ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEDURE: CURRENT LEGAL REGULATIONS IN THE EU

Chernychenko Iryna

DOI: https://doi.org/10.61345/1339-7915.2025.3.1

Annotation. The increasing deployment of artificial intelligence (AI) technologies changed all areas of our lives and has raised urgent legal and ethical questions.

This article explores the integration of artificial intelligence technologies into criminal procedure within the European Union (EU), focusing on the current state of legal regulation.

The article provides an overview of five key documents: European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment, White Paper on Artificial Intelligence: A European Approach to Excellence and Trust, European Parliament Resolution on Artificial Intelligence in Criminal Law and its Use by the Police and Judicial Authorities in Criminal Matters, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law and Artificial Intelligence Act.

Particular attention is paid to the compatibility of AI-based tools with the right to a fair trial, the presumption of innocence, the principle of non-discrimination, data protection and information security standards.

The methodological basis of the study is grounded in a doctrinal legal research approach, combining normative analysis of EU and Council of Europe legal instruments with a comparative review of relevant policy documents and ethical frameworks.

The paper argues that while the EU has made notable progress in outlining a normative framework for trustworthy AI, the regulation of AI specifically within the criminal justice context remains fragmented and requires further harmonization. It also emphasizes the importance of maintaining a balance between innovation, efficiency and the protection of fundamental rights.

Key words: artificial intelligence, criminal procedure, digital technologies, legal regulation, European Union.

1. Introduction.

In recent years, the integration of artificial intelligence technologies has radically changed all areas of our lives and continues to develop rapidly. The field of criminal justice is no exception.

From predictive policing and risk assessment tools to automated evidence analysis and facial recognition systems, AI-based applications are increasingly being used by law enforcement agencies and judicial authorities across the European Union. While acknowledging the growing importance of artificial intelligence in modern societies and its potential to enhance the efficiency and quality of justice, it must be noted that digital transformation continues to have an uneven impact on the judicial systems of the Council of Europe member states.

According to Figure 44 of the EU Justice Scoreboard 2024, AI are used only in courts in Germany, Austria, Spain, Luxembourg, and France, and in prosecution services in Germany, Austria, Portugal and Luxembourg [1, p. 36].

Currently, legislative bodies and governments of many countries have implemented and continue to implement special regulations aimed at legally ensuring the use of artificial intelligence. The undisputed leader in shaping the legal landscape of AI applications is the European Union. Therefore,

an urgent scientific and practical task is to analyze the state of legal regulation of artificial intelligence in the EU, to determine its trends and prospects.

2. Analysis of scientific publications.

The problems of legislative regulation of the use of AI are quite new in jurisprudence at both the international and national levels. Despite this, the issues related to the international regulation of AI in the field of criminal procedure, are the subject of research by a fairly wide range of ukrainian scholars: Oksana Kaplina, Anush Tumanyants, Iryna Krytska and Olena Verkhoglyad-Gerasymenko [2], Julia Repina [3], Oleg Plakhotnik [4], Oleksandr Kozhukhar [5] and others. The issue of regulating AI systems has also been the subject of publications by a number of foreign researchers, including Thomas Burri and Fredrik von Bothmer [6], Sophie Noiret, Jennifer Lumetzberger, Martin Kampel [7], Katerina Entcheva, Ioana Mazilescu [8] and others.

3. The main aim of this paper is to analyse the current legal regulation of artificial intelligence within the European Union, focusing on its application in the field of criminal procedure and paying particular attention to compliance with fundamental rights and the rule of law.

4. Presentation of the research material.

The development of artificial intelligence technologies and their integration into the functioning of judicial and law enforcement authorities in European countries represent a significant advancement. AI serves as a highly effective tool for safeguarding the right to judicial protection, enhancing access to justice, and improving the efficiency and transparency of judicial processes.

We agree that possible areas of use of AI in the field of criminal process are:

(1) Related to the collection and processing of evidence (recognition of images, such as people and objects in video and photo images; DNA analysis; identification of weapons and other objects).

(2) Related to the so-called "predictable" decision-making (pre-trial release of a person from custody; selection of the most appropriate type and measure of punishment, including probation).

(3) Related to the performance of auxiliary tasks arising in criminal proceedings, (automatic preparation of forms of certain procedural documents, including summonses, applications, petitions, and complaints; generalisation and systematisation of evidence; search of relevant case law; forecasting of judicial prospects; automated preparation of court transcripts using natural language recognition technologies; provision of legal advice using chatbots) [2, p. 151].

This analysis of the current legal regulation of artificial intelligence begins with the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment, adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, December 3-4, 2018).The Charter is a soft law document that essentially codifies five basic principles for the application of AI in the field of justice: 1) respect for fundamental rights; 2) non-discrimination; 3) quality and security: 4) transparency, impartiality and fairness; 5) under user control [9, p. 7].

In the field of justice, four categories of AI use have been proposed:

Uses to be encouraged;

Possible uses, requiring considerable methodological precautions;

Uses to be considered following additional scientific studies;

Uses to be considered with the most extreme reservations.

The involvement of AI can vary greatly according to the applications. For instance: advanced case-law search engines, online dispute resolution, assistance in drafting deeds, analysis,"chatbots" to inform litigants or support them in their legal proceedings etc. [9, p. 17].

Besides this the document provides the differences in the scope of application of AI in civil, commercial and administrative justice, on the one hand, and criminal justice, on the other. Specific tools are used by investigative authorities before the criminal trial. Commonly they used to prevent the commission of criminal acts (by identifying possible places where this could happen or their authors) or prosecute them more effectively.

The use of predictive tools by judges in criminal trials is rare in Europe. Perhaps this is due to negative cases of AI use. For example, the program, Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), was much more prone to mistakenly label black defendants as likely to reoffend – wrongly flagging them at almost twice the rate as white people (45% to 24%), according to the investigative journalism organisation ProPublica [10]. Undoubtedly, negative experiences with the use of artificial intelligence in judicial systems will serve as a basis for correcting errors in the future. However, the aforementioned statistics once again highlight the need for continuous monitoring to prevent unforeseen consequences. In criminal matters, the use of artificial intelligence requires the utmost caution due to its direct impact on individuals' personal freedoms. It must be approached with the highest level of scrutiny to prevent discrimination based on sensitive data and to ensure full compliance with the guarantees of a fair trial.

Another source for shaping European Union legislation in the field of artificial intelligence is the White Paper on Artificial Intelligence: A European Approach to Excellence and Trust. This strategic document, published on February 19, 2020, outlines the key priorities for the development of artificial intelligence and sets out the fundamental principles for its design and application. establish legally binding rules; rather, it presents the European Commission's vision, objectives, and possible courses of action for regulating artificial intelligence. It outlines a set of policy proposals, intentions, and recommendations. White Paper presents policy options to enable a trustworthy and secure development of AI in Europe, in full respect of the values and rights of EU citizens. It is assumed that Europe can develop an AI ecosystem that brings the benefits of the technology to the whole of European society and economy for citizens, for business development and for services of public interest.

It is widely acknowledged that, as with any technology, the use of artificial intelligence presents both significant opportunities and potential risks. There is a clear danger that AI systems may produce unintended consequences or be exploited for malicious purposes. This may be one of the factors holding back the wider adoption of artificial intelligence. Therefore, a whole separate section 5 of the White Paper, entitled «The ecosystem of trust». The main risks related to the use of AI concern the application of rules designed to protect fundamental rights, as well as safety and liability-related issues. The use of AI can affect the values on which the EU is founded and lead to breaches of fundamental rights, including the rights to freedom of expression, freedom of assembly, human dignity, non-discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation, as applicable in certain domains, protection of personal data and private life, or the right to an effective judicial remedy and a fair trial, as well as consumer protection [10, p. 10-11].

The implications of AI are analysed in the Commission Report accompanying White Paper. It is noted that the emergence of new digital technologies like AI raise new challenges in terms of product safety and liability like connectivity, autonomy, data dependency, opacity, complexity of products and systems, software updates and more complex safety management. Autonomy is one of the main features of AI. Artificial intelligence based unintended outcomes could cause harm to the users and exposed persons. A big portion of the Union product safety framework was written prior to the emergence of digital technologies such as AI. It therefore does not always contain provisions explicitly addressing the new challenges and risks of these emerging technologies. The current product safety legislation contains a number of gaps that need to be addressed. Future work on the adaptation of different pieces of legislation in this framework will be done in a consistent and harmonised manner [12].

It is also important to analyse the European Parliament Resolution on Artificial Intelligence in Criminal Law and its Use by Police and Judicial Authorities in Criminal Matters, adopted on December 1, 2021. AI applications may offer great opportunities in the field of law enforcement, in particular in improving the working methods of law enforcement agencies and judicial authorities, and combating certain types of crime more efficiently (financial crime, money laundering and terrorist financing, online sexual abuse and exploitation of children as well as certain types of cybercrime), thereby contributing to the safety and security of EU citizens.

AI is in use by law enforcement in applications such as: facial recognition technologies, e.g. to search suspect databases and identify victims of human trafficking or child sexual exploitation and abuse; automated number plate recognition; speaker and speech identification; lip-reading technologies; gunshot detection algorithms; autonomous research and analysis of identified databases; forecasting; behaviour detection tools; advanced virtual autopsy tools to help determine cause of death; autonomous tools to identify financial fraud and terrorist financing; social media monitoring and automated surveillance systems incorporating different detection capabilities such as heartbeat detection and thermal cameras)

We agree that the use of AI applications in criminal procedure must be classified as high-risk in cases where they have the potential to significantly impact individuals' lives. In this context, any AI tools developed or deployed by law enforcement or judicial authorities should, at a minimum, be safe, robust, secure, and fit for purpose. They must adhere to the principles of fairness, data minimization, accountability, transparency, non-discrimination, and explainability. Furthermore, their development, deployment, and use should be subject to rigorous risk assessment, as well as strict necessity and proportionality tests, with safeguards that are proportionate to the identified risks. [13].

The first-ever international legally binding treaty in the field of Artificial Intelligence is Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Opened for signature on September 5, 2024, it aims to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law, while being conducive to technological progress and innovation. The Convention has been signed not only by countries of the European Union but also by the USA, Switzerland, Canada, United Kingdom, Ukraine, Japan, Norway and others [14].

The Framework Convention covers the use of AI systems by public authorities or private actors acting on their behalf. The document provides that the activities within the lifecycle of AI systems must comply with the following fundamental principles: human dignity and individual autonomy, equality and non-discrimination, respect for privacy and personal data protection, transparency and oversight, accountability and responsibility, reliability, safe innovation (Articles 7-13) [15].

The use of artificial intelligence in the EU is also regulated by the Artificial Intelligence Act. This is the world's first comprehensive AI law that entered into force on August 1, 2024. The Act will become fully applicable 24 months after its entry into force, although certain provisions will apply earlier. For example, the prohibitions on certain AI systems and the requirements related to AI literacy (Chapters I and II) have been in effect since February 2, 2025. Provisions concerning notified bodies (Chapter III, Section 4), general-purpose AI models (Chapter V), governance (Chapter VII), confidentiality (Article 78), and penalties (Articles 99 and 100) will become applicable on August 2, 2025.

The official definition of "AI system" is provided in the aforementioned document in paragraph 1 of Article 3 – a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments [16].

Act establishes a risk-based AI classification system. AI systems that can be used in different applications are analysed and classified according to the risk they pose to users. Four categories are highlighted.

1. Prohibited AI practices – the use is completely prohibited due to unacceptable risk to fundamental rights. For example, AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques etc. Also, it is prohibited the use of "real-time" remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

– the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

– the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

– the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II of AI Act and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

2. High-risk AI systems – use is permitted, but subject to strict regulation and mandatory conformity assessment. For example, regarding criminal proceedings in the framework of an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence, the deployer of a high-risk AI system for post-remote biometric identification shall request an authorisation, ex ante, or without undue delay and no later than 48 hours, by a judicial authority or an administrative authority whose decision is binding and subject to judicial review, for the use of that system, except when it is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence. Each use shall be limited to what is strictly necessary for the investigation of a specific criminal offence.

3. Certain AI systems – requires minimum transparency requirements, the user must be informed that they are interacting with AI. For example, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated.

4. General-purpose AI models with systemic risk – can cause serious accidents, incidents or are misused for large-scale cyberattacks, that's why additional obligations regarding risk assessment and mitigation, incident reporting and cybersecurity protection imposes by the Article 55 of AI Act.

5. Conclusions.

AI development has made a big leap forward in recent years, making it one of the strategic technologies of the 21st century. Having analyzed certain regulatory documents that play a key role in regulating the basic principles, approaches and recommendations for the use of artificial intelligence in the field of criminal justice, we conclude that the rapid development of artificial intelligence presents both opportunities and challenges for criminal justice systems within the European Union. Both the benefits and the drawbacks of the application of such tools in the judicial field should be carefully measured. Current EU legal instruments and policy documents reflect an evolving approach toward ensuring that AI technologies are implemented in compliance with fundamental rights, the rule of law and democratic principles. In particular, the use of artificial intelligence by law enforcement agencies and courts must be clearly regulated and strictly monitored to ensure compliance with established standards, as it may pose significant risks to fundamental rights, including the right to a fair trial, the presumption of innocence, the right to privacy and data protection, and the principle of non-discrimination.

References:

1. The 2024 EU Justice Scoreboard. Publications Office of the European Union (2024). https://commission.europa.eu/document/download/84aa3726-82d7-4401-98c1-fee04a7d2dd6_en?filename=2024%20EU%20Justice%20Scoreboard.pdf[in English].

2. 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, 3 (20), 147–166. https://doi.org/10.33327/AJEE-18-6.3-a000314 [in English].

3. Repina, Y. S. (2024). Stages of regulatory regulation of the use of artificial intelligence technologies in criminal justice in the European Union and in Ukraine. Yurydychnyi Naukovyi Elektronnyi Zhurnal, (1), 629–634. http://www.lsej.org.ua/1_2024/152.pdf [in Ukrainian].

4. Plakhotnik, O. (2019). Practical use of artificial intelligence in criminal proceeding. Visnyk Kryminalnoho Sudochynstva, (4), 45–57. [in Ukrainian].

5. Kozhukhar, O. (2024). Legal regulation of artificial intelligence systems in the EU: Prerequisites, current state and prospects. Naukovi Zapysky NaUKMA. Yurydychni Nauky, 13, 65–73. https://ekmair.ukma.edu.ua/items/b5f8e717-3a11-403b-a28f-cfc12cc8c41f. [in Ukrainian].

6. Burri, T., & von Bothmer, F. (2021). The new EU legislation on artificial intelligence: A primer. SSRN. https://ssrn.com/abstract=3831424 [in English].

7. Noiret, S., Lumetzberger, J., & Kampel, M. (2022). Bias and fairness in computer vision applications of the criminal justice system. https://arxiv.org/pdf/2208.03209 [in English].

8. Entcheva, K., & Mazilescu, I. (2024). Artificial intelligence and digitalisation of judicial cooperation: The main provisions in recent EU legislation. eucrim, (3), 202-205. https://eucrim.eu/articles/artificial-intelligence-and-digitalisation-of-judicial-cooperation/ [in English].

9. Council of Europe, CEPEJ. (2018, December 3-4). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. Strasbourg. https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c [in English].

10. Rise of the racist robots – how AI is learning all our worst impulses. The Guardian (2017). https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses [in English].

11. European Commission. (2020, February 19). White Paper on Artificial Intelligence: A European approach to excellence and trust (COM(2020) 65 final). https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf [in English].

12. European Commission. (2020, February 19). Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (COM(2020) 64 final). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020DC0064 [in English].

13. European Parliament. (2021, October 6). Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_132_R_0003 [in English].

14. Council of Europe. The Framework Convention on Artificial Intelligence. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence [in English].

15. Council of Europe. (2024, September 5). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Vilnius. https://rm.coe.int/1680afae3c [in English].

16. European Parliament & Council of the European Union. (2024, June 13). Artificial Intelligence Act (Regulation EU 2024/1689). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 [in English].

Iryna Chernychenko,
Candidate of Science of Law (Equiv. Ph.D.), Docent,
Associate professor of the Criminal Law and Law Enforcement Department,
Faculty of Law,
«Uzhhorod National University», Ukraine
E-mail: iryna.chernichenko@uzhnu.edu.ua
ORCID: 0000-0002-2284-1930