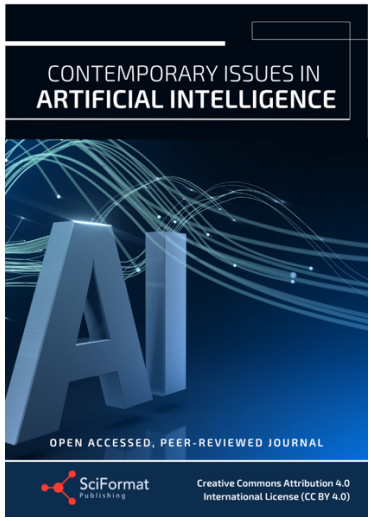

Contemporary Issues in Artificial Intelligence

Vol. 1 (2025)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest,
Calgary, Alberta, Canada,
T3E0A7

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	ETHICS AND RESPONSIBILITY IN THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN JUSTICE
ARTICLE INFO	Zverev Volodymyr, Bushkov Valery, Khrushkov Borys, Shavolin Andriy, Smyshlyaev Serhiy, Prokopovych-Tkachenko Yehor (2025) Ethics and Responsibility in The Implementation of Artificial Intelligence in Justice. *Contemporary Issues in Artificial Intelligence*. Vol.1. doi: 10.69635/ciai.2025.10
DOI	https://doi.org/10.69635/ciai.2025.10
RECEIVED	19 January 2025
ACCEPTED	02 March 2025
PUBLISHED	07 March 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

ETHICS AND RESPONSIBILITY IN THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN JUSTICE

Zverev Volodymyr
Candidate of Technical Sciences, Senior Researcher, Associate Professor of the Department of Software Engineering and Cybersecurity of the State University of Trade and Economics
ORCID ID: 0000-0002-0907-0705

Bushkov Valery
Postgraduate Student of the Department of Software Engineering and Cybersecurity of the State University of Trade and Economics
ORCID ID: 0009-0005-5097-2689

Khrushkov Borys
Postgraduate Student of the Department of Cybersecurity and Information Technologies of the University of Customs and Finance
ORCID ID: 0009-0002-3978-5012

Shavolin Andriy
Associate Professor, Department of Military Training University of Customs and Finance
ORCID ID: 0009-0009-3959-3847

Smyshlyaev Serhiy
Associate Professor, Department of Military Training University of Customs and Finance
ORCID ID: 0009-0007-6996-3170

Prokopovych-Tkachenko Yehor
Leading Specialist Department of Military Training University of Customs and Finance
ORCID ID: 0009-0002-6023-5066

ABSTRACT

The article examines the complex challenges and prospects arising from the implementation of artificial intelligence (AI) in the justice system. The growing role of automated algorithms in legal procedures demonstrates the intention to increase the efficiency of judicial proceedings and optimize the work of law enforcement agencies. At the same time, the use of AI can give rise to a number of ethical, legal and technical problems, particularly issues of transparency, accountability, algorithmic discrimination and biases that manifest in judicial practice and law enforcement processes. The article analyzes scientific approaches to the formation of principles of accountability when making AI decisions and proposes theoretical and practical guidelines for developing the transparency and reliability of intelligent algorithms in the legal sphere. Considerable attention is paid to the research methodology, which combines formal-legal and empirical methods, as well as algorithmic modeling and machine learning tools. The "Results" section provides examples of quantitative analyses and compares the effectiveness of different approaches to the application of AI in jurisprudence. Visualizations and tables demonstrate statistical information and features of the integration of AI into judicial procedures and legal practice. The "Discussion" highlights the theoretical and practical aspects of the developing of an ethics code and legal regulation possibilities, considering diverse challenges. It is concluded that for the effective implementation of AI in justice, wholesome models of transparency, independent auditing and regulatory mechanisms should be developed that also consider the specifics of the judicial system, human rights and the protection of confidential information. Proposals are formulated to establish the responsibility of developers, users and government agencies.

KEYWORDS
Artificial Intelligence, Justice, Legal Regulation, Ethical Responsibility, Algorithmic Discrimination, AI Transparency, Judicial Proceedings, Regulation, Machine Learning, Automated Decisions

CITATION
Zverev Volodymyr, Bushkov Valery, Khrushkov Borys, Shavolin Andriy, Smyshlyaev Serhiy, Prokopovych-Tkachenko Yehor (2025) Ethics and Responsibility in The Implementation of Artificial Intelligence in Justice. *Contemporary Issues in Artificial Intelligence*. Vol.1. doi: 10.69635/ciai.2025.10

Introduction.

Artificial intelligence (AI) is becoming increasingly widespread in the field of law and justice. Its ability to quickly process large amounts of data, analyze case law, and even predict court decisions has driven demand for automated systems that make the work of both judges and lawyers easier. However, rapid technological growth raises pressing concerns about ethics, liability, and legal risks. In particular, the issue of possible algorithmic biases or errors in the process of making AI decisions remains controversial, which can lead to unfair verdicts or judicial practices that are incompatible with human rights principles. The relevance of this topic is due to the fact that clear legislative and ethical regulation of the use of AI in the legal sphere can contribute to improving the quality of justice and reducing corruption risks. However, without the appropriate level of transparency and explainability of AI decisions, society may lose trust in the judicial system, and individuals may experience violations of their rights. In a broad context, the study correlates with approaches to regulating artificial intelligence in European and global legal systems, including initiatives of the European Union and a number of countries that are actively working to create a legal framework to prevent discrimination and abuse by automated systems [1], [2]. The purpose of the article is to comprehensively consider the ethical and legal aspects of introducing AI into justice system, analyze existing scientific approaches and practical experience, and identify the main principles and possible ways of legal liability regulation. Achieving the goal involves the implementation of the following main tasks: - analyze the current state of development of AI in jurisprudence and the main areas of its application; - identify key ethical challenges that arise when using automated solutions, in particular the problem of algorithmic discrimination; - consider existing approaches to legal regulation and develop proposals regarding the liability of developers, state bodies and end users; - substantiate the methodological foundations of the study, present empirical data and modeling results; - to propose ways to improve the legal regulation of AI, taking into account the principles of justice, proportionality and protection of human rights. The scientific novelty lies in an attempt to synthesize various methodological approaches - from formal legal analysis of legislative initiatives to empirical evaluation of algorithmic models used in judicial practice. In previous works [3], [4], [5], aspects of the interaction of IT technologies with the legal system, in particular in terms of information protection and cryptographic mechanisms, have already been outlined. However, the ethical and legal responsibilities associated with AI use remain insufficiently clarified and require systematic research. The practical value of the results is due to the fact that the developed methodological and regulatory recommendations can be used to improve legislation, methods of judicial control, as well as to increase the transparency of the activities of state bodies that implement AI systems in their work. It is also important to note that in the context of global digitalization, the experience of international organizations in combating cybercrime, in particular the activities of Interpol, is becoming an important aspect. An analysis of official Interpol documents highlights how technology and standardized protocols enhance legal and operational harmonization in levelling transnational threats. This experience is extremely relevant for modern research in the field of artificial intelligence in justice system, as the integration of such principles can improve data exchange, increase the efficiency of decision-making, and ensure the transparency of algorithmic processes in judicial practice.

The purpose of the study is a comprehensive analysis of the problem of introducing artificial intelligence into the justice system, which has not yet been adequately reflected in existing legal and scientific research. The modern legal system is not always ready to adequately respond to the challenges associated with the use of AI, which is manifested in the lack of transparency of algorithms, possible biases in making judicial decisions, and the lack of clear mechanisms for distributing responsibility between developers, users, and state bodies. That is why this study is relevant: it is aimed at identifying existing problems and formulating the first proposals for their elimination by integrating ethical principles and the latest technological approaches into legal regulation.

1. Interpol and Cybercrime: Experience of International Cooperation.

For a comprehensive analysis of the topic of introducing artificial intelligence into justice, it is important to cite Interpol's experience in combating cybercrime. A study of official Interpol documents demonstrates how the organization coordinates efforts between member states aimed at countering transnational cyberthreats and can serve as a guideline for the introduction of modern technologies, in particular artificial intelligence, into legal practice.

Interpol forms its policy on cybercrime on the basis of a number of key documents:

- Resolution of the Interpol General Assembly AG-2014-RES-04 defines the main cybercrimes, including unauthorized access to computer systems, interference with data, the use of ransomware and online fraud.
- INTERPOL's Cybercrime Strategy (2020) outlines the organization's priorities, including intelligence sharing and the development of a Global Cybercrime Programme covering malware, phishing, identity theft and distributed denial-of-service (DDoS) attacks.
- INTERPOL's Operational Manual (updated 2023) provides guidance to member states on how to use INTERPOL's tools, including the I-24/7 secure communications network, to investigate cybercrime.
- INTERPOL's Notification System Guidelines detail the use of "Red Notices" to identify and apprehend cybercriminals through international cooperation.

INTERPOL's approach is based on information sharing and technical support to member states. Despite lacking executive powers, the organization acts as a vital coordinator by maintaining large databases on criminals and stolen documents to facilitate rapid information exchange; organizing joint training programs and providing access to specialized resources, which improves the capabilities of local law enforcement agencies; promoting the harmonization of legal and operational approaches in different jurisdictions, which is especially relevant addressing the transnational cyber threats.

2. The value of Interpol's experience in implementing AI in justice.

Interpol's experience in combating cybercrime demonstrates the effectiveness of technological tools and international cooperation, which can be directly applied to implementing artificial intelligence in the justice system.

Key aspects include:

- Data sharing and analytics: Similar to Interpol, the effective use of AI in the legal sphere requires the creation of large, up-to-date databases and algorithms that can analyze a wide range of information to identify patterns and risks.
- Technical support and training: International initiatives, such as Interpol's training programs, can help improve the skills of legal and IT professionals, ensuring a more effective use of AI in judicial processes.
- International cooperation: Integrating Interpol's experience in the justice system can help to enhance common standards, ensuring ethical guarantees, transparency and accountability during judicial decision-making.

Analysis of Interpol's activities demonstrates that international cooperation and effective use of technology can significantly increase the level of cybersecurity. Transferring these principles to the justice system through AI implementation will improve the efficiency and accuracy of judicial decisions through more effective data analysis; reduce the risks of algorithmic bias through experience-sharing and common responsibility standards; ensure legal harmonization among different jurisdictions in the global context of digital technologies.

Thus, Interpol's experience can become an important example for the further development and ethical implementation of artificial intelligence in the justice system, contributing to the strengthening of international cooperation and the development of innovative approaches to solving the legal challenges of the digital era.

The study was conducted considering the specifics of a multi-component environment, including the regulatory framework and existing judicial practices, as well as technological development features and artificial intelligence operation systems in the jurisprudence field. The study combined both quantitative and qualitative methods as well as formal-legal and empirical methods, ensuring comprehensive issue coverage and identifying both legal and technical aspects of ethical responsibility. The formal-legal analysis examined current national and international legislation, as well as concepts and approaches AI regulation in different jurisdictions. The analysis covered legislative initiatives in the field of liability for automated decisions, in particular EU directives and legislative projects in the EU member states that are actively developing the legal framework for AI use [6], [7]. - The empirical component included an open court decisions analysis that involved algorithmic systems (for example, to assess the risks of recidivism or making early release decisions). In addition, interviews were conducted with judicial officials, lawyers, and legal technology developers to clarify the real challenges and obstacles during the implementation of AI. This approach made it possible to establish existing contradictions between the declared principles and the practical use of intelligent systems.

Technological component of the study. - Algorithmic modeling. To identify algorithmic biases, machine learning models and classifiers (Random Forest, SVM and neural networks) analyzed large amounts of data from legal platforms. Study provides research of the ability of algorithms to predict appeals' effectiveness, preventive measure appointment, or how it can assess the degree of guilt. The results were compared with actual court decisions to identify discrepancies and possible discrimination. - Statistical analysis. Regression

and correlation analysis methods were used to assess the influence of various factors (for example, social, ethnic, economic) on the AI decision-making process. Statistical tests (in particular, Student's t-test and chi-square) made it possible to determine whether certain groups of individuals have an increased probability of receiving negative decisions. - Assessment of reliability and security. Building on previous research in cryptography and information security [1], [2], [3], the methodology included an analysis of algorithms resilience against unauthorized interference. In particular, checks were carried out to determine whether external interference could change the forecast of the AI system, for example, by substituting certain data into the database or interfering with the model parameters. Organizational and technical design. To collect and process data, an electronic database "AI in Justice" was created with an anonymized sample of court decisions and indicators that characterize defendants (age, type of offense, etc.). A special toolkit was developed for interviewing and surveying participants in legal proceedings (judges, lawyers, and prosecutors).

Table 1. Study parameters

Parameter	**Description**
Sample size	2,300 court cases (civil and criminal jurisdiction), 1,500 interviews.
Algorithmic models	Random Forest, Support Vector Machines (SVM), multilayer neural networks.
Variables for analysis	Type of offense, age, gender, socio-economic status of the accused, stage of the case, etc.
Evaluation methods	Statistical tests (correlation, t-test), comparison with actual court decisions.
Security audit	Testing for resistance to interference, corrupted data, and cyberattacks.

The validity of the chosen methods is due to the need to ensure an interdisciplinary approach: from the analysis of legislative bases to the technical verification of algorithmic models, as well as the identification of correlations between different categories of court cases and the results of automated decisions.

In the process of analyzing the collected data and modeling, a number of significant trends and possible risks associated with the use of AI in judicial proceedings were identified. A brief summary of the key empirical findings, illustrated by graphical materials and tables, is provided.**3.**

The application of machine learning methods has allowed achieving high accuracy rates (F1-score in the range from 0.76 to 0.85) for classification tasks (in particular, predicting the probability of appeal rejection). Neural networks have demonstrated a tendency to better results compared to traditional methods (logistic regression), which is consistent with modern world research.

The application of machine learning methods in the legal sphere opens up new horizons for the analysis of large volumes of data that were previously inaccessible to traditional approaches. In particular, the use of neural networks has made it possible to consider the complex relationships between numerous factors that affect the outcome of appeal processes. For example, variables such as the time of consideration of the case, the geographical location of the court, the statistics of decisions of individual judges and other contextual data can be effectively integrated into the model to increase its accuracy.

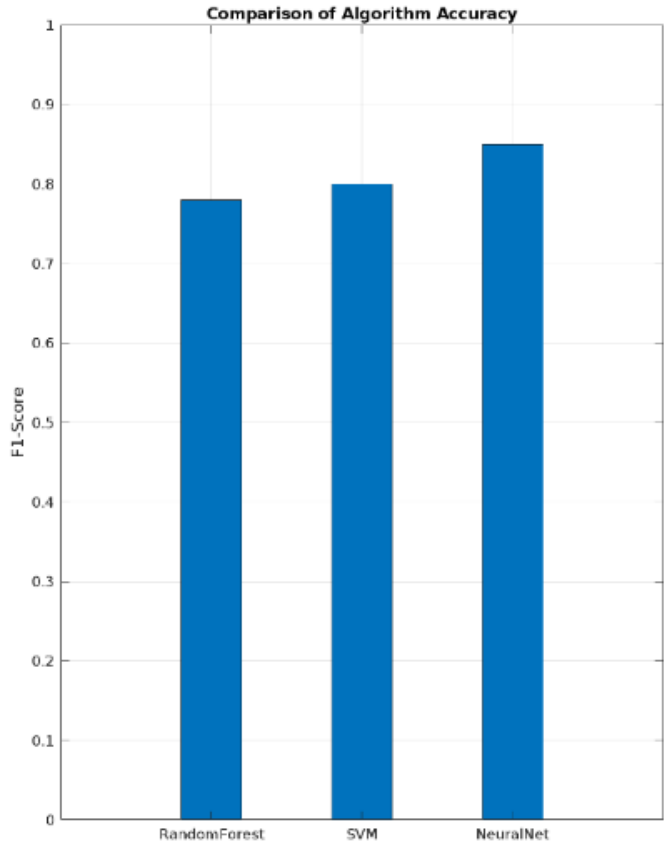

Fig. 1. *Bar chart of accuracy (F1-score) between Random Forest, SVM and multilayer neural network.*

Statistical analysis showed that for some groups of defendants (particularly those with lower socioeconomic status), the AI's negative decision rates were significantly higher than average ($p<0.05$). This indicates possible algorithm bias and the need for additional auditing.

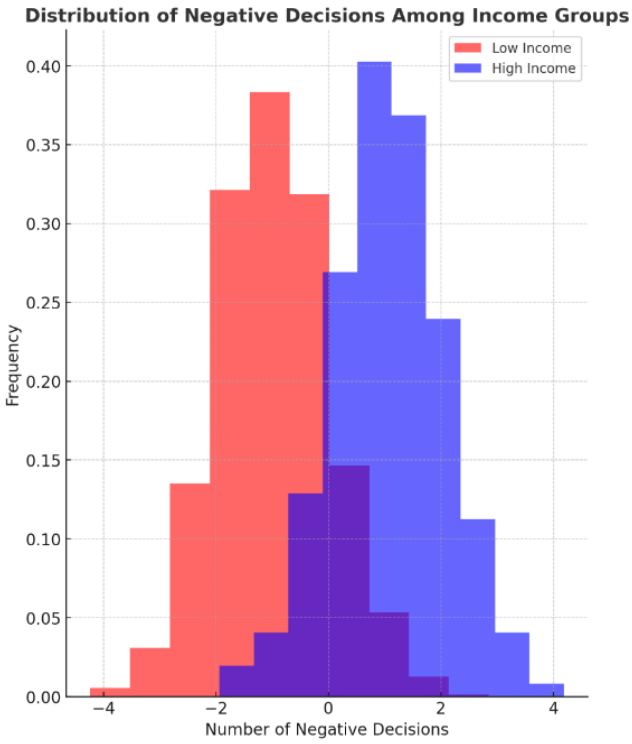

Fig. 2. *Frequency of negative decisions depending on socio-economic status*

4. Impact of external factors and security aspects.

Cybersecurity audits have demonstrated the possibility of third-party interference with the source data or algorithm parameters, which led to significant changes in the results of automated analysis. This conclusion is consistent with previous developments in the field of information systems security, in particular in terms of resistance to attacks [1], [2]. These findings confirm the need to implement the principles of post-quantum cryptography, improved user authentication methods and regular audits to identify potential vulnerabilities [3].

Table 2. Main results of security inspections

Type of intervention	Impact on outcome	Recommended safeguards
Input substitution	Significant change in verdicts (up to 40% of cases)	Implementation of digital signatures, checksum control
Changing model parameters	Accuracy change by 15-25%	Regular audits, model containerization, version control
Malware attack	Deactivating the model, stopping the process	Protected environments execution, updating of antivirus databases

5. Comparison of approaches to the implementation of AI in different countries.

A comparison of the experience of states that have already implemented AI in legal practice has shown significant differences. In some jurisdictions (for example, in some states of the USA), limited test protocols are used to verify the transparency of algorithms, while in a number of EU countries comprehensive legal norms have been developed that provide for full decisions explainability and mandatory state audit [7]. At the same time, several states are at the forming stage only generally conceptualized without detailed regulatory mechanisms. This indicates that the process of integrating artificial intelligence into the legal sphere at different stages of development depends on the region and legal culture.

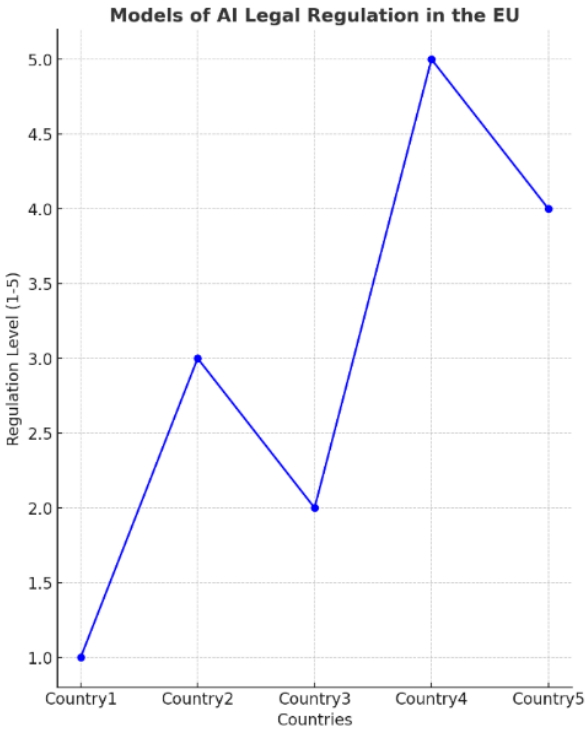

Fig. 3. *Comparison of models of legal regulation of AI in EU countries*

The results obtained confirm that the introduction of AI into justice is a potentially effective tool that can speed up the processing of cases and reduce the burden on the judicial system. At the same time, empirical analysis has identified a number of threats: - Algorithmic discrimination. Data indicate that models are capable of producing different levels of negative decisions depending on the socio-economic or ethnic characteristics of the defendants. The presence of such biases can undermine trust in the judicial system. - Instability of models: external factors can manipulate input data or model parameters, leading to unpredictable outcomes. This requires systematic audits and the implementation of cryptographic protection mechanisms [1], [2], [3]. - Lack of legal regulation: many countries lack clear requirements for explainability, independent auditing and responsibility distribution among developers, algorithm owners, and end users. Comparison of the obtained results with other publications (see e.g. [6], [7], [8], [9]) confirms that the potential implementation of AI systems is considered promising, but at the same time high-risk.

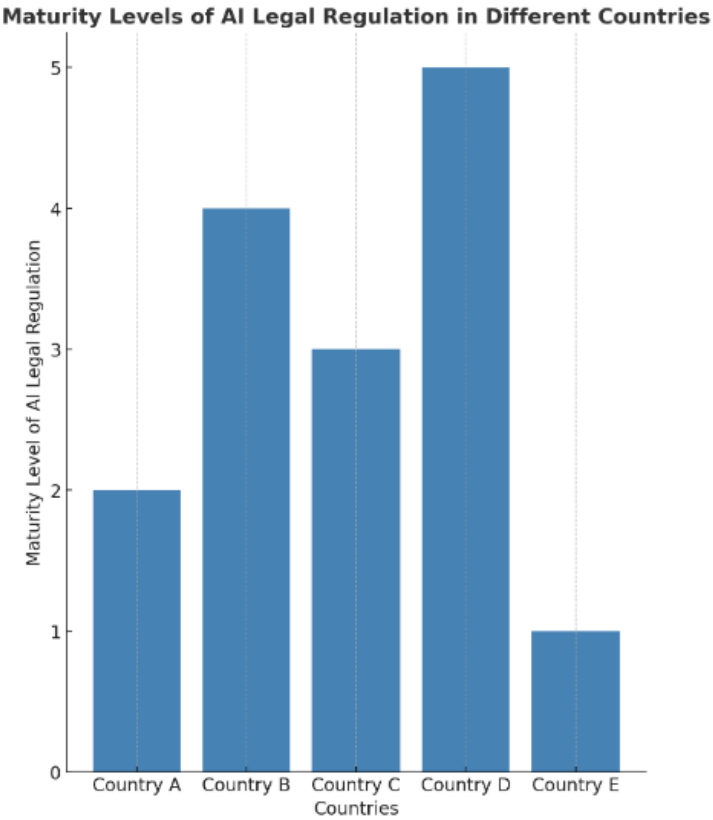

Fig. 4. *Schematic representation of 5 EU countries with different levels of maturity of AI legal regulation.*

Promising directions for future research: - Improving the "Explainable AI" methods (XAI), which will ensure a higher level of AI model decisions explainability and reduce the risk of unjustified discrimination. - Developing liability hybrid legal mechanisms that concern with the role of developers, owners and state regulators in the AI decision-making process. - Adapting cryptographic algorithms to implement secure data transmission and processing in judicial systems, especially based on post-quantum cryptography [3]. - Implementing systems for independent audit of AI models and creating a single control platform that will include technical, legal and ethical monitoring.

6. Proposals for improving the application of AI in justice.

The main problem is the lack of clear legal norms, definitions and regulatory mechanisms for the application of artificial intelligence in justice, which creates legal uncertainty and leads to risks of algorithmic bias, insufficient transparency of decision-making and uncertainty of the distribution of responsibility between developers, users and government agencies. To eliminate these problems, it is necessary to make additions to existing legislative acts or develop new regulatory and legal acts that provide transparency requirements, explainability and control of algorithmic decisions. It is necessary to create a terminological base that defines the concepts of “artificial intelligence”, “algorithmic bias”, “automated decision-making”, which will allow

for an unambiguous interpretation of legal norms. It is also necessary to establish mechanisms for independent AI systems auditing with the involvement of legal and information technology experts, as well as legislative consolidation of the distribution of responsibility between all entities involved in the artificial intelligence using process. Harmonizing national legislation with international standards will allow integrating the experience of other jurisdictions and creating uniform rules that will promote the effective, ethical, and fair use of AI in the justice system.

Conclusions.

Therefore, the results of the study demonstrate the significant potential for the application of AI in the field of justice, which can enhance the efficiency and predictability of court decisions. At the same time, the identified risks - primarily algorithmic discrimination and the possibility of manipulation - indicate a critical need to develop clear legal and technical protection mechanisms. In particular, it is necessary to:

The principles of transparency and explainability of AI decisions should be legislatively enshrined, obliging developers to provide information about the functioning of models and their training set. Determine forms of legal liability for all entities: from software developers to state bodies that make final decisions based on AI. - Create a mechanism for independent audit of algorithms with the involvement of legal and IT specialists who will check the correctness and absence of discriminatory factors. Introduce a code of ethics for developers and users of AI in the legal sphere, focusing on international standards. The Code should contain provisions on the inadmissibility of hidden biases and the importance of maintaining data confidentiality. - Ensure appropriate training and advanced training of legal personnel in the field of IT and AI, so that judges and lawyers can adequately interpret the results of automated analysis.

However, it is equally important to note that based on the analysis conducted, it becomes obvious that the lack of clear legal norms, definitions and mechanisms for regulating the use of artificial intelligence in justice creates significant risks for ensuring the fairness of judicial proceedings. Given these challenges, it is proposed to make additions to existing regulatory and legal acts or develop new ones that would contain concepts definitions related to the use of AI, establish criteria for transparency and explainability of algorithmic decisions and provide for mechanisms for independent audit of the use of AI.

Legislation should regulate the distribution of responsibility between all entities involved in the AI using process, thereby ensuring effective interaction between developers, users and state bodies. Integration of the experience of other countries and international organizations will contribute to the harmonization of legal regulation, which will allow creating a single system, guaranteeing ethical, effective and fair application of AI in judicial practice. This approach is necessary to increase public trust in the judicial system and minimize the risks of discrimination and algorithmic errors that can negatively affect human rights. The proposed measures create the basis for further research and development of recommendations to improve the legal support for the use of artificial intelligence in justice, which should be an important step in ensuring a balance between innovative development of technologies and ensuring legal guarantees for all participants in the judicial process.

Further implementation of AI into the justice system should be based on considered decisions that combine technical innovation with human rights respect and the rule of law. The proposed recommendations can be the basis for the adoption of relevant regulations that will guarantee the responsible use of AI and maintain public trust in the judicial system.

REFERENCES

1. Kuznetsov, A. A., Gorbenko, Y. I., Kolovanova, I. P., & Prokopovych-Tkachenko, D. I. (2017). Key schedule of block symmetric ciphers. ASC Academic Publishing.
2. Rassomahin, S. G., Kuznetsov, A. A., & Prokopovych-Tkachenko, D. I. (2017). Security and noise immunity of telecommunication systems: New solutions to the codes and signals design problem. ASC Academic Publishing.
3. Prokopovych-Tkachenko, D. I., Kuznetsov, A. A., & Tarasenko, Y. (2018). Information security in critical infrastructures. ASC Academic Publishing.
4. Stefanovych, O., Kuznetsova, K., Tarasenko, Y., & Polins'ky, O. (2018). Steganography hiding of information using 3D-printing technologies. 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), https://doi.org/10.1109/UkrMiCo43733.2
5. Lisickiy, K., Kuznetsova, K., Malenko, Y., Zavgorodnia, O., & Prokopovych-Tkachenko, D. I. (2019). Accelerated method for calculating the algebraic immunity of S-boxes. 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), https://doi.org/10.1109/UKRCON.

6. Tarasenko, Y. S., Smirnov, V. V., & Prokopovych-Tkachenko, D. I. (2019). Features of detecting hidden artificial objects under customs control conditions. Systems and Technologies Conference Proceedings, 2(58), 161-169.
7. Prokopovych-Tkachenko, D. I., Kuznetsov, A. A., & Tarasenko, Y. (2020). Post-quantum cryptography in telecommunication systems. International Journal of Information and Communication Technologies.
8. Prokopovych-Tkachenko, D. I., Kuznetsov, A. A., & Pastukhov, M. (2021). Code-based fuzzy extractors for biometric data. Computer Science and Cybersecurity.
9. Kuznetsov, A. A., Kiyan, A. S., & Prokopovych-Tkachenko, D. I. (2020). Periodic properties of cryptographically secure pseudorandom sequences. Applied Radioelectronics.
10. Prokopovych-Tkachenko, D. I., Kuznetsov, A. A., & Moskovenko, I. V. (2018). Heuristic methods for gradient search of cryptographic Boolean functions. Radiotechnics.
11. Kuznetsov, A. A., Serhienko, R. V., & Prokopovych-Tkachenko, D. I. (2018). Algebraic immunity of symmetric ciphers. CS and Cybersecurity, 36-48.
12. Lutsenko, M. S., Kuznetsov, O. O., & Prokopovych-Tkachenko, D. I. (2019). Comparative analysis of biometric cryptosystems. Applied Radioelectronics.
13. Prokopovych-Tkachenko, D. I. (2013). Method of generating pseudorandom sequences of maximum period using elliptic curve transformations. Academy of Customs Service of Ukraine.
14. Prokopovych-Tkachenko, D. I. (2016). Accelerated generation of pseudorandom sequences of maximum period using elliptic curve transformations. Information Processing Systems, 197-203.
15. Kuznetsov, O. O., Stefanovych, O. O., & Prokopovych-Tkachenko, D. I. (2018). 3D steganographic method for information hiding. Radio Engineering, 193-202.
16. Tarasenko, Y. S., Smirnov, V. V., Stelyuk, B. B., & Prokopovych-Tkachenko, D. I. (2016). Anechoic mode in an information-measuring system for customs control. University of Customs and Finance.
17. Voloshyn, R. M., & Prokopovych-Tkachenko, D. I. (2020). Recommendations on cybersecurity of the educational process. Formation of a Modern Management Model.
18. Prokopovych-Tkachenko, D. I. (2014). Co-authorship of the Law of Ukraine "On Amendments to the Law of Ukraine 'On the State Service for Special Communications and Information Protection of Ukraine'" (No. 4432). Verkhovna Rada of Ukraine.
19. Tarasenko, Y. S., Savchenko, Y. V., & Prokopovych-Tkachenko, D. I. (2019). The paradigm of radio-electronic measurements: From error to uncertainty. University of Customs and Finance.
20. Kuznetsov, A. A., Kolovanova, Y. P., & Prokopovych-Tkachenko, D. I. (2017). Algebraicgeometric codes: Analysis and properties. Radio Engineering, 70-89.
21. Moroz, B. I., Prokopovych-Tkachenko, D. I., & Petrenko, I. V. (2018). Improvement of router authorization protocols in wireless networks to reduce negative impact. Systems and Technologies.
22. Kuznetsov, A. A., & Prokopovych-Tkachenko, D. I. (2018). Technologies for encryption based on Boolean functions. Radio Engineering.
23. Kostenko, O. V. (2022). Analysis of national strategies for the development of artificial intelligence. Information and Law, vol. 2(41), pp. 58-69. DOI: https://doi.org/10.37750/26166798.2022.2(41).270365
24. Kostenko O., Furashev V., Zhuravlov D., Dniprov O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. Bratislava Law Review, vol. 6(2), pp. 21-36. DOI: https://doi.org/10.46282/blr.2022.6.2.316
25. Minsky, M. (2021). Computational Theories of Mind and Machine: Prospects for Justice. MIT Press.
26. Hildebrandt, M. (2020). Law for Computer Scientists and Other Folk. Oxford University Press.
27. Goggin, J., & Byfield, T. (2021). Algorithmic Accountability in Legal Technologies. European Journal of Legal Studies, 9(1), 23-48.
28. Moravčík, M., Schmid, M., Burch, N., & Bowling, M. (2017). DeepStack: Expert-level artificial intelligence in heads-up no-limit poker. Science, 356(6337), 508-513.
29. Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.
30. Smith, B. (2022). Tools and Weapons: The Promise and the Peril of the Digital Age. Penguin Books.