ISSN 2078-4503. Вісник Львівського університету. Серія юридична. 2026. Випуск 82. С. 182–192
Visnyk of the Lviv University. Series Law. 2026. Issue 82. P. 182–192

УДК 342.9:004.8:347.998.85

ARTIFICIAL INTELLIGENCE IN ADMINISTRATIVE PROCEEDINGS: RISK CLASSIFICATION, HUMAN OVERSIGHT, AND PROSPECTS FOR IMPLEMENTATION IN UKRAINE

Halyna Zabolotna

Ivan Franko National University of Lviv,
1, Universytetska Str., Lviv, Ukraine, 79000,
e-mail: halyna.zabolotna@lnu.edu.ua
ORCID ID: 0000-0003-1027-0680

The article examines the legal framework for the use of artificial intelligence in administrative proceedings, emphasizing the significance of risk classification for effective regulation. The EU AI Act distinguishes between prohibited, high-risk, transparency-risk, and minimal-risk AI systems. AI tools designed to support judicial decision-making are generally classified as high-risk due to their potential effects on fundamental rights, procedural fairness, and legal certainty. The article analyzes the principal legal requirements for such systems, including risk management, data governance, technical documentation, transparency, human oversight, and cybersecurity.

The issue of human oversight in the judicial context receives particular attention. Although judges may formally participate in human oversight mechanisms, they should not hold primary or exclusive responsibility for monitoring high-risk AI systems. Article 14(4) of the EU AI Act requires a degree of technical competence and operational control that cannot reasonably be expected from judges. Consequently, a more balanced model is proposed in which judges retain responsibility for legal assessment and final decisions, while technical experts and court administration assume responsibility for system-level supervision and operational control.

The article further explores the potential integration of AI into Ukraine's administrative proceedings via the Unified Judicial Information and Telecommunication System. Should Ukraine enact legislation similar to the EU AI Act, the legal status of the State Judicial Administration of Ukraine will depend on the development and implementation of relevant AI modules, potentially qualifying it as either a provider or a deployer. The article concludes that any future Ukrainian model for AI use in administrative proceedings should ensure clear role allocation, risk-based differentiated regulation, and a realistic assessment of the limits of judicial involvement in technical oversight.

***Keywords*:** administrative proceedings; judge; high-risk AI systems; Unified Judicial Information and Telecommunication System; administrative justice; judicial digitalization.

DOI: http://dx.doi.org/10.30970/vla.2026.82.182

Introduction. The rapid development of Artificial Intelligence (AI) technologies has become a central feature of digital transformation, significantly affecting various sectors of public life, including the justice system. Within contemporary digital society, the implementation of AI is widely recognized as a key mechanism for enhancing the efficiency and objectivity of judicial processes, reducing procedural delays, and mitigating corruption risks. In Ukraine, the digitalization of administrative proceedings holds particular importance due to its connection with the need to ensure consistent judicial practice and to meet the country's European integration commitments. However, the integration of AI into the judiciary presents complex legal and ethical challenges,

particularly regarding procedural fairness, the protection of fundamental rights, and the preservation of substantive human oversight in judicial decision-making.

State of Research. In the international legal doctrine and the framework of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (hereinafter referred to as the EU AI Act) [1], the discourse on "trustworthy AI" and the implementation of risk-based regulation has been shaped by a multidisciplinary group of scholars. Much of the literature addresses risk assessment methodologies, as examined by C. Novelli, F. Casolari, A. Rotolo, M. Taddeo, L. Floridi [2], [3], Jonas Schuett [4], H. Fraser, J-M. Bello y Villarino [5], Cornelia Kutterer [6], Martin Ebers [7], Tiago Sérgio Cabral [8], among others. Isabel Kusche explores the sociological implications of conceptualizing potential harms as risks to fundamental rights, identifying communicative paradoxes in the EU's efforts to establish trustworthiness through legal standards [9].

Technical and industrial challenges related to compliance are documented in the works of M. Wagner, Q. Song, M. Borg [10], Isabella Banks [11], A. Buscemi, T. Deckenbrunnen, K. Mishchenko [12], and others. Despite the breadth of international scholarship, the practical application of these doctrines continues to be debated as global standard-setting bodies seek to bridge the gap between abstract legal norms and technical realities.

Within Ukrainian legal scholarship, the digitalization of justice and the role of artificial intelligence in administrative proceedings have been examined by numerous researchers, including O. Barabash [13], Y. Bernazyuk [14], M. Bielikova [15], V. Krat [16], M. Vasylenko, V. Slatvinska [17], I. Mishchenko [18], T. Proskurnia [19], N. Ilchyshyn [20], L. Kovalenko, M. Soloninka [21], O. Melnyk, I. Yurko [22], among others. Nevertheless, the legal status of AI in Ukraine remains fragmented and requires a more comprehensive regulatory framework to align with international standards.

The purpose of this article is to analyze the legal framework governing the use of artificial intelligence in administrative proceedings, with particular emphasis on the risk-based approach of the EU AI Act, the classification of judicial AI systems as high-risk, and the issue of human oversight in their application. Additionally, the article evaluates the prospects for future implementation of AI regulation in Ukraine, taking into account both European experience and the institutional characteristics of the Ukrainian judicial system.

Results and Discussion. In December 2020, the Cabinet of Ministers of Ukraine approved the Concept for the Development of Artificial Intelligence [23], which outlines limited tasks concerning the prospective use of AI in the justice sector. On 26 June 2024, the Ministry of Digital Transformation of Ukraine introduced *the White Paper on AI Regulation in Ukraine* [24]. This policy document recommends that Ukraine develop and adopt legislation broadly modeled on the EU AI Act [1], while deferring the implementation of certain AI-related provisions, particularly those that impose obligations on relevant stakeholders. Instead of an immediate, comprehensive, mandatory regime, the White Paper advocates a phased approach to AI regulation.

Under this approach, Ukraine would initially rely on non-legislative instruments and soft-law initiatives during a transitional period, and adopt a specialized legislative act on artificial intelligence only at a later stage. Accordingly, the proposed regulatory model consists of two phases: a preparatory phase focused on building institutional, legal, and practical readiness, followed by a phase dedicated to adopting and implementing legislation analogous to the EU AI Act.

Given Ukraine's intention to implement a legislative framework analogous to the EU AI Act, a thorough and critical assessment of this regulatory model is essential. This evaluation is warranted not only because the EU AI Act represents the first comprehensive legal instrument of its kind, but also due to the ongoing development of its practical application within the European Union. For Ukraine, the challenge extends beyond formal alignment with EU law and necessitates a nuanced understanding of the model's practical functioning, the challenges encountered during implementation, and the identification of elements that may require adaptation.

The EU AI Act is based on a risk-based regulatory approach, under which AI systems may be broadly divided into four categories based on the level and nature of the risk posed to individuals, society, and fundamental rights. These categories include prohibited AI practices, high-risk AI systems, AI systems presenting systemic (limited) risks, and low-risk or minimal-risk AI systems [3, c. 2493], [5, c. 1]. Cornelia Kutterer observes that, while the regulation of advanced AI models maintains a risk-based approach, it remains complex and uncertain, particularly in identifying specific risks, establishing benchmarks, and clarifying the roles of standards and codes of conduct [6, c. 13].

Isabel Kusche argues that the EU AI Act's risk-based approach, predicated on AI's potential to harm fundamental rights, introduces conceptual challenges. The framework simultaneously treats fundamental rights as legal principles, political values, and a foundation for trust in AI, resulting in ambiguity and occasional circularity. Kusche further suggests that, although the EU AI Act will impose substantive obligations on companies and yield practical effects, it may fall short of its primary objective of clearly identifying and managing AI risks. Instead, the Act is likely to increase reliance on legal and political judgments in individual cases, leaving many decisions subject to interpretation, value conflicts, and power dynamics rather than objective risk assessment [9, c. 10–11].

The EU AI Act establishes unacceptable risk as its most restrictive category, resulting in the prohibition of certain AI practices (art. 5) [1]. This category encompasses uses of AI that are incompatible with fundamental rights and freedoms. In the public sector, particularly in administrative proceedings, this category is highly relevant. For instance, it includes social scoring by public authorities or other entities based on an individual's behaviour or irrelevant personal data, which is subsequently used to justify restrictions or adverse treatment. Another prohibited practice involves the untargeted collection of facial images from the internet or CCTV footage to create or expand facial recognition databases. These examples demonstrate that, under the EU AI Act, certain practices are deemed unacceptable not because of potential algorithmic inaccuracy, but because even highly accurate systems could facilitate state or institutional actions that violate fundamental rights standards.

The second category under the EU AI Act is high-risk AI systems (chapter III, Art 6-49). These systems may be placed on the market or used only if they meet stringent legal and technical requirements. In the administration of justice, this category is especially significant. Annex III of the EU AI Act specifically includes high-risk AI systems intended for use by judicial authorities, or on their behalf, to assist in researching and interpreting facts and law, as well as applying the law to specific cases. Consequently, AI tools that support adjudicative or quasi-adjudicative functions are generally classified as high-risk due to their potential effects on procedural fairness, legal certainty, and the safeguarding of fundamental rights.

Examples relevant to the judiciary include AI tools that analyze case materials and generate recommendations regarding legal classification, applicable rules, evidentiary

structures, or likely conclusions. Additionally, this category encompasses outcome-prediction systems that estimate the probable outcome of a case, the likelihood that a claim will be upheld, or the expected amount of recovery, particularly when such outputs inform judicial assessments of facts and law. Accordingly, AI systems involved in decision-making or decision prediction should be classified as high-risk.

Recital 61 of the EU AI Act states that AI tools may support judicial decision-making or reinforce judicial independence, but must not replace human judgment; final decisions must remain human-driven [1]. Consequently, any AI tool deployed in the judicial context should be designed so that judges can clearly understand its function, purpose, and the meaning of its outputs. The system should not operate as a "black box" whose recommendations cannot be interpreted or critically assessed by the judge. Only when the logic, limitations, and practical significance of the system's operation are sufficiently transparent can judges exercise genuine control over its use and maintain independent judicial reasoning.

The EU AI Act establishes strict obligations for high-risk AI systems. These obligations include risk management throughout the system's lifecycle, requirements for data quality and data governance, technical documentation, logging and traceability, and the provision of adequate information and transparency to users or deployers. The Act further mandates human oversight and sufficient levels of accuracy, robustness, and cybersecurity. Collectively, these safeguards demonstrate the EU's position that AI may be used in sensitive domains such as judicial decision-support only within a comprehensive framework of legal and technical guarantees.

Given the requirements for high-risk AI systems, a judge, as a potential user, might be positioned primarily within the domain of human oversight. This prompts the question of whether a judge should be solely responsible for overseeing such systems. According to Isabella Banks, while judges may formally appear in the human oversight chain, they should not be expected to serve as the sole overseers of high-risk judicial decision-support systems. Banks contends that the scope of oversight is too extensive for judges alone, as many associated risks require broader structural and institutional measures beyond the capacity of individual judges. She therefore advocates for shared oversight responsibilities between judges and technical experts. In this model, judges retain authority over the decision-making process but do not bear exclusive responsibility for monitoring and controlling the AI system [11, 20].

In my view, judges should not bear primary responsibility for the human oversight of AI systems in use. Although Article 14(4) of the EU AI Act formally outlines the capacities required of a human overseer, these requirements assume a level of technical understanding and operational control that a judge cannot reasonably be expected to possess. Judges are neither appointed nor trained to master the technical architecture, performance limitations, anomalies, or dysfunctions of complex AI tools. The judicial office should not be transformed into a hybrid technical-supervisory role.

This is particularly evident in the requirements set out in Article 14(4). The individual responsible for oversight must be able to understand the system's capacities and limitations, detect anomalies and unexpected performance, remain vigilant regarding automation bias, accurately interpret outputs using available methods and tools, determine when to override or refrain from using the system, and, if necessary, intervene in or halt its operation. These responsibilities extend beyond procedural or legal tasks and demand technical literacy, operational familiarity, and institutional support. Assigning this burden solely to judges is unrealistic and risks creating an accountability gap, where

responsibility for AI-related failures is shifted to the judicial user rather than being shared with providers and deployers.

Accordingly, judges should remain responsible for legal assessment and the final court decision, but not for the full scope of human oversight in the technical sense described in Article 14(4). A more balanced approach would assign oversight responsibilities to technical experts and the court administration, who would ensure the system's safe and reliable operation. Judges would retain the authority to disregard, override, or refuse to rely on AI outputs in specific cases.

Recent empirical research demonstrates that, from an industry perspective, the most challenging obligations under the EU AI Act for high-risk AI systems relate to data quality and governance (Art 10), accuracy, robustness, and cybersecurity (Art 15), risk and quality management systems (Art 9, 17), and transparency (Art 13) [10, c. 108067]. The participating companies in that study did not identify human oversight as a particularly difficult requirement to operationalize. The authors explicitly note that no votes were attributed to the human oversight requirement as being especially challenging [10]. The study attributes this to the fact that the human–machine interface tools used by respondent companies were highly product-dependent, and interviewees generally expressed confidence in the interfaces already implemented within their organizations.

Administrative proceedings may involve not only high-risk AI systems but also the integration of lower-risk AI services. The EU AI Act differentiates among AI applications in the judicial sphere based on the function performed and the level of risk posed to fundamental rights, procedural fairness, and legal decision-making.

Certain AI tools used in court administration or in communication with court users may be classified as limited-risk or transparency-risk AI. Although the EU AI Act does not formally define “limited-risk systems,” Article 50 imposes specific transparency obligations in defined situations, such as human interaction with AI systems, synthetic content, deepfakes, emotion recognition, and biometric categorisation. In administrative justice, this may include a chatbot on a court website that provides citizens with procedural information regarding claim filing, court fees, or stages of proceedings. In these cases, individuals must be clearly informed that they are interacting with an AI system, unless the context makes this evident. Similar transparency obligations apply when AI is used to generate or modify synthetic audio or video content, or when voice assistants are employed to receive calls, process requests, or arrange appointments within courts or public service centres.

Certain AI applications used within judicial infrastructure are generally considered to pose minimal risk and, as such, typically do not trigger additional specific obligations under the EU AI Act beyond the general requirements of other applicable legal regimes, such as data protection law. In administrative proceedings, these tools may include optical character recognition (OCR) systems for scanned documents, automated file sorting, technical routing of correspondence, spell-checking or formatting tools for drafts, and internal cybersecurity or anti-spam filters for court networks and email systems. These systems can enhance the technical efficiency of judicial administration without directly influencing the assessment of facts, the interpretation of law, or the outcome of cases.

In Ukraine, the Unified Judicial Information and Telecommunication System (UJITS) functions as an organisational and technical system comprising interconnected modules. These modules automate judicial processes, including document management, automated case allocation, document exchange between courts and parties, recording of court proceedings, participation in hearings via videoconference, preparation of

operational and analytical reports, and provision of informational support to judges. In this context, integrating AI systems into administrative proceedings would most logically involve supplementing existing modules with AI-based functions or introducing new dedicated modules. Such modules could include AI tools for processing and analysing evidence, structuring case materials, or preparing draft judicial decisions.

The State Judicial Administration of Ukraine (SJA) is responsible for the organisational and financial support required for the creation and functioning of individual subsystems and modules of UJITS, as well as for their proper operation and information security. If high-risk AI modules are introduced into the system of administrative justice, the legal status of the SJA under the AI regulatory framework will depend on how the relevant software is developed and implemented. When the SJA commissions or controls the development of such software and deploys it under its own authority, it may be classified as a provider. Conversely, if an external entity develops the AI system and the SJA primarily integrates and uses it within ESITS, its role may align more closely with that of a deployer. This distinction is significant because the scope of legal obligations, including those related to conformity, oversight, documentation, and accountability, will depend on the precise allocation of these roles.

If Ukraine were to enact legislation similar to the EU AI Act, and the SJA were designated as a provider of a high-risk AI system within the judicial infrastructure, it would be subject to a comprehensive set of legal obligations. The SJA would be required to ensure that the system meets all substantive requirements for high-risk AI systems, including risk management (Art. 9), data and data governance (Art. 10), technical documentation (Art. 11), record-keeping and logging (Art. 12), transparency and information provision to deployers (Art. 13), human oversight (Art. 14), and standards for accuracy, robustness, and cybersecurity (Art. 15). Additionally, the provider would need to establish and maintain a quality management system encompassing compliance strategies, design control, testing, change management, and post-market monitoring (Art. 17).

Moreover, as a provider, the SJA would be obligated to prepare the required technical documentation and implement appropriate logging and traceability mechanisms to demonstrate compliance (Arts. 11–12). Prior to placing the system on the market or putting it into service, the provider must complete the relevant conformity assessment procedure (Art. 43). If the necessary conditions are satisfied, the provider must issue an EU declaration of conformity (Art. 47) and apply the CE marking (Art. 48). Where registration is mandated, the provider must also register the high-risk AI system in the EU database (Art. 49).

The provider's responsibilities extend beyond the system's deployment. If a high-risk AI system is determined to be non-compliant with the Regulation, the provider must implement corrective actions, which may include achieving conformity, withdrawal, disabling, or recall of the system (Art. 20). The provider is also required to cooperate with competent authorities by supplying all necessary information and documentation to demonstrate compliance (Art. 21). Furthermore, the provider must establish a post-market monitoring system based on a monitoring plan included in the technical documentation (Art. 72) and report any serious incidents or malfunctions that could constitute a breach of obligations under the Regulation (Art. 73).

Conclusions. The analysis demonstrates that integrating artificial intelligence into administrative proceedings should not be regarded solely as technological modernization. Under the EU AI Act, AI systems that participate in or influence judicial decisions must be assessed according to the risks they present to fundamental rights, procedural fairness, and judicial independence. High-risk AI systems, which include tools designed to assist

judicial authorities in interpreting facts and law and applying legal norms to specific cases, represent the most sensitive category. In contrast, administrative justice may also use lower-risk AI services, such as chatbots, optical character recognition tools, or technical routing systems, which require a distinct, more proportionate regulatory approach.

A principal finding is that, although judges may formally be included within the framework of human oversight, they should not bear primary or exclusive responsibility for supervising high-risk AI systems. The obligations set out in Article 14(4) of the EU AI Act require technical expertise, operational monitoring, and institutional control that cannot reasonably be expected of judges. Judicial responsibility should therefore remain centered on legal assessment and the final human decision, while technical oversight and system-level supervision should be allocated to specialized experts and court administration. This division of responsibilities preserves the human-centered character of adjudication and upholds the integrity of the judicial system.

From the Ukrainian perspective, implementing legislation analogous to the EU AI Act will require not only formal legal reforms but also comprehensive institutional planning. As AI systems are likely to be integrated into the existing Unified Judicial Information and Telecommunication System, the role of the State Judicial Administration of Ukraine becomes particularly significant. Depending on the development and deployment of AI modules, the State Judicial Administration may assume the status of either provider or deployer, which will directly determine its legal obligations. Consequently, any future Ukrainian framework for AI use in administrative justice should be based on a clear allocation of roles, risk-based differentiated regulation, and a realistic assessment of the limits of judicial involvement in technical oversight.

Список використаних джерел

1 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення: 29.03.2026).

2 AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act [Electronic resource] / Claudio Novelli [et al.]. *Digital Society*. 2024. Vol. 3. No. 1. DOI: https://doi.org/10.1007/s44206-024-00095-1 (date of access: 29.03.2026).

3 Taking AI risks seriously: a new assessment model for the AI Act / Claudio Novelli [et al.]. *AI & SOCIETY*. 2023. DOI: https://doi.org/10.1007/s00146-023-01723-z (date of access: 29.03.2026).

4 Schuett J. Risk Management in the Artificial Intelligence Act. *European Journal of Risk Regulation.* 2023. P. 1–19. DOI: https://doi.org/10.1017/err.2023.1 (date of access: 30.03.2026).

5 Fraser H., José-Miguel Bello y Villarino. Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough. *European Journal of Risk Regulation.* 2023. P. 1–16. DOI: https://doi.org/10.1017/err.2023.57 (date of access: 30.03.2026).

6 Kutterer C. Regulating Foundation Models in the AI Act: From «High» to «Systemic» Risk. *AI-Regulation Papers.* 2024. P. 14. URL: https://ai-regulation.com/regulating-foundation-models- in-the-ai-act-from-high-to-systemic-risk/.

7 Ebers M. Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act. *European Journal of Risk Regulation.* 2024. P. 1–20. DOI: https://doi.org/ 10.1017/err.2024.78 (date of access: 30.03.2026).

8 Cabral T. S. Rethinking the List-Based Approach to High-Risk Systems under the AI Act. *SSRN Electronic Journal*. 2025. DOI: https://doi.org/10.2139/ssrn.5206860 (date of access: 30.03.2026).

9 Kusche I. Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk. *Journal of Risk Research*. 2024. P. 1–14. DOI: https://doi.org/10.1080/13669877.2024.2350720 (date of access: 29.03.2026).

10 AI Act high-risk AI Compliance challenge and industry impact: A multiple case study. *Information and Software Technology*. 2026. P. 108067. DOI: https://doi.org/10.1016/j.infsof.2026.108067 (date of access: 29.03.2026).

11 Banks I. Judges-in-the-loop? Judicial involvement in human oversight of high-risk decision support systems under the EU AI Act. ArXiv. *International Journal of Law and Information Technology*. 2026. Vol. 34. No. 1. P. 1–22.

12 Assessing High-Risk AI Systems under the EU AI Act: From Legal Requirements to Technical Verification [Electronic resource] / Alessio Buscemi [et al.]. *Computers and Society*. DOI: https://doi.org/10.48550/arXiv.2512.13907 (date of access: 30.03.2026).

13 Барабаш О. О. Цифровізація правосуддя у контексті впровадження системи е-суд: виклики та завдання. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2023. № 1. С. 57–66. DOI: https://doi.org/10.32782/2311-8040/2023-1-8 (дата звернення: 30.03.2026).

14 Берназюк Я. Штучний інтелект і його використання для забезпечення єдності судової практики як складової довіри до суду. *Слово Національної школи суддів України*. 2024. № 4 (49). С. 16–35.

15 Бєлікова М. Штучний інтелект в адміністративному судочинстві. *Наука і техніка сьогодні*. 2024. № 12(40). DOI: https://doi.org/10.52058/2786-6025-2024-12(40)-44-52 (дата звернення: 30.03.2026).

16 Крат В. Довіра суспільства до судової влади втрачається швидко, а здобувається важко. URL: https://supreme.court.gov.ua/supreme/pres-centr/zmi/961750 (дата звернення: 30.03.2026).

17 Василенко М., Слатвінська В. Штучний інтелект в судовій практиці: особливості та його можливості (міжгалузеве дослідження). *Право і суспільство*. 2022. Т. 4. С. 271–278. DOI: https://doi.org/10.32842/2078-3736/2022.4.39 (дата звернення: 30.03.2026).

18 Міщенко І. Якісних рішень та єдності практики можна досягти лише діджиталізувавши суди. URL: https://supreme.court.gov.ua/supreme/pres-centr/zmi/838768 (дата звернення: 30.03.2026).

19 Проскурня Т. Єдність судової практики в умовах розвитку штучного інтелекту. *Право і суспільство*. Т. 2. № 2024. С. 149–154. DOI: https://doi.org/10.32842/2078-3736/2024.2.19 (дата звернення: 30.03.2026).

20 Ільчишин Н. Роль штучного інтелекту в адміністративному судочинстві україни: виклики цифрової держави. *Науковий вісник Ужгородського Національного Університету*. 2025. Т. 4. № 88. С. 245–253. DOI: https://doi.org/10.24144/2307-3322.2025.88.4.36 (дата звернення: 30.03.2026).

21 Коваленко Л., Солонінка М. Використання штучного інтелекту при оформленні адміністративного акта: переваги та ризики. *Слово Національної школи суддів України*. 2024. № 4 (49). С. 85–94. DOI: https://doi.org/10.37566/2707-6849-2024-4(49)-7 (дата звернення: 30.03.2026).

22 Мельник О., Юрко І. Застосування штучного інтелекту у здійсненні адміністративного судочинства: аналіз правового регулювання, ризики та перспективи. *Адміністративне право і процес*. 2025. № 3. С. 58–79. DOI: https://doi.org/10.32782/2227-796X.2025.3.05 (дата звернення: 30.03.2026).

23 Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text (дата звернення: 22.11.2025).

24 Біла книга з регулювання ШІ в Україні: бачення Мінцифри. URL: https://storage.thedigital.gov.ua/files/a/ba/d5da75c2613e331bb89258f950adcbae.pdf (дата звернення: 22.11.2025).

References

1. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence*. Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
2. Novelli, C. F., Rotolo, A., Taddeo, M., & Floridi, L. (2024). AI risk assessment: A scenario-based, proportional Casolari methodology for the AI act. *Digital Society*, *3*(1). DOI: https://doi.org/10.1007/s44206-024-00095-1.
3. Novelli, C., Casolari, F., Rotolo, A., Taddeo, M., & Floridi, L. (2023). Taking AI risks seriously: A new assessment model for the AI Act. *Ai & society*. DOI: https://doi.org/10.1007/s00146-023-01723-z.
4. Schuett, J. (2023). Risk management in the artificial intelligence act. *European Journal of Risk Regulation*, 1–19. DOI: https://doi.org/10.1017/err.2023.1.
5. Fraser, H., & Bello y Villarino, J.-M. (2023). Acceptable risks in Europe's proposed AI act: reasonableness and other principles for deciding how much risk management is enough. *European Journal of Risk Regulation*, 1–16. DOI: https://doi.org/10.1017/err.2023.57.
6. Kutterer, C. (2024). Regulating foundation models in the AI act: From «high» to «systemic» risk. *AI-Regulation Papers*, 14. Retrieved from https://ai-regulation.com/regulating-foundation-models-in-the-ai-act-from-high-to-systemic-risk/.
7. Ebers, M. (2024). Truly risk-based regulation of artificial intelligence how to implement the EU's AI act. *European Journal of Risk Regulation*, 1–20. DOI: https://doi.org/10.1017 err.2024.78.
8. Cabral, T. S. (2025). Rethinking the List-Based Approach to High-Risk Systems under the AI Act. *SSRN Electronic Journal*. DOI: https://doi.org/10.2139/ssrn.5206860.
9. Kusche, I. (2024). Possible harms of artificial intelligence and the EU AI act: Fundamental rights and risk. *Journal of Risk Research*, 1–14. DOI: https://doi.org/10.1080/13669877.2024.2350720.
10. Wagner, M., Song, Q., Borg, M., Engström, E., & Lysek, M. (2026). AI Act high-risk AI Compliance challenge and industry impact: A multiple case study. *Information and Software Technology*, 108067. DOI: https://doi.org/10.1016/j.infsof.2026.108067.
11. Banks, I. (2026). Judges-in-the-loop? Judicial involvement in human oversight of high-risk decision support systems under the EU AI Act. *International Journal of Law and Information Technology*, *34*(1), 1–22.
12. Buscemi, A., Deckenbrunnen, T., Kabir, F., Mishchenko, K., & Mowla, N. (б. д.). Assessing high-risk AI systems under the EU AI act: From legal requirements to technical verification. *ArXiv. Computers and Society*. DOI: https://doi.org/10.48550/arXiv.2512.13907.
13. Barabash, O. O. (2023). Tsyfrovizatsiia pravosuddia u konteksti vprovadzhennia systemy e-sud: vyklyky ta zavdannia. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav (seriia yurydychna).* (1), 57–66. DOI: https://doi.org/10.32782/2311-8040/2023-1-8.
14. Bernaziuk, Ya. (2024). Shtuchnyi intelekt i yoho vykorystannia dlia zabezpechennia yednosti sudovoi praktyky yak skladovoi doviry do sudu. *Slovo Natsionalnoi shkoly suddiv Ukrainy*, (4 (49)), 16–35.

15. Bielikova, M. (2024). Shtuchnyi intelekt v administratyvnomu sudochynstvi. *Nauka i tekhnika sohodni*, (12(40)). DOI: https://doi.org/10.52058/2786-6025-2024-12(40)-44-52.
16. Krat, V. (2020). *Dovira suspilstva do sudovoi vlady vtrachaietsia shvydko, a zdobuvaietsia vazhko.* Retrieved from https://supreme.court.gov.ua/. https://supreme.court.gov.ua/supreme/pres-centr/zmi/961750.
17. Vasylenko, M. D., & Slatvinska, V. M. (2022). Artificial intelligence in judicial practice: Features and it's capabilities (intersectoral research). *Law and Society*, (4), 271–278. DOI: https://doi.org/10.32842/2078-3736/2022.4.39.
18. Mishchenko, I. (2019). *Yakisnykh rishen ta yednosti praktyky mozhna dosiahty lyshe didzhytalizuvavshy sudy*. Retrieved from https://supreme.court.gov.ua/. https://supreme. court. gov.ua/ supreme/ pres-centr/zmi/838768.
19. Proskurnya, T. V. (2024). Unity of judicial practice in the development of artificial intelligence. *Law and Society*, (2), 149–154. DOI: https://doi.org/10.32842/2078-3736/2024.2.19.
20. Ilchyshyn, N. V. (2025). The role of artificial intelligence in administrative proceedings in Ukraine: challenges of the digital state. *Uzhhorod National University Herald. Series: Law*, *4*(88), 245–253. DOI: https://doi.org/10.24144/2307-3322.2025.88.4.36.
21. Kovalenko, L., & Soloninka, M. (2025). The use of artificial intelligence in the preparation of an administrative act: Benefits and risks. *Slovo of the National School of Judges of Ukraine*, (4(49)), 85–94. DOI: https://doi.org/10.37566/2707-6849-2024-4(49)-7.
22. Melnyk, O., & Yurko, I. (2025). Artificial intelligence application in administrative judicial proceedings: Analysis of legal regulation, risks and perspectives. *Administrative Law and Process*, (3), 58–79. DOI: https://doi.org/10.32782/2227-796x.2025.3.05.
23. *Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini: Rozporiadzhennia Kabinetu Ministriv Ukrainy 02.12.2020 № 1556-p.* URL: https:// zakon.rada.gov.ua/laws/show/ 1556-2020-p#Text.
24. *Bila knyha z rehuliuvannia ShI v Ukraini: bachennia Mintsyfry*. Retrieved from https:// storage.thedigital.gov.ua/files/a/ba/d5da75c2613e331bb89258f950adcbae.pdf.

ШТУЧНИЙ ІНТЕЛЕКТ В АДМІНІСТРАТИВНОМУ СУДОЧИНСТВІ: КЛАСИФІКАЦІЯ РИЗИКІВ, ЛЮДСЬКИЙ НАГЛЯД ТА ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ В УКРАЇНІ

Галина Заболотна

Львівський національний університет імені Івана Франка,
вул. Університетська, 1, Львів, Україна, 79000,
e-mail: halyna.zabolotna@lnu.edu.ua
ORCID ID: 0000-0003-1027-0680

Присвячено аналізу правових засад використання штучного інтелекту в адміністративному судочинстві з урахуванням положень Регламенту Європейського Союзу 2024/1689 про штучний інтелект та перспективи упровадження подібного правового регулювання в Україні. Актуальність теми зумовлена активною цифровізацією правосуддя, розвитком інструментів штучного інтелекту та наміром України гармонізувати національне законодавство з європейськими підходами до регулювання цієї сфери. У статті вихідним є положення про те, що інтеграція штучного інтелекту в судову діяльність не може розглядатися виключно як технічне оновлення, оскільки вона безпосередньо зачіпає основоположні права людини, принципи справедливого суду, правової визначеності та незалежності судді.

Охарактеризовано ризик – орієнтований підхід Регламенту Європейського Союзу про штучний інтелект, відповідно до якого системи штучного інтелекту поділяються на заборонені практики, високоризикові системи, системи з обмеженим ризиком і системи

мінімального ризику. Обґрунтовано, що системи, призначені для використання судовими органами з метою дослідження і тлумачення фактів та права, а також застосування права до конкретних обставин справи, мають кваліфікуватися як високоризикові. До таких систем можуть належати засоби аналізу матеріалів справи, прогнозування можливого результату спору, оцінки ймовірності задоволення позову чи формування проєктів судових рішень. Водночас у сфері адміністративного судочинства можуть використовуватися і системи нижчого рівня ризику, зокрема електронні помічники для надання інформації учасникам процесу, засоби розпізнавання тексту, інструменти технічного розподілу документів, перевірки правопису та захисту судових мереж від небажаних повідомлень.

Окрему увагу приділено змісту обов'язків, які європейський регламент покладає на осіб, що створюють, впроваджують і використовують високоризикові системи. Проаналізовано вимоги щодо управління ризиками протягом усього строку функціонування системи, належної якості даних, технічної документації, фіксації дій системи, прозорості, людського нагляду, точності, стійкості та кіберзахисту. На підставі наукових джерел і положень регламенту доведено, що вимога людського нагляду в судовій сфері не повинна тлумачитися як покладення повної відповідальності за нагляд за системою на суддю. Аргументовано, що суддя має зберігати вирішальну роль у правовій оцінці обставин і в ухваленні остаточного рішення, однак не повинен нести виключну відповідальність за технічний контроль за функціонуванням системи штучного інтелекту. Таке твердження обґрунтовано тим, що європейський підхід вимагає від особи, яка здійснює нагляд, розуміння технічних можливостей і меж системи, здатності виявляти аномалії, враховувати схильність до надмірної довіри до автоматично сформованих результатів, належно їх тлумачити та, за потреби, зупиняти роботу системи. Зроблено висновок, що ці вимоги передбачають такий рівень технічної підготовки та інституційної підтримки, який не може розумно очікуватися від судді як носія судової влади.

Також досліджено український контекст. Розглянуто Концепцію розвитку штучного інтелекту, Білу книгу з регулювання штучного інтелекту в Україні та можливість майбутнього прийняття закону, подібного до європейського регламенту. Зазначено, що інтеграція штучного інтелекту в адміністративне судочинство в Україні найімовірніше відбуватиметься через Єдину судову інформаційно-телекомунікаційну систему шляхом доповнення наявних підсистем або створення нових модулів для аналізу доказів, упорядкування матеріалів справи та підготовки проєктів процесуальних документів. Обґрунтовано, що в разі запровадження подібного правового регулювання особливе значення матиме визначення ролі Державної судової адміністрації України як суб'єкта, який або забезпечує створення такої системи, або використовує її у своїй діяльності, оскільки від цього залежатиме обсяг її правових обов'язків.

Зроблено висновок, що майбутнє правове регулювання використання штучного інтелекту в адміністративному судочинстві України має будуватися на чіткому розмежуванні повноважень учасників, диференціації правового режиму залежно від рівня ризику системи, а також на реалістичному розумінні меж участі судді в технічному нагляді за штучним інтелектом. Оптимальною моделлю є така, за якої суддя зберігає провідну роль у здійсненні правосуддя, тоді як технічні фахівці та судова адміністрація забезпечують належне функціонування, безпеку та контроль за відповідними системами.

Ключові слова: адміністративне судочинство; суддя; високоризикові системи штучного інтелекту; Єдина судова інформаційно-телекомунікаційна система; адміністративна юстиція, цифровізація судочинства.

Стаття: надійшла до редакції 03.04.2026
прийнята до друку 16.04.2026