, performance reviews, and workforce management changes traditional employment relationships and creates new legal issues, especially in the areas of algorithmic control and personal data security. While AI presents new legal challenges in the identification of its operations, the ability of robots to analyse data, learn, and make decisions opens up new opportunities. However, technological advances pose challenges for legal systems to regulate and protect the rights and interests of citizens (Getman et al., 2023).

Working life is affected by the rise and development of the knowledge-based economy and communication technologies. While productivity and competitiveness are benefiting from these developments, there are several risks and obstacles (Bondarenko et al., 2022). Knowledge and information are now essential components of the post-industrial labour economy; as a result, there is a marked increase in information flows in labour relations. This is particularly influenced by the new human resource management, which views employees as the key to corporate success. Furthermore, the globalization of the economy, the increase in international corporate mergers, and the development of an information society driven by technological innovation have increased the information needs of both companies and the workforce.

Information regulation, including the protection of employees' personal information, is directly related to labour relations, which are particularly sensitive to it. For this reason, the protection of employees' data has become a pressing issue and is the focus of ongoing academic and applied debate, legislation, and research at the international, European, and national levels. At every level of employment, a significant part of the duties that employees regularly perform at work already involves the gathering and processing of personal information. The purpose of modern advances in human resource management is to boost the value of human capital in business in terms of work organization and the use of technologies; as a result, personal information about employees is constantly collected and processed at work.

Consequently, the fundamental human rights of workers, including the right to privacy and the protection of personal data, along with the role of effective employment in promoting a robust economy, the creation of more and better jobs, and the nurturing of an inclusive society, are gaining increasing recognition (Kalina et al., 2022). Several scholars have studied the topic of AI and human rights. In their study of personal data protection in the context of AI use, Bielova and Byelov (2023a) analysed challenges such as the instability of technological progress and security threats such as unauthorized access and algorithmic bias; they proposed recommendations to ensure data security and privacy, such as strict processing rules, encryption, and data anonymization. Asiryan (2023a) analysed the regulation of AI use, personal data protection, and the transparency of automated systems, claiming that the EU was active in protecting the rights of citizens, but pointing out that further measures are needed to develop standards on digital rights. The issue of protecting the privacy of personal information in labour relations, particularly in light of the proliferation of artificial intelligence, was examined by Kronivets and Dorosh (2024), who placed particular emphasis on the importance of establishing precise guidelines for the utilization of such data in conjunction with ethical considerations.

Kolesnikov and Karapetian (2023) studied the current state, opportunities, threats, and limitations of AI in Ukraine and worldwide. They outlined the main aspects of AI implementation in Ukrainian society and pointed out the need for legislative regulation in the areas of privacy and data protection, ethical aspects, the regulation of inter-sectoral relations, and support for innovation and start-ups. Predmestnikov and Yarmolyuk (2023) analysed the problems of human rights protection in the digital environment; they investigated the social, legal, and ethical facets of these technologies and created regulatory frameworks to reconcile innovation with the defence of human rights.

However, this issue requires additional research due to the speed at which AI technologies are developing and the need to establish a legal framework to regulate AI use in Ukraine. In addition to comparing Ukrainian and EU approaches, this study aims to determine if Ukrainian labour law is prepared to adopt European standards on AI regulation and under what legal circumstances such harmonization is feasible. Hence our objectives are as follows:

- to analyse the legislation on AI use in labour relations in Ukraine;
- to study approaches to AI regulation of labour in the EU, in particular the GDPR and the AI Act;
- to define the main legal, ethical, and security aspects of AI application in recruitment, HR management, and employee rights protection;
- to compare Ukrainian and EU legislation in the main areas of AI regulation in labour;
- to suggest a conceptual model for the regulation of AI application in labour in Ukraine.

1. Methodological framework

Several research methods were used to achieve the research aim and objectives. The dialectical method was the basis of the research, and helped us to identify the current state of the topic under consideration through a thorough study of procedures for collecting, processing, and protecting employees' information against the background of digital transformation. This facilitated an assessment of the inconsistencies and conflicts that arise, in order for us to consider these processes as a connected system and to understand their evolution. In addition, this strategy encourages multidisciplinary research, which is critical to understanding the current situation and the potential future directions of the sector.

The functional method has proven to be an important part of analysing systemic relationships in the context of employee data protection. By describing the functions of and links between different components of the system, its use allows us to consider these as functional parts of the system. This method helps us to understand the interaction between data protection procedures and functions within the system, as well as between other systems and the outside world. As a result, this methodology ensures an effective approach to data protection and helps us to highlight important aspects of employee data protection.

The critical analysis of the current labour legislation that regulates the protection of employees' data in the light of AI was conducted using the formal-logical method. This approach allowed for a systematic and logical analysis of the legal acts regulating these issues. Using this approach, specific recommendations were developed to strengthen the laws that address legal issues of the security of employees' personal information in the context of AI development. By identifying these shortcomings and inconsistencies in Ukrainian legislation and suggesting solutions, this strategy helps to ensure more effective regulation of these issues.

In order to examine the European experience of the legal regulation of AI use with regard to employees' data protection, the paper employs the comparative technique. This methodology makes it possible to compare national norms and strategies for dealing with this matter with EU laws and practices. Analysing the European experience can yield best practices and recommendations that can be used to reinforce national laws pertaining to the protection of personal data. In addition to understanding the trends and quirks of controlling this issue in the context of AI development, such a comparative analysis aids in the creation of more efficient data management and security techniques.

2. Results

2.1. The Ukrainian legal framework on AI use in labour relations

The creation and adoption of suitable legislation that governs the AI processing of employees' personal data in labour relations is crucial to prevent the possibility of leaks or misuse of data and violation of employees' privacy. Several normative legislative acts that govern this sector are now included in Ukraine's national legislation. First, Article 32 of the Constitution of Ukraine forbids the gathering, storing, using, and disseminating of private information about an individual without that person's agreement, unless it is in situations allowed by law and exclusively in the interests of human rights, economic prosperity, and national security (Verkhovna Rada of Ukraine, 1996).

The Law of Ukraine no. 2297-VI 'On Personal Data Protection' establishes the rights and obligations of subjects of personal information and the requirements for organizations that process such data. It is aimed at ensuring the confidentiality and protection of the personal data of citizens of Ukraine and other persons staying on the territory (Verkhovna Rada of Ukraine, 2010). Furthermore, when an employment contract is signed, it is illegal to ask someone who has been accepted for work for information about their origin, political party and national affiliation, place of residence or where their stay is registered, and any documents whose submission is not required by law, according to Article 25 of the Labour Code of Ukraine (Verkhovna Rada of Ukraine, 1971). This standard highlights how crucial it is to safeguard privacy and avoid discrimination in the workplace on the basis of individual traits.

However, the right to protect personal information, and in particular to ensure the confidentiality of health information, has real value only when it can be protected in the event of a violation. Thus Article 188-39 of the Code of Ukraine on Administrative Offences establishes responsibility for violations of legislation on personal data protection (Verkhovna Rada of Ukraine, 1984). The civil law of Ukraine therefore does not restrict the right to protection to actions taken by the government or other recognized entities that have the authority to use coercive measures against criminals. The link between victims' rights and self-defence is mostly governed by Article 19 of the Civil Code of Ukraine (Verkhovna Rada of Ukraine, 2003). Therefore a person has the freedom to pick their own protection methods based on the specifics of the right that has been violated, the type of violation committed, and its repercussions.

Initial measures to control the use of AI have already been implemented in Ukraine: the Concept of Artificial Intelligence Development in Ukraine was developed in 2020, outlining the definition, goals, guiding principles, and objectives of AI development for the first time at the legislative level (Ministry of Digital Transformation of Ukraine, 2020). A working group on AI regulation was also created by the National Association of Lawyers of Ukraine. The working group protects personal data collected by AI systems, establishes guidelines for its use and storage, and analyses legal issues

related to AI application (Vyshnevskyi, 2023); it also defines the limits of its application in various industries. The working group strives to guarantee that human rights are appropriately safeguarded when AI systems are utilized (Bielova & Byelov, 2023b).

Furthermore, the ratification of the Artificial Intelligence Act (European Parliament, 2024) will directly affect AI regulation in Ukraine. Consequently, the Ukrainian government has decided to implement a regulated sandbox for AI developers. Gordiy Rummyantsev, a state expert in the Directorate of European and Euro-Atlantic Integration at the Ministry of Digital Transformation of Ukraine, has posited a managed ecosystem within which developmental enterprises would be empowered to cultivate their products from the outset, encompassing design considerations, with the objective of aligning with the stipulated criteria of the impending EU standards. This legislation signifies a major milestone in the realm of AI legislation, offering a framework for addressing concerns regarding the potential implications of this technology while fostering innovation (Ministry of Digital Transformation of Ukraine, 2020).

When implementing AI systems into organizational processes and the work environment in Ukraine, there are several legal challenges related to ensuring the confidentiality and protection of the personal data of employees. The list of AI applications that improve labour relations, especially when used by employers, is not exhaustive, nor are the procedures that require them. Therefore, scholars have identified the stages of labour relations that are associated with computerized databases, data processing programs, and customer relationship management (CRM) systems which also collect personal data:

- a) Interviews with a potential employee, because at the stage of receiving a CV, the employer already receives the relevant data.
- b) The conclusion of an employment contract, filling out an identity card, and other documents necessary for employment.
- c) The dismissal process, after which the personal data of the employee must be destroyed immediately or after a certain period, which is determined by consent and the policy of personal data processing by the employer.

The vast majority of these processes are carried out by HR specialists, who use AI technologies to automate the relevant activities. It is appropriate to note that the World Economic Forum has predicted, based on analytical data and various studies, that from 2025 the encryption industry will grow and the field of robotics will develop, which will also necessarily be reflected in labour relations (Predmestnikov & Yarmolyuk, 2023). With this in mind, employers should take extra care when collecting and using employee data. Legislation should delineate the limits on and types of data that AI can process. For example, it would be reasonable to include relevant norms in the Law of Ukraine 'On Artificial Intelligence', if it is adopted (Vavzhenchuk & Zhmaka, 2024).

AI techniques can be unpredictable and complex, so it can be difficult to understand and defend the choices they make. This may affect the right to a fair trial and

the right to explanation, two important provisions of the GDPR (European Parliament, 2016), determining who is responsible for the decisions or actions of AI systems, especially when those actions cause a breach of security or privacy involving employees. They may misidentify or recognize employees, violating their right to privacy and confidentiality. AI systems could discriminate against workers because of their differences, which would violate human rights and create inequality (Nikitenko et al., 2024).

When AI systems are used in an organizational environment, personal data about employees can be collected and processed in large volumes from various sources using a range of technologies. This may involve automating HR procedures, tracking performance, evaluating staff performance, and analysing workplace behaviour. To avoid any breach of employee privacy and confidentiality, strict data protection and security guidelines must be followed when collecting and processing personal information. To guarantee employees' privacy and to protect their rights, it is important to ensure that they are fully informed about how AI systems will use their data and that they give their consent.

A comprehensive strategy that integrates technological, legal, and ethical responses is needed to address these legal challenges in a way that protects workers' rights and complies with data protection regulations. By taking the actions discussed below, the state can resolve legal issues related to the security of the personal data of employees when AI systems are used (Asiryan, 2023b). It is important to create and implement special laws in Ukraine that regulate AI use when employees' personal data are processed; this may entail new legislation or changes or additions to current data protection laws.

Effective implementation will necessitate institutional capacity, supervisory procedures, and procedural protections that ensure adherence to data protection standards in AI systems related to employment, in addition to legal reform. However, rather than depending only on voluntary corporate practices, such measures must be included in a logical legal framework. For example, by implementing reporting and auditing systems, organizations can be encouraged to be open and transparent about AI use and the processing of personal data (Raji et al., 2020). An appropriate legislative framework will enable the adoption of AI systems, and these measures will facilitate the protection of the privacy and confidentiality of employees' personal data (Asiryan, 2023b). Thus the implementation of all recommendations in practice should reduce the probability of data security failures and guarantee the confidentiality of personal data in employment contracts.

2.2. International and EU standards on AI in labour relations

The growth of information in today's world has advanced significantly over the past few decades. AI is now widely used in many aspects of society, including labour relations. For example, in a dynamic workplace, hiring selection, employee performance analysis, and several company processes can be automated using the latest

information-processing techniques. However, these technologies also pose some challenges, such as protecting the privacy of personal information, in addition to their many benefits.

In light of the increasing use of AI in labour relations, protecting the privacy of personal data is an important issue that needs to be given more attention by legislatures, employers, and employees alike. AI makes possible the efficient management of personnel and the monitoring and forecasting of trends in the labour market, as well as the automation of many other important operations, thanks to its analytical and predictive capabilities. Algorithmic management, according to De Stefano (2019), alters traditional labour relations by transferring managerial authority to opaque digital systems. This leads to a structural imbalance and necessitates procedural labour safeguards that go beyond typical data protection standards. The development of technology not only simplifies the gathering and processing of personal information, which is widely applied in many industries, but can also become a tool for violating people's freedoms and rights (Yaroshenko et al., 2023). According to its definition, AI is a structured collection of information technologies that can be used to process information that is created on its own or acquired while working, as well as to create and apply one's own knowledge, decision-making models, information-processing algorithms, and task-solving techniques (Bielova & Byelov, 2023a).

Regarding international standards, it is essential to bring up the General Data Protection Regulation (European Parliament, 2016), the European Convention on Human Rights (Council of Europe, 1950), and the Universal Declaration of Human Rights (United Nations, 1948). For instance, the main goal of Article 8 of the Convention is to shield an individual from arbitrary interference with his or her home, communications, and private and family life. The European Court of Human Rights has established the state's procedural requirements in the context of this Article, which are crucial in establishing the bounds of a Member State's discretion. The decision-making process that leads to the intervention must thus be fair and such that it ensures due regard for the interests guaranteed to the individual under Article 8, even though this article does not contain any explicit procedural criteria, based on recognized prior practice (Havrylov, 2023).

It is crucial to distinguish between the laws of the European Union (such as the GDPR, the Artificial Intelligence Act, and the Platform Work Directive 2024) and the Council of Europe (such as the European Convention on Human Rights and Convention 108+ (Council of Europe, 2018)). While EU law becomes pertinent in the context of European integration and legal approximation, Ukraine is a member of the Council of Europe and is directly bound by its treaties (Asiryan, 2023a). General principles of lawful processing, openness, data minimization, and restrictions on fully automated decision-making are established by the GDPR inside the EU legal framework. These principles include the right to relevant information about the reasoning behind such choices. A risk-based approach is introduced by the Artificial

Intelligence Act, which also imposes stricter compliance requirements on some AI systems related to employment. Furthermore, algorithmic management is expressly covered by the Platform Work Directive, which calls for human oversight of important choices, the transparency of automated monitoring systems, and the ability to contest algorithmic results.

Protection of the right to privacy and legal use of personal information in the process of the training and work of AI has become an urgent problem that has to be solved by regulatory bodies in various countries. In addition to establishing guidelines for the gathering, use, and preservation of personal data inside the EU, the GDPR also sets strict privacy protection requirements (European Parliament, 2016). Because the respective data protection authorities (National Commission on Informatics and Liberty and Garante) have taken proactive stances on AI-related data protection issues, France and Italy can be presented as examples. Their actions show how EU regulations are implemented in practical situations. Both jurisdictions are appropriate case studies for illustrating how EU-level norms function in national legal systems because they have also produced useful guidelines and enforcement practices on algorithmic management in employment.

These national and international standards are therefore aimed at respecting the fundamental rights to personal privacy and data protection in the digital era. They establish frameworks to prevent the unauthorized collection and use of personal information and to monitor issues affecting people's privacy and confidentiality in the workplace and other areas of life. However, there are still issues with the actual implementation of protections in AI systems related to employment, especially in regard to algorithmic transparency, accountability, and efficient worker remedies, even with the GDPR and AI Act in place. Despite adopting a comprehensive legal framework, the EU is still in the early stages of institutional adaptation and enforcement when it comes to its actual use in employment contexts (Kaplina et al., 2023).

In June 2023, the European Parliament took a significant step towards creating legislation for the effective and ethical use of AI by approving the Artificial Intelligence Act. One of the primary objectives of the law is to safeguard rights against the impact of AI. The legislation sets rules and regulations for processing personal data using automated decision-making systems and other AI applications in order to guarantee the transparency, equity, and legality of data processing (Kariev, 2022). Its scope extends to all fields and forms of AI, except the military. This Act regulates the actions of companies that provide AI systems and those who use them for work purposes, although it primarily establishes obligations for providers and deployers rather than introducing new individual rights (Razmetaeva & Razmetaev, 2021).

The Artificial Intelligence Act also classifies AI use according to the possible level of risk. This classification consists of three key groups: prohibited practices, high-risk systems, and other AI technologies. It is forbidden to use AI to intentionally manipulate or abuse human weaknesses, which could lead to physical or psychological

harm. Law enforcement agencies are prohibited from using AI-generated social scoring systems to limit the rights of individuals or groups, as such practices are expressly banned under the Artificial Intelligence Act. However, certain uses of real-time biometric identification may be allowed under strictly defined conditions, including appropriate authorization and compliance with legal safeguards (Kronivets & Dorosh, 2024). The law defines high-risk systems as those that present a serious threat to human security or health. According to the requirements of the Artificial Intelligence Act, for particularly high-risk applications such as medical devices, the results of the supplier's self-audit must be verified by an authorized assessment body under relevant EU regulations (Prystai, 2023).

A broad approach to the Law on Artificial Intelligence was agreed by the European Council on 6 December 2022 (Pingen, 2023). Germany does not yet have any laws pertaining to autonomous AI, only current legislation and voluntary arrangements. One of the likely recommended steps is to require AI product makers, like OpenAI, the maker of ChatGPT, to disclose whether their system was trained using copyrighted content (Kolesnikov & Karapetian, 2023).

The law obliges Member States to establish their authorized bodies, as already noted. A conformity assessment is carried out to confirm whether AI systems meet the requirements enshrined in the Artificial Intelligence Act. This conformity assessment can be performed by a third party, i.e. an authorized organization, or independently, i.e. by an AI-system vendor who verifies the conformity itself. Audits can still be conducted by notified organizations to make sure the conformance assessment is completed accurately. According to critics, the current paradigm does not seem to necessitate third-party compliance reviews for many high-risk AI systems. This critique is based on the notion that in order to guarantee complete security, such systems need to be assessed by an unbiased third party (Bielova & Byelov, 2023b).

2.3. Regulation of AI use in labour relations in Ukraine and the European Union

Unlike Ukraine, the EU is developing a special set of legislative acts regulating AI as a technology in general and its application in labour relations, taking into account human rights risks. In this regard, the Artificial Intelligence Act establishes categories of AI risks and relevant requirements for developers and users. Along with this document, the GDPR is particularly strict in regulating the automated processing of personal data that directly affects employees (Table 1). Furthermore, particular guidelines for algorithmic management are introduced by Directive (EU) 2024 on platform work, which calls for human oversight of critical choices, openness in automated monitoring systems, and the right of employees to contest algorithmic conclusions and obtain explanations.

Table 1. Comparison of AI regulation in labour relations in Ukraine and the EU.

Aspect	Ukraine	EU
Legal framework	There is no special legislation on AI in labour relations. It is regulated by general labour law, the law on personal data protection, and information laws. Ethical and security issues are mostly addressed at the level of employers' internal policies.	Comprehensive legislation has been developed (Artificial Intelligence Act, GDPR). Ethical, legal, and security standards are taken into account.
AI in recruitment and personnel management	There are no special requirements for the transparency of algorithms, explanation of decisions, or appeal of decisions made by AI. There is protection of personal data, but control of algorithms is not regulated.	There is mandatory transparency, a right of employees to explain automated decisions, and the possibility of appeal. Conduct of risk audits, preventing discrimination.
AI application control and liability	The employer is liable under the general rules of labour and civil law. There are no special control bodies or audit procedures. Cybersecurity and ethics are mostly regulated by corporate policies.	Specialized control bodies have been introduced. The responsibilities of developers, users, and employers are defined. Mandatory audit and monitoring of AI systems.
Personal data protection	Regulated by the Law 'On Protection of Personal Data' (Verkhovna Rada of Ukraine, 2010), which partially complies with the GDPR but contains less detail on automated processing. Employees have general data protection rights.	The GDPR provides a high level of protection: strict requirements for automated processing, employee rights to access data, rectification, appeal, and the right to explain decisions.
Ethical and security requirements	Partially regulated by employers' internal policies; a lack of legislative provisions.	Legally enshrined requirements for ethics and safety, minimizing risks to employee rights.
Regulation level	Initial stage, lack of a coordinated approach, fragmentation of norms.	Well-developed legislation with clear requirements and continuously improving controls.

Source: Compiled by the author

As Table 1 shows, in Ukraine there are no specific regulatory requirements for the use of AI-based automated systems in the recruitment or management of personnel. This means that employers can use different technologies, but there are no requirements for transparency, explanations of AI decisions or the possibility to challenge such decisions. At the same time, employees have the right to personal data protection, but control over algorithms is not regulated. By contrast, in the EU such practices are strictly controlled. Thus the use of algorithms in recruitment must be transparent, and employees have the right to receive explanations for automated decisions (the right to an explanation). However, as Edwards and Veale (2017) and Wachter, Mittelstadt, and Floridi (2017) show, the GDPR establishes a restricted transparency framework rather than a fully developed individual right to explanation. Because automated choices have the potential to greatly impact workers' rights, this theoretical argument is especially pertinent to employment relations. Moreover, the law obliges employers to conduct risk assessments to avoid discrimination and

human rights violations. The GDPR imposes restrictions on automated decisions without human intervention.

Furthermore, in Ukraine control over AI use in labour relations is exercised by general mechanisms of labour and civil law. The responsibility lies with the employer, but there are no specialized control bodies or clear procedures for auditing algorithms. Cybersecurity and ethics issues are usually regulated by internal corporate standards that are not legally binding. In contrast, in the EU specialized control mechanisms are being created to audit AI systems and monitor compliance with security and ethical standards. The responsibility of employers, AI developers, and suppliers is defined to minimize risks for employees and society.

Personal data protection is key in the context of AI in labour relations, as AI is often based on the processing of large amounts of employees' data. In Ukraine personal data protection legislation has basic compliance with the GDPR but contains certain differences and a lower level of detail regarding automated data processing. This creates the risks of privacy violations and the inability to control algorithmic decision-making. In the EU the application of the GDPR is mandatory, which provides for high standards of transparency and control over the processing of personal information. Strict rules also apply to automated decisions that may affect employees. Employees have the right to information and access to it, and may challenge automated decisions (Edwards & Veale, 2017).

On the contrary, the regulation of AI use in labour in Ukraine is at an early stage. Currently, it is based on general labour law and personal data protection legislation, i.e. the Law of Ukraine no. 2297–VI 'On Protection of Personal Data' (Verkhovna Rada of Ukraine, 2010), with no specialized AI regulations. This creates certain risks related to the transparency of algorithms, employee rights, and control over AI. In the EU, a clear legal framework includes personal data protection and special requirements for AI use, including in labour relations. The emphasis is on minimizing risks, transparency, ethics, and ensuring control by the state and society.

3. The regulatory model for harmonizing AI use in labour relations

In response to the challenges linked to the integration of AI systems into labour, a model of multi-level regulation of AI use in labour relations in Ukraine is suggested. Its conceptual framework is based on a combination of national legislation and European law, in particular the GDPR and the principles enshrined in the Artificial Intelligence Act. The model is based on several key principles that should be implemented in the regulation of labour. First, the principle of legality stipulates that all processes of collecting, processing, and using employees' personal data using AI must have a legal basis. Moreover, the principle of proportionality means that the amount of information collected corresponds to the necessary purpose and does not violate the employee's

privacy. Apart from that, the principle of non-discrimination prohibits the use of algorithms that directly or indirectly create inequality between employees. In addition, the principle of transparency requires providing access to the logic of automated solutions, and data minimization means limiting their volume to what is necessary to perform job functions. The regulation should take into account all stages of labour relations, from hiring to dismissal. Table 2 illustrates this model of the implementation of legal restrictions and the procedures of AI use in labour at each stage.

Table 2. Model of multi-level regulation of AI use in labour relations.

Stage	Actions	Legal requirements
1. Recruitment	Automated CV selection, chatbots, candidate scoring	Obtaining informed consent of the applicant; prohibition of discrimination; algorithmic transparency
2. Performance evaluation	Work monitoring, behavioural and performance assessment	Employee's right to access data; limitation of information; technical guarantees
3. Decision-making	Appointment, dismissal, bonuses	Human control over automated decisions; the right to appeal
4. Termination of employment	Archiving and deletion of personal data	Regulated retention periods; requirement to destroy or anonymize data

Source: Compiled by the author

As demonstrated in Table 2, a specific function is attributed to the entities tasked with implementing and overseeing compliance within the context of the proposed model. The employer must ensure the transparency of data processing, develop personal information protection policies, and appoint a Data Protection Officer. Employees, in turn, have the right to be informed, access their data, correct it, and refuse processing or limit it to the extent permitted by law. At the same time, public authorities supervise and control the compliance of the applied AI systems with EU legal standards. In this regard, regulatory tools include contractual regulation (the inclusion of AI terms in employment contracts), an AI impact assessment before implementation of high-risk systems, algorithmic audits for bias or errors, and the creation of effective complaint mechanisms (Kaminski & Malgieri, 2021). It is also important to integrate Ukrainian legislation with the EU law on AI through the implementation of the GDPR, the Artificial Intelligence Act, and Convention 108+.

Another important component of the model is institutional support through the creation of specialized bodies, including the National Centre for Artificial Intelligence Ethics, which would act as an advisory and expert body in the formation of policy on the use of AI in the labour sphere. Such a centre could provide recommendations to employers, assess the risk level of specific solutions, and develop ethical standards of conduct for labour market participants. Thus the suggested model seeks to strike a balance between innovation in HR management and respect for employees' labour and personal rights. Its implementation will help harmonize regulation in

Ukraine with the EU standards, reduce the risks of human rights violations, and increase confidence in digital technologies in the labour market. Even before Ukraine joins the EU, the suggested approach may be progressively adopted. However, additional harmonization within the scope of European integration would be necessary for its complete realization. At the same time, the model allows the preservation of national legal traditions and the adaption of EU standards to Ukraine's digital and labour market realities.

Conclusions

The evolution of labour relations is now significantly influenced by artificial intelligence. Its incorporation into hiring procedures increases productivity but poses serious concerns about workers' rights and the security of personal information. According to this analysis, Ukrainian labour law does not yet have a thorough and specialized regulatory framework that is on a par with European norms. It is possible to classify Ukrainian labour law as normatively unprepared but partially institutionally ready. Although there are general data protection measures in place, there are no particular assurances about algorithmic transparency, human monitoring, or automated decision-making.

This analysis has shown a significant difference between the level of regulation of AI use in labour relations in Ukraine and the EU. From a doctrinal standpoint, there are no particular protections against algorithmic managerial authority in Ukrainian labour law, a problem that is frequently addressed in modern labour studies (De Stefano, 2019). Therefore regulatory readiness cannot be assessed solely through general data protection legislation. The EU has already created laws that protect employees' rights in the context of digitalization, ensure the transparency of algorithms, promote the ethical use of technologies, and provide effective control mechanisms. Meanwhile, in Ukraine, the legislation on AI is at an early stage of development and does not contain specialized rules governing the use of AI in the labour process.

Given the growing influence of digital technologies on the labour market, it is critical that Ukraine create legislation that includes the particulars of AI use in the workplace while also taking employee rights into consideration. The harmonization of Ukrainian legislation with European standards, such as the GDPR and the AI Act, will be a prerequisite for creating legal guarantees of transparency and the accountability of automated solutions. However, mechanisms for ethical assessments, risk audits, and control over the use of digital technologies in the labour sphere should be introduced. The adaptation of European experience to Ukrainian realities will thus strengthen the protection of workers' rights. In such a way, it will also promote the sustainable and responsible introduction of innovative technologies in the national labour market.

Suggested legislative actions include the following: a unique Ukrainian law for the application of AI to work relations should be adopted; high-risk systems must undergo AI impact assessments; to guarantee that automated choices are examined by a human, the Labour Code ought to be modified; it should be forbidden for dismissal decisions to be fully automated; a dedicated monitoring body for AI in the workplace should be created. These suggestions align with EU regulations regarding automated decision-making and algorithmic management in the workplace. Practically speaking, their implementation in Ukraine would necessitate changes to the Labour Code that would require algorithmic management systems to be transparent, would grant employees the right to human review of automated decisions, and would provide procedural safeguards that would enable workers to contest algorithmic results in labour courts.

Ukrainian labour laws should take into account the Platform Work Directive's specific requirements, which include human oversight of important choices, the transparency of automated monitoring and decision-making technologies, and efficient channels for contesting algorithmic results. Furthermore, the GDPR framework supports restrictions on purely automated judgments and upholds employees' rights to information and to challenge, while the AI Act views some employment-related AI systems as high-risk, which justifies the required AI impact studies and frequent algorithmic audits.

REFERENCES

- Asiryan, S. R. (2023a). Legislative practice of Singapore on the use of artificial intelligence. *Analytical and Comparative Jurisprudence*, 3, 313–317. <https://doi.org/10.24144/2788–6018.2023.03.57>
- Asiryan, S. R. (2023b). Steps of the EU countries in the direction of protecting the constitutional rights of citizens in the era of artificial intelligence. *Scientific Bulletin of Uzhhorod University: Series: Law*, 2(76), 285–290. <https://doi.org/10.24144/2307–3322.2022.76.2.45>
- Bielova, M. V., & Byelov, D. M. (2023a). Challenges and threats of personal data protection in working with artificial intelligence. *Scientific Bulletin of Uzhgorod University: Series: Law*, 2(79), 17–22. <https://doi.org/10.24144/2307–3322.2023.79.2.2>
- Bielova, M. V., & Byelov, D. M. (2023b). Implementation of artificial intelligence in pretrial investigation of criminal cases: International experience. *Analytical and Comparative Jurisprudence*, 2, 448–453. <https://doi.org/10.24144/2788–6018.2023.02.78>
- Bondarenko, S., Bratko, A., Antonov, V., Kolisnichenko, R., Hubanov, O., & Mysyk, A. (2022). Improving the state system of strategic planning of national security in the context of informatization of society. *Journal of Information Technology Management*, 14, 1–24. <https://doi.org/10.22059/jitm.2022.88861>
- Council of Europe. (1950). *Convention on the protection of human rights and fundamental freedoms*. https://www.echr.coe.int/documents/d/echr/convention_ENG

- Council of Europe. (2018). *Convention 108+. Convention for the protection of individuals with regard to the processing of personal data*. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
- De Stefano, V. (2019). *Negotiating the algorithm: Automation, artificial intelligence, and labour protection*. International Labour Organization. <https://www.ilo.org/publications/negotiating-algorithm-automation-artificial-intelligence-and-labour>
- Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke Law & Technology Review*, 16, 18–84. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855
- European Parliament. (2016). General Data Protection Regulation. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- European Parliament. (2024). 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). <http://data.europa.eu/eli/reg/2024/1689/oj>
- Getman, A. P., Yaroshenko, O. M., Sereda, O. H., Maliuha, L., & Zhygalkin, I. P. (2023). Social dialogue at the national and European levels as a factor in the formation of a common labor and social policy. *Society Register*, 7(3), 51–72. <https://doi.org/10.14746/sr.2023.7.3.04>
- Havrylov, M. V. (2023). Using artificial intelligence to detect malicious software in X in real time. In *Materials of the 11th Scientific and Technical Conference 'Information Models, Systems and Technologies' (Ternopil, 13–14 December 2023)* (pp. 7–27). Ternopil National Technical University.
- Kalina, I., Khurdei, V., Shevchuk, V., Vlasiuk, T., & Leonidov, I. (2022). Introduction of a corporate security risk management system: The experience of Poland. *Journal of Risk and Financial Management*, 15(8), article number 335. <https://doi.org/10.3390/jrfm15080335>
- Kaminski, M. E., & Malgieri, G. (2021). Algorithmic impact assessments under the GDPR. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3811067
- Kaplina, O., Tumanyants, A., Krytska, I., & Verkhoglyad-Gerasymenko, O. (2023). Application of artificial intelligence systems in criminal procedure: Key areas, basic legal principles and problems of correlation with fundamental human rights. *Access to Justice in Eastern Europe*, 6(3), 147–166. <https://doi.org/10.33327/AJEE-18-6.3-a000314>
- Kariev, I. Y. (2022). Protection of privacy when using cookies: Analysis of the state of legal regulation abroad. *Information and Law*, 3(42), 80–88. [https://doi.org/10.37750/2616-6798.2022.3\(42\).270239](https://doi.org/10.37750/2616-6798.2022.3(42).270239)
- Kolesnikov, A., & Karapetian, O. (2023). Artificial intelligence: Benefits and threats of use. *Efficient Economy*, 8, 1–13. <https://doi.org/10.32702/2307-2105.2023.8.9>
- Kronivets, T., & Dorosh, V. (2024). Ensuring the confidentiality of personal data in labor relations in connection with the spread of the use of artificial intelligence technologies. *Information and Law*, 1(48), 133–138. [https://doi.org/10.37750/2616-6798.2024.1\(48\).300797](https://doi.org/10.37750/2616-6798.2024.1(48).300797)
- Ministry of Digital Transformation of Ukraine. (2020). *Concept of artificial intelligence development*. <https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2023%2Fdata%2FpolicyInitiatives%2F99993318>

- Nikitenko, V., Voronkova, V., Tupakhina, O., & Sorokina, O. (2024). European practices of digital humanism in the context of global challenges. *Humanities Studies: Social Philosophy and Philosophy of History*, 18(95), 52–64. <https://doi.org/10.32782/hst-2024-18-95-06>
- Pingen, A. (2023). *Council's common position on Artificial Intelligence Act*. Eucrium. <https://eucrim.eu/news/councils-common-position-on-artificial-intelligence-act>
- Predmestnikov, O., & Yarmolyuk, O. (2023). Problems of human rights protection in the era of artificial intelligence and machine learning. *Scientific Collection 'InterConf'*, 156, 285–291. <https://archive.interconf.center/index.php/conference-proceeding/article/view/3486>
- Prystai, R. (2023). Privacy by design: User-held data model as a basis for privacy and personal data protection in social networks. *Scientific Bulletin of the Uzhhorod National University: Series: Law*, 80(1), 551–556. <https://doi.org/10.24144/2307-3322.2023.80.1.84>
- Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In M. Hildebrandt, C. Castillo, E. Celis, S. Ruggieri, L. Taylor, & G. Zanfir-Fortuna (Eds.), *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT*)* (pp. 33–44). ACM. <https://arxiv.org/abs/2001.00973>
- Razmetaeva, Y., & Razmetaev, S. (2021). Justice in the digital age: Technological solutions, hidden threats and enticing opportunities. *Access to Justice in Eastern Europe*, 2(10), 104–117. <https://doi.org/10.33327/AJEE-18-4.2-n000061>
- United Nations. (1948). *Universal declaration of human rights*. <https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf>
- Vavzhenchuk, S.Ya., & Zhmaka, V. O. (2024). Problems of protecting labor rights during hiring using artificial intelligence algorithms. *Problems of Legality*, 164, 19–38. <https://doi.org/10.21564/2414-990X.164.288964>
- Verkhovna Rada of Ukraine. (1971). *The labor code of Ukraine*. <https://zakon.rada.gov.ua/laws/show/322-08?lang=en#Text>
- Verkhovna Rada of Ukraine. (1984). *Кодекс України про адміністративні правопорушення*. <https://zakon.rada.gov.ua/laws/show/80731-10#Text>
- Verkhovna Rada of Ukraine. (1996). *The constitution of Ukraine*. <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80?lang=en#Text>
- Verkhovna Rada of Ukraine. (2003). *Цивільний кодекс України*. <https://zakon.rada.gov.ua/laws/show/435-15#Text>
- Verkhovna Rada of Ukraine. (2010). *Law of Ukraine no. 2297-VI 'On protection of personal data'*. <https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text>
- Vyshnevskiy, V. O. (2023). Personal data in data compilations (databases): Preserving the balance between the right to freedom of expression and the right to privacy. *Bulletin of the Kyiv University of Law*, 3, 136–141. <https://chasprava.com.ua/index.php/journal/article/download/972/908/>
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://academic.oup.com/idpl/article/7/2/76/3860948>

Yaroshenko, O. M., Lutsenko, O. Ye., Melnychuk, N. O., Mohilevskyi, L. V., & Vapnyarchuk, N. M. (2023). The impact of digitalization on labor relations in Ukraine. *InterEULawEast*, 10(1), 67–82. <https://doi.org/10.22598/iele.2023.10.1.4>