

DOI:

<https://doi.org/10.33327/AJEE-18-8.S-a000155>

Date of submission: 03 Sep 2025

Date of acceptance: 01 Oct 2025

Date of Publication 30 Dec 2025

Disclaimer:

The authors declare that opinion and views expressed in this manuscript are free of any impact of any organizations. One of the authors additionally declares that her opinion and views expressed in this manuscript are free from any influence of any organization, including the Constitutional Court of Ukraine, despite the fact that she is a member of the Scientific Advisory Council of the Constitutional Court.

Copyright:

© 2025 Lidiia Moskvych, Iryna Borodina and Olga Ovsiannikova

Research Article

ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE IN GERMANY AND UKRAINE: A COMPARATIVE LEGAL STUDY

Lidiia Moskvych, Iryna Borodina and Olga Ovsiannikova*

ABSTRACT

Background: Artificial intelligence (AI) is rapidly evolving from peripheral administrative tools into applications that directly influence the functioning of criminal justice systems. In Europe, this integration proceeds under a cautious, law-centred approach that seeks to balance innovation with the preservation of judicial independence, fairness, and the rule of law. This article offers a comparative legal analysis of AI deployment in the criminal justice systems of Germany and Ukraine, situating national developments within the broader framework of the EU Artificial Intelligence Act (2024), Council of Europe standards, and constitutional safeguards. Germany's structured, federally coordinated rollout contrasts with Ukraine's targeted yet ethically constrained implementation, reflecting divergent institutional capacities and legal traditions.

Methods: *This study adopts a comparative legal approach that combines functionalist and contextualist perspectives. The functionalist dimension examines how Germany and Ukraine employ AI in criminal justice to address analogous issues—such as efficiency, transparency, and rights protection—while the contextualist dimension situates these developments within each country’s constitutional framework, institutional capacity, and socio-political environment, notably the impact of wartime conditions in Ukraine. This combined perspective ensures that similarities and divergences are assessed not in abstraction but against the broader background of European and national legal cultures. The analysis draws on primary law, regulatory instruments, official court and ministerial reports, and peer-reviewed scholarship. Empirical examples include German pilot projects in predictive policing (PRECOBS, KLB-operativ), investigative filtering tools, and administrative AI in courts, as well as Ukraine’s probation risk-assessment algorithm Cassandra and AI-assisted systems for legal research and translation. Experiences from the United States with algorithmic risk assessment are used as a cautionary benchmark.*

Results and Conclusions: *The study finds that, while both jurisdictions restrict the use of AI as a substitute for core judicial decision-making, Germany leverages its infrastructure, coordinated administration, and legislative oversight to test and evaluate AI tools. By contrast, Ukraine’s integration is more selective, subject to explicit ethical limitations, but hindered by gaps in transparency and the constraints imposed by wartime conditions. The analysis identifies common challenges—including algorithmic bias, explainability, evidentiary admissibility, and the protection of fair trial guarantees—and formulates context-specific recommendations. These include mandatory external audits, codified procedural rights to challenge AI-generated data, clearer evidentiary protocols, and enhanced judicial awareness of AI technologies. The study underscores that the sustainable integration of AI into criminal justice must remain supportive, auditable, and under human control to comply with European legal standards and safeguard fundamental rights.*

1 INTRODUCTION

Across the world, emerging technologies are transforming judicial systems. Countries such as China, Singapore, and the United States have launched pilot projects for “intelligent courts” or algorithmic tools designed to optimise the handling of specific cases, reportedly leading to greater efficiency. In China, for instance, AI-based systems are already assisting in analysing evidence and even drafting decisions in minor civil disputes, substantially reducing case-processing times.¹

By contrast, European jurisdictions have pursued a more cautious approach, limiting artificial intelligence to supportive functions such as electronic filing systems and digital

1 Changqing Shi, Tania Sourdin and Bin Li, ‘The Smart Court – A New Pathway to Justice in China?’ (2021) 12(1) International Journal for Court Administration 4. doi:10.36745/ijca.367.

databases, and firmly preserving human judgment in adjudication.² A notable expression of this cautious philosophy is the adoption of the European Union's Artificial Intelligence Act (2024),³ which embodies the regional consensus that technological innovation must be reconciled with reliable oversight and the protection of fundamental rights.

Germany and Ukraine exemplify this model of cautious integration within Europe, albeit under very different circumstances. Germany, a long-standing EU member with a federal judicial system and stringent data protection rules, has implemented a systematic "Justice 4.0" strategy. Ukraine, by contrast, as an EU candidate state with a judiciary in transition, is modernising rapidly through the digitalisation of court services despite the obstacles posed by the ongoing armed conflict. For more than a decade, Ukrainian courts have used digital platforms to provide public access to judicial decisions and facilitate remote hearings—measures that have improved transparency and reduced backlogs. Nevertheless, Ukraine's ability to introduce advanced AI technologies remains constrained by limited resources and wartime priorities.

Taken together, these two countries illustrate a striking contrast: one relies on substantial resources and a methodical, EU-based approach, while the other introduces innovations under pressure, guided largely by European recommendations.

2 METHODOLOGY

This study employs a comparative legal methodology designed to illuminate both convergences and divergences in the integration of artificial intelligence within the criminal justice systems of Germany and Ukraine. The analysis rests on three interrelated pillars.

First, a functionalist inquiry identifies how AI technologies are deployed to address analogous challenges—efficiency in case management, transparency in judicial reasoning, and the safeguarding of fundamental rights. This dimension enables the systematic comparison of institutional responses to shared problems without presuming that similar technologies necessarily yield identical legal consequences.

Second, a contextualist approach situates these functional developments within each jurisdiction's constitutional architecture, institutional capacity, and socio-political environment. Particular attention is given to the embeddedness of AI regulation within

2 Elif Kiesow Cortez and Nestor Maslej, 'Adjudication of Artificial Intelligence and Automated Decision-Making Cases in Europe and the USA' (2023) 14(3) *European Journal of Risk Regulation* 457. doi:10.1017/err.2023.61.

3 Regulation (EU) 2024/1689 of the European Parliament and of the Council 'Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' (13 June 2024) <<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>> accessed 10 August 2025.

European legal culture in Germany, and to the constraints and innovations shaped by wartime conditions in Ukraine. By embedding national practices within their broader normative and political contexts, the analysis avoids decontextualised parallels and instead highlights the distinctive logics guiding adoption.

Third, a multi-source research design provides a robust evidentiary base for the comparative exercise. The study draws on primary legislation, constitutional and international instruments, ministerial and judicial policy documents, and case law, complemented by secondary materials such as peer-reviewed scholarship and professional reports. Empirical illustrations are incorporated through pilot projects and operational tools, including German initiatives in predictive policing (PRECOBS, KLB-operativ), investigative data-filtering algorithms, and administrative AI systems in courts; and Ukraine's Cassandra risk-assessment program and AI-supported legal research and translation services. Comparative references to the United States' experience with algorithmic risk assessment further serve as a cautionary benchmark.

Analytically, the study combines doctrinal legal reasoning with normative evaluation. Doctrinally, it maps the extent to which AI applications comply with constitutional safeguards, data protection requirements, and procedural rights. Normatively, it interrogates whether these safeguards are adequate to sustain fairness, accountability, and human oversight in criminal justice. This dual perspective allows the inquiry to transcend mere description and to formulate context-sensitive recommendations.

In sum, the methodology integrates functionalist comparison, contextualist interpretation, and multi-source triangulation to provide a comprehensive and rigorous assessment of how two distinct legal systems navigate the opportunities and risks of AI in criminal justice.

3 LEGAL AND POLITICAL FOUNDATIONS IN EUROPE

Before examining national developments, it is necessary to outline the general European legal and ethical framework governing the use of AI in the administration of justice. Both Germany and Ukraine operate within this framework, which establishes fundamental restrictions and requirements for any application of AI in criminal proceedings.

At its core lies the EU Artificial Intelligence Act (2024),⁴ which establishes a comprehensive risk-based regulatory framework. Crucially, it classifies AI systems deployed by law enforcement or judicial authorities as “high-risk,” thereby imposing stringent obligations. Providers and users of such systems must implement documented risk-management processes, ensure the high quality of training data, guarantee human oversight at critical decision points, maintain detailed operational logs, and provide transparency to affected individuals. Certain AI practices are categorically prohibited as posing an “unacceptable

4 *ibid.*

risk”—for example, social scoring and real-time biometric identification in public spaces—because they are incompatible with fundamental rights. The designation of judicial and law-enforcement AI as “high-risk” means that tools such as predictive policing software or decision-support systems must undergo prior conformity assessments and continuous monitoring to ensure compliance. The EU Artificial Intelligence Act entered into force on 1 August 2024 and will become fully applicable on 2 August 2026. Germany, as an EU member, will apply its provisions directly, while Ukraine, as a candidate state, is preparing its legislation to align with them.

The Council of Europe has likewise issued influential ethical recommendations on the use of AI in judicial systems, which are recognised by both Germany and Ukraine. The European Ethical Charter on the Use of AI in Judicial Systems⁵ (adopted by CEPEJ in 2018) identifies five guiding principles: (1) respect for fundamental rights; (2) non-discrimination; (3) quality and security; (4) transparency and impartiality; and (5) user control. In essence, these principles require that any application of AI respect the rights guaranteed by the European Convention on Human Rights, avoid perpetuating bias or injustice, function reliably and securely, remain open to scrutiny—both in terms of its operation and in ensuring that judicial impartiality is not undermined—and remain subject to the final authority of human judicial actors.

In 2024, the Council of Europe also opened for signature the world’s first binding international treaty on AI: the Framework Convention on AI and Human Rights.⁶ This instrument obliges signatory states to adopt safeguards proportionate to the risks posed by AI systems, ensure effective remedies for individuals affected by AI-based decisions, and preserve judicial independence and the rule of law in the era of automation. Although neither Germany nor Ukraine has yet ratified this newly established convention, its principles reinforce those of the Ethical Charter. Taken together, the EU and Council of Europe instruments establish a common foundation: AI may be used to enhance efficiency and access to justice, but it must not compromise fundamental rights, equality, or the human-centred character of the judiciary.

Beyond the European legal framework, global ethical and policy debates provide additional critical perspectives. UNESCO’s Recommendation on the Ethics of Artificial Intelligence (2021)⁷ and its ongoing Judicial AI Ethics Guidelines Project (2025)⁸ underline concerns

5 CEPEJ, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment* (Council of Europe 2018) <<https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>> accessed 10 August 2025.

6 Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (5 September 2024) CETS 225 <<https://rm.coe.int/1680afae3c>> accessed 10 August 2025.

7 UNESCO, *Recommendation on the Ethics of Artificial Intelligence: Adopted on 23 November 2021* (SHS/BIO/PI/2021/1, UNESCO 2022) <<https://unesdoc.unesco.org/ark:/48223/pf0000381137>> accessed 10 August 2025.

8 UNESCO, *Draft Guidelines for the Use of AI Systems in Courts and Tribunals* (CI/DIT/2025/GL/01, UNESCO 2025) <<https://unesdoc.unesco.org/ark:/48223/pf0000393682>> accessed 10 August 2025.

about fairness, transparency, and human oversight. Interdisciplinary scholarship on AI ethics and digital governance⁹ similarly emphasises accountability gaps, opacity, and the societal risks of overreliance on algorithms. Integrating these perspectives situates the experiences of Germany and Ukraine within a broader global conversation on responsible AI, highlighting that the challenges at stake are not only legal but also ethical and societal. Complementing these debates, the OECD/G20 AI Principles (2019)¹⁰ further underline global consensus on human-centred values, transparency, robustness, and accountability.

These principles—endorsed by leading economies—situate the European and national experiences of Germany and Ukraine within a truly international governance landscape.

4 GERMANY: USE CASES, REGULATION, AND DEVELOPMENT PATHWAYS

Germany has adopted a proactive yet cautious stance towards the integration of AI into its judicial system, characterised by close coordination between federal and state authorities (Bund und Länder). In June 2025, for example, the justice ministers of the federal government and all 16 Länder issued a Joint Declaration on the Use of AI in the Judiciary, setting the tone for future adoption.¹¹ The declaration commits the German judiciary to employing AI in a manner that is “responsible, comprehensible, and reliable,” highlighting its potential to enhance efficiency in routine tasks and in handling cases with substantial information volumes, while making it unequivocally clear that AI is not to replace judges or judicial discretion. In other words, every algorithm is to remain a tool for human decision-makers rather than a decision-maker in itself. The joint strategy also emphasises the importance of transparency and accountability for any AI deployed within the courts.

This high-level policy is reinforced by concrete national initiatives. The federal Digital Summit Communiqué introduced the modernisation program *Justice 4.0*, which envisions the development of a nationwide platform for court translations (to support multilingual proceedings), the exploration of a large language model (LLM) owned by the judiciary for legal research, and the creation of a unified IT architecture for the justice system. A tangible outcome is the establishment of a secure nationwide judicial cloud,

9 Luciano Floridi and Josh Cowl, 'A Unified Framework of Five Principles for AI in Society' (2019) 1(1) *Harvard Data Science Review* 1. doi:10.1162/99608f92.8cd550d1; Brent Mittelstadt, 'Principles Alone Cannot Guarantee Ethical AI' (2019) 1 *Nature Machine Intelligence* 501. doi:10.1038/s42256-019-0114-4.

10 G20, 'G20 Ministerial Statement on Trade and Digital Economy; Annex: G20 AI Principles' (9 June 2019) <<https://oecd.ai/en/wonk/documents/g20-ai-principles>> accessed 10 August 2025; OECD, *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449, OECD Legal Instruments 2025) <<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>> accessed 10 August 2025.

11 Justizminister von Bund und Ländern, 'Gemeinsame Erklärung zum Einsatz von KI in der Justiz' (June 2025) <https://justiz.de/laender-bund-europa/bund_laender/Gemeinsame-Erklaerung-zum-Einsatz-KI/index.php?sessionid=21C24681D0563738863495FD5BA330C2> accessed 10 August 2025.

approved at the end of 2024, designed to host judicial IT services (including future AI tools) within a standardised and secure environment. The judicial cloud is intended to ensure that all AI systems used in German courts remain under national jurisdiction and comply with rigorous data-security protocols.¹²

Within the field of criminal justice, several AI-based tools have been piloted or deployed, though predominantly under the auspices of police forces and judicial administrations rather than by judges in courtrooms. These applications remain limited in scope and are subject to careful evaluation.

First, Germany was among the earliest European jurisdictions to experiment with predictive policing software. Several Länder have piloted systems that analyse crime data to forecast where offences are likely to occur. Bavaria, for example, has employed the PRECOBS (Pre-Crime Observation System) tool to anticipate burglaries; the police in Hesse have used a system known as KLB-operativ; and Berlin briefly tested an instrument called KrimPro.¹³ These programs process historical crime reports and other datasets to detect patterns (such as locations repeatedly targeted by theft) and generate “risk maps” or alerts for law enforcement agencies. In practice, their use has been uneven and their outcomes inconclusive. Baden-Württemberg, for instance, discontinued the testing of PRECOBS, judging its predictive value insufficient to justify the costs and data demands, whereas Bavaria continues to employ it in a limited capacity to optimise patrol distribution for burglary prevention. Preliminary assessments indicate that, although these tools may correlate with modest reductions in property crime in targeted areas, their impact on overall crime rates has been marginal, while concerns persist regarding data quality and “blind spots.”¹⁴ It is noteworthy that such predictive systems are used at the investigative stage, prior to court proceedings, but may nonetheless indirectly affect the course of criminal justice by shaping police focus, arrests, and subsequent prosecutions.¹⁵

Second, German law enforcement authorities are increasingly deploying AI-based tools to filter and analyse vast datasets in criminal investigations. The growing prevalence of digital evidence—from mobile phone data and surveillance camera footage to online communications—has rendered manual review impracticable. AI algorithms are thus used to flag relevant images or messages (for example, in child abuse cases) and to monitor open-

12 Nicola Hauptmann, ‘Aufbau der bundesweiten Justiz-Cloud beschlossen’ (*eGovernment: Verwaltung Digital*, 9 December 2024) <<https://www.egovernment.de/aufbau-der-bundesweiten-justizcloud-beschlossen-a-782965/>> accessed 10 August 2025.

13 ‘PRECOBS - Predictive Policing in German Administrations’ (*IPS-X*, 2018) <<https://ipsoeu.github.io/ips-explorer/case/10433.html>> accessed 10 August 2025.

14 Libuše Hannah Vepřek and others, ‘Legitimising Predictive Policing in Germany’ (2020) 2(3) *Kriminologie* 1. doi:10.18716/ojs/krimoj/2020.3.3.

15 Amelie Spell, ‘The Use of Predictive Policing in German Law Enforcement: A Discourse Analysis’ (Bachelor’s thesis, University of Twente 2023) <<https://purl.utwente.nl/essays/96893>> accessed 10 August 2025.

source information (OSINT) from social networks during investigations. While these tools hold promise for the efficient processing of “big data,” German scholars and practitioners have highlighted significant evidentiary implications. Key concerns include explainability (investigators must understand why the AI flagged particular elements), the integrity of the chain of custody (ensuring that AI processing does not distort or invalidate evidence), and the risk of confirmation bias (where investigators may give disproportionate weight to AI-identified items). In light of these concerns, internal guidelines often require human analysts to review AI outputs, and any new forensic algorithm must undergo legal vetting for compliance with evidentiary rules.¹⁶

Third, within the judiciary, AI adoption has so far been concentrated in civil proceedings, notably in the automated processing of mass debt-collection cases. In criminal justice, the use of AI by judges or prosecutors remains largely experimental. Nonetheless, the Federal Ministry of Justice’s Digitalisation Fund is investing in AI initiatives (*KI-Vorhaben*) that could eventually be extended to criminal proceedings. Current projects include tools for automating the anonymisation of court decisions—a prerequisite for publication—and real-time translation of court hearings. Such instruments could ultimately prove valuable in criminal courts, particularly in cases with international dimensions or sensitive personal data. Additionally, prosecutors are piloting text-analysis algorithms designed to sort and summarise voluminous case materials, such as those arising in complex financial crime investigations.

It is important to stress that no German court or correctional authority employs algorithmic risk-assessment tools in sentencing, bail determinations, or parole decisions—a deliberate departure from U.S. practice.¹⁷ The judiciary has categorically rejected the use of “risk scores” in adjudication, reflecting a legal culture that demands individualised, reasoned judgments by judges and remains sceptical of opaque indicators that could lead to deprivations of liberty.¹⁸ As one observer has noted, criminal justice in Germany remains “judge-centred”: while administrative tasks may be optimised through technology, the act of judicial decision-making itself remains insulated from automation.¹⁹

16 Johanna Sprenger and Dominik Brodowski, “Predictive Policing”, “Predictive justice”, and the Use of AI in the Administration of Justice in Germany’ [2023] *e-Revue Internationale de Droit Pénal* 117. doi:10.22028/D291-39980.

17 Case No 2015AP157-CR *State of Wisconsin v Eric L Loomis* (Wisconsin Supreme Court, 13 July 2016) <<https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690>> accessed 10 August 2025.

18 Ministerium der Justiz des Landes Nordrhein-Westfalen and Landtag Nordrhein-Westfalen, Kooperationsvereinbarung und Werkvertrag für das Vorhaben Generatives Sprachmodell der Justiz (GSJ) im Rahmen der Digitalisierungsinitiative für die Justiz (Drucksache 18/2717, 20 June 2024) <<https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV18-2717.pdf>> accessed 10 August 2025.

19 ‘Justiz: KI soll Richter nicht ersetzen’ (*Move-online*, June 2023). <<https://www.move-online.de/>> accessed 10 August 2025.

Any use of AI within the German justice system is also subject to stringent legal constraints. The German Basic Law (Grundgesetz) enshrines human dignity and the rule of law, which, according to judicial interpretation, prohibit fully automated decision-making in areas that significantly affect individual rights. Combined with Germany's obligations under the European Convention on Human Rights—such as the right to a fair trial and equality before the law—this constitutional backdrop ensures that human judges must remain responsible for sentencing and adjudication. In addition, German data protection law imposes further restrictions: Article 22 of the EU General Data Protection Regulation (GDPR),²⁰ implemented domestically through the Federal Data Protection Act (BDSG),²¹ prohibits decisions that produce legal effects for individuals from being based solely on automated processing, except in narrowly defined circumstances. This means that if an AI system is used to assist decision-making in a criminal case, a human official must carefully review and approve the outcome rather than merely rubber-stamp the algorithm's result. The use of profiling or predictive analytics is further subject to the GDPR's principles of necessity and proportionality.

Beyond these binding legal requirements, Germany has also issued political recommendations on the deployment of AI. The 2025 Joint Declaration of the Federal Government and the Länder sets out clear red lines: AI tools may be used to enhance efficiency in routine processes, but “in all cases the independence of the judge and his or her decision-making authority must remain inviolable,” and all AI outputs must be explainable and verifiable.²² The declaration and related policy documents also foresee accountability mechanisms, including documentation and audit trails for each AI system used. Meanwhile, ethics councils and professional associations (including judicial associations) are drafting guidelines for AI. These include recommendations that every algorithmic tool should be tested for bias prior to use, that judges should be trained in the limitations of AI, and that defendants or counsel should be informed if AI has been used to analyse evidence in their cases. Although these guidelines are not yet legally binding, they reflect Germany's strong inclination toward caution in the use of AI in criminal justice—an effort to gradually increase efficiency while rigorously safeguarding constitutional rights.

20 Regulation (EU) 2016/679 of the European Parliament and of the Council ‘On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)’ (27 April 2016) [2016] OJ L 119/1 <<http://data.europa.eu/eli/reg/2016/679/oj>> accessed 10 August 2025.

21 Federal Data Protection Act (BDSG) (30 June 2017) <https://www.gesetze-im-internet.de/englisch_bdsge/> accessed 10 August 2025.

22 Justizminister von Bund und Ländern, ‘Gemeinsame Erklärung (n 11).

5 UKRAINE: USE CASES, REGULATION, AND DEVELOPMENT PATHWAYS

Ukraine's judicial and legal system has demonstrated openness to technological innovation while deliberately establishing ethical boundaries from the outset. In September 2024, the Judicial Council of Ukraine amended the national Code of Judicial Ethics by introducing a new Article 16 addressing the use of AI.²³ This provision permits judges to employ AI tools in their work only under strict conditions: the use of AI must neither compromise judicial independence or impartiality, nor affect the evaluation of evidence or the substance of judicial decisions, nor breach existing laws.

In effect, Ukraine has codified the principle of the “exclusively supportive use” of AI in adjudication. Judges may, for instance, utilise an AI-powered translation service or a tool for legal research, but they are expressly prohibited from delegating to AI the assessment of evidence or the determination of guilt or innocence. This position has been underscored in public statements by the judiciary, which has repeatedly affirmed that technology will not replace human reasoning. Commentators note that this approach is consistent with European ethical standards and helps reinforce public trust during a period of rapid transformation.²⁴

Ukrainian legal scholars and reformers are actively debating the future integration of AI into the judicial system. Many argue that rules and legislation must be formalised now—before the widespread adoption of AI—in order to prevent ethical violations. For example, Zhukevych, Moskvych, Manhora et al. emphasise the growing importance of establishing a comprehensive legal framework for the use of AI in judicial proceedings and law enforcement, underscoring that the introduction of such technologies must be accompanied by clear legal safeguards.²⁵ Others highlight the potential benefits of AI. A striking example is the empirical study by Izarova and colleagues, which explored the application of AI-driven precedent analysis to the Unified State Register of Court Decisions.²⁶ This national archive, containing more than 100 million judicial decisions, has

23 Decision of the Congress of Judges of Ukraine 'On Approval of the Code of Judicial Ethics' of 22 February 2013 (amended 18 September 2024) <<https://zakon.rada.gov.ua/rada/show/n0001415-13#Text>> accessed 10 August 2025.

24 Ian Bernaziuk, 'Artificial Intelligence and the Judicial System of Ukraine: Results of Cooperation in the Past Year: Presentation' (JAR-Association Conference “Judicial Systems in Transition: Reforms, Innovations and Justice”, JAR-Association, OMIJ, Faculty of Law University of Limoges, 11 June 2025) <https://court.gov.ua/storage/portal/supreme/prezentacii_2025/AI_Ukraine_bernaziuk.pdf> accessed 10 August 2025; Yuliia Moskvytyn and Agne Limante, 'Integrating Artificial Intelligence in Ukraine's Courts: State of Play and Future Prospect' (*Verfassungsblog*, 12 December 2024) <<https://verfassungsblog.de/ai-ukraine-judiciary/>> accessed 10 August 2025.

25 Ihor Zhukevych and others, 'Analysis of Issues Related to the Legalization of Artificial Intelligence, Its Use in Legal Proceedings, Legal Consultation and Law Enforcement' (2024) 27 *Legal Scientific Journal* 17.

26 Iryna Izarova and others, 'Advancing Sustainable Justice Through AI-Based Case Law Analysis: Ukrainian Experience' (2024) 7(1) *Access to Justice in Eastern Europe* 127. doi:10.33327/AJEE-18-7.1-a000123.

proven to be an unparalleled resource for identifying systemic deficiencies, developing predictive models for case outcomes, and providing an objective empirical foundation for judicial reform. These discussions frequently point out that Ukraine's aspiration to join the European Union provides a strong incentive to align national legislation with EU trends in AI governance, while simultaneously adapting legal solutions to the post-Soviet legal culture and the current realities of the country.

Despite difficult circumstances, Ukraine has already introduced several noteworthy applications of AI in criminal justice. One of the earliest was the 2020 launch of *Cassandra*, an algorithm developed by the State Probation Service under the Ministry of Justice²⁷ to predict the risk of recidivism among convicted offenders eligible for probation or early release. Probation officers input data from structured questionnaires covering the offender's biography, the nature of the offence, and behavioural characteristics, after which the system generates a risk assessment intended to guide decisions on the level of supervision or recommendations to courts regarding release. Officials describe the system as a hybrid decision-support tool that combines human judgment with algorithmic suggestions.²⁸

However, limited public information is available regarding *Cassandra's* internal operation or accuracy. Neither the full list of input variables nor evaluations of its prediction accuracy have been published. This lack of transparency has prompted criticism from civil society and academia, who express concern about possible biases or errors in the algorithm that could influence judicial decision-making. Questions remain unanswered: Does *Cassandra* disproportionately classify certain groups as high-risk? How does it account for socio-economic factors? The absence of transparency reinforces calls for greater openness concerning the tool's design and operation.²⁹

The judiciary has likewise embraced AI to enhance its capacity for legal research and to overcome linguistic barriers. In 2025, the Supreme Court of Ukraine modernised its Unified Legal Positions database by incorporating an AI-based search engine and even experimental generative AI functions designed to assist judges and clerks in rapidly locating relevant precedents and summaries of legal principles. The system employs natural language processing, allowing users to submit queries in plain Ukrainian (or potentially in English) and receive concise answers or lists of relevant cases—resembling, in some respects, an advanced legal chatbot. In addition, the Supreme Court has developed an AI-powered translation service for judicial documents and decisions, including a module trained on previous translations of European Court of Human Rights judgments to ensure accuracy in

27 Fair Trials, *Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe* (Fair Trials 2021) <<https://www.fairtrials.org/articles/publications/automating-injustice/>> accessed 10 August 2025.

28 Johanna Jacobson, 'Algorithmic Risk Assessment Tools in Criminal Proceedings: An Analysis in Light of Articles 6 and 14 of the European Convention on Human Rights' (Master's thesis, Uppsala University 2022).

29 Moskvytyn and Limante (n 24).

Ukrainian legal terminology. These innovations are clearly designed to improve productivity: they save time in legal research and ensure that parties receive information in their own language, but they play no role in judicial decision-making itself. Their rollout was accompanied by training sessions for judges, and early reports reflect cautious enthusiasm: judges value the assistance in navigating vast jurisprudential archives, yet remain acutely aware that the responsibility for legal reasoning rests exclusively with them.³⁰

In contrast to Germany, Ukraine has not yet introduced predictive policing or other AI-driven investigative methods on a significant scale. This is partly due to limited resources and institutional capacity, partly due to the ongoing war, which has shifted national priorities. Nonetheless, Ukrainian law enforcement has been exploring the potential of AI in specific areas. Pilot projects have investigated the use of machine learning to match ballistic evidence or to detect suspicious financial transactions linked to corruption. Academic discussions have also considered the possible use of facial recognition or video analytics for suspect identification and public security monitoring. Yet, as of 2025, such ideas remain at the stage of pilot projects or proposals—publicly available information indicates that the Ukrainian police do not operate any predictive AI systems. In fact, the wartime environment, mass displacement of the population, and exceptional circumstances have significantly hindered the adoption of new technologies in policing. Apart from Cassandra and the aforementioned judicial tools, AI in Ukrainian criminal justice thus remains at an early stage of development. This situation creates a certain ambiguity: on the one hand, Ukraine can observe and learn from the experiences (and mistakes) of other countries before implementing AI domestically; on the other, the risk remains that Ukrainian authorities may import solutions developed abroad—whether by private suppliers or international partners—that fail to reflect domestic legal specificities if internal regulatory frameworks do not keep pace.³¹

Overall, Ukraine's legal framework for AI in criminal proceedings continues to evolve, combining general legislation, ethical codes, and the influence of European standards that are currently shaping practice. In the absence of a specific Ukrainian statute regulating AI, oversight is grounded in existing legal principles. The Constitution of Ukraine guarantees the right to a fair trial and respect for human dignity—providing a fundamental safeguard against any uncontrolled automated decision-making that might compromise these rights. The national Data Protection Act, which largely mirrors the principles of the European GDPR, likewise discourages fully automated profiling in criminal matters without consent or explicit legal authorisation. Moreover, as a member of the Council of Europe, Ukraine is politically and legally bound to observe instruments such as the CEPEJ Ethical Charter (not legally binding but normatively persuasive) and the jurisprudence of the European Court of Human Rights. For example, if an AI tool were to be deployed in a way that undermined the

30 Bernaziuk (n 24).

31 Oleksandr Halahan and others, 'Digitalization of the Criminal Process: Is for the Better?' (2023) 38 IDP Revista de Internet, Derecho y Política 1. doi:10.7238/idp.v0i38.408495.

fairness of a trial, such use could amount to a violation of Article 6 of the European Convention on Human Rights.³²

The Code of Judicial Ethics (Article 16) effectively establishes a strict limitation: judges may not delegate their decision-making authority to AI, particularly with regard to the evaluation of evidence or the rendering of judgments. This rule functions as a safeguard in the adjudicatory phase of proceedings. By contrast, the use of AI at earlier stages—such as by the police or within correctional institutions—is being closely monitored. Observers emphasise that, absent reliable safeguards, AI should remain a purely supportive instrument in criminal proceedings.³³

The *Cassandra* example encapsulates many of these concerns. Issues of bias (does the algorithm overestimate risks for certain minorities?), transparency (can defendants challenge the manner in which their risk is calculated?), and contestability (what remedies are available to individuals who believe a decision influenced by AI was unjust?) are central to the Ukrainian debate and echo broader European discussions about algorithmic justice. In response, there have been growing calls for Parliament to adopt legislation specifically addressing AI in the judiciary.³⁴ Such a framework could, for instance, clarify the evidentiary status of AI-generated materials (for example, whether they constitute expert evidence or merely recommendations), establish transparency obligations (including disclosure to defendants), and establish oversight mechanisms such as certification or judicial council approval.

As of 2025, Ukraine stands at a crossroads. While it broadly endorses European principles and has introduced ethical restrictions, concrete legislative measures and systematic oversight mechanisms have yet to catch up with the few AI tools already in use.

6 SAFEGUARDING RIGHTS, EVIDENCE, AND FAIR TRIAL STANDARDS

Having outlined the introduction and governance of AI in Germany and Ukraine, the discussion now turns to several cross-cutting issues that are fundamental to ensuring that the deployment of AI in criminal justice does not undermine fundamental rights or the integrity of legal processes. These include algorithmic bias and explainability, the

32 Tetyana Antsupova and Sergii Koziakov, 'News Digest No 2 on Ukraine Judiciary: (research project The Dynamics of the Judiciary in Ukraine in the Context of the Rule of Law and the EU Accession Aspirations, September 15 – October 15, 2024)' (*Bingham Centre for the Rule of Law*, 19 August 2025) <<https://binghamcentre.biicl.org/newsitems/185/news-digest-no-12-on-ukraine-judiciary>> accessed 21 August 2025.

33 Oksana Kaplina and others, 'Application of Artificial Intelligence Systems in Criminal Procedure: Key Areas, Basic Legal Principles and Problems of Correlation with Fundamental Human Rights' (2023) 6(3) *Access to Justice in Eastern Europe* 147. doi:10.33327/AJEE-18-6.3-a000314

34 Zhukevych and others (n 25).

implications of predictive policing for the presumption of innocence and proportionality, and the challenges posed by evidence generated or processed by AI.

The risk of algorithmic bias constitutes a central concern in the use of AI within criminal justice. Both Germany and Ukraine remain mindful of cautionary examples from other jurisdictions, particularly the United States, where investigations into the COMPAS risk-assessment tool revealed that Black defendants were disproportionately classified as high-risk compared to white defendants. Such findings underscore the danger that AI systems may unintentionally entrench or even exacerbate historical biases embedded in data. If left unaddressed, this risk could undermine the principle of equality before the law.³⁵

Accordingly, in Europe, explainability and contestability are regarded as non-negotiable safeguards. The EU Artificial Intelligence Act effectively requires that high-risk AI systems—such as those deployed in the justice sector—be designed with explainability in mind, meaning their outputs must be interpretable and understandable to humans and subject to continuous human oversight.³⁶ Similarly, the Council of Europe standards demand transparency concerning the functioning of AI instruments.³⁷

From a practical perspective, explainability is essential to ensure that judges, lawyers, and defendants can understand the recommendations produced by AI. For instance, if Ukraine's Cassandra tool classifies a probationer as "high risk," the probation officer and the court must be able to determine whether this assessment was driven by the individual's prior convictions, employment status, or some other factor—and this must be communicated in accessible language rather than as a mere numerical score. Contestability goes hand in hand with explainability: the affected person (or their counsel) must have the opportunity to challenge the algorithm's suggestion. At present, however, neither Germany nor Ukraine has clear procedural rules for contesting AI-generated information in court.³⁸ One can imagine, for example, a defence lawyer filing a motion to disclose the parameters of the algorithm or requesting an expert to scrutinise its methodology. In practice, a robust system might in the future require that any use of AI in criminal proceedings be disclosed to all parties, with input and output records preserved for potential review. Such measures would safeguard the right to a fair trial in the age of AI: ensuring that no decision rests on blind reliance on a machine, and that every statement influencing a case can be examined and contested.³⁹

Predictive policing tools, such as those currently tested in Germany, raise unique legal and ethical challenges. One concern relates to proportionality: the deployment of resource-

35 Julia Angwin and others, 'Machine Bias' (*ProPublica*, 23 May 2016) <<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>> accessed 10 August 2025.

36 Regulation (EU) 2024/1689 (n 3).

37 Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (n 6).

38 Fair Trials (n 27).

39 Jacobson (n 28).

intensive, privacy-invasive surveillance measures on the basis of algorithmic forecasts must demonstrably yield tangible security benefits to justify their impact on citizens' privacy and freedom of movement.⁴⁰ German experiments with predictive policing to date have shown, at best, modest benefits—such as slight reductions in theft in certain areas—casting doubt on the compatibility of such systems with the constitutional requirements of necessity and proportionality. A further issue concerns the presumption of innocence and the closely related principle that law enforcement authorities must not pursue individuals without concrete suspicion. Is it sufficient, for instance, for an algorithm to identify a “high-risk area” or a “high-risk person” on the basis of data correlations to initiate a police investigation? German legal doctrine tends towards a negative answer: algorithmic risk profiles alone cannot substitute for individualised suspicion.⁴¹ As a result, tools such as PRECOBS have been deliberately confined to supplementing, rather than replacing, traditional investigative methods, and police are generally instructed not to arrest or prosecute individuals solely because an algorithm flagged them.⁴²

To safeguard rights in this context, experts recommend multi-layered oversight. In Germany, any sustained use of predictive policing algorithms must be accompanied by regular independent evaluations of their effectiveness and bias. A Data Protection Impact Assessment (DPIA) is, or soon will be, mandatory under the Artificial Intelligence Act and the GDPR whenever such tools are used extensively to process personal data, thereby ensuring thorough scrutiny of their privacy implications. Furthermore, proposals have been made to involve local legislatures or city councils in authorising and reviewing predictive policing pilot projects, in order to provide democratic oversight. Ukraine, by contrast, has not yet introduced predictive policing, giving it the advantage of learning before taking that step. Should Ukrainian authorities consider deploying such instruments (perhaps to relieve overburdened police forces), they could develop a legal framework in advance—for example, requiring judicial authorisation for certain types of AI-based surveillance, or imposing a moratorium on predictive systems until thorough public consultations and pilot studies have been completed.

In both countries, it is essential that crime prediction algorithms, if used, do not become covert tools of profiling or arbitrary enforcement. Predictive alerts should ideally be treated as leads requiring traditional verification, with human judgment firmly at the forefront of law enforcement—consistent with both Germany's and Ukraine's emphasis on human oversight in criminal justice.

With the growing prevalence of AI tools, courts will increasingly encounter evidence generated, influenced, or processed by algorithms. This may include, for example, AI-based translations of foreign-language materials, transcripts of audio recordings produced by

40 Vepřek and others (n 14).

41 Spell (n 15).

42 PRECOBS (n 13).

speech-recognition software, or AI-enhanced images—such as sharpened surveillance footage. In the near future, such issues may extend even further, encompassing the need to detect “deepfake” audio or video fabrications. German and Ukrainian courts alike will need to adapt evidentiary rules to meet these scenarios.

A pressing concern is authentication: how can a court be confident that a digital exhibit is genuine and has not been altered by AI? And if it has been altered—even for ostensibly legitimate purposes such as enhancing clarity—how should this affect its admissibility or evidentiary weight? At present, Germany has no official protocol governing AI-modified evidence, though these questions are increasingly acknowledged. Scholars caution that judges must remain vigilant regarding the provenance of digital materials and may require expert assistance in verifying authenticity. For instance, if prosecutors present a video that has been enhanced or edited by software, the defence should be entitled to review the original and to question an expert about the reliability of the software used.

Another issue concerns the interpretation of AI-generated results submitted as evidence. Suppose an algorithm scans a hard drive and flags 1,000 out of 50,000 images as likely illegal. Should these flagged files automatically be accepted as proof of an offence? Certainly not: human investigators must review each image individually, and in court the mere fact that the algorithm pre-selected them may be irrelevant—or even prejudicial—if not handled with caution. In Ukraine, where digital forensics is still in its infancy, reliance on AI tools supplied by external partners (for example, Interpol or Europol instruments in combating cybercrime) means that Ukrainian courts sometimes receive analytical reports not produced domestically. Judges, therefore, require guidance from the Ministry of Internal Affairs on how to handle such evidence.

Both countries would benefit from publishing practical guidelines or handbooks for judges on AI-related evidence. Such guidance might include: obligations to disclose any use of AI in evidence processing; guarantees that the defence has an opportunity to examine the algorithm or its outputs; and instructions that any uncertainty arising from AI processing should be resolved in favour of the defendant, consistent with the principle of *in dubio pro reo*. As a proactive measure, the Federal Ministry of Justice in Germany could convene a working group to examine these questions and propose necessary amendments to evidentiary rules. Ukraine, which often looks to Germany and other European states for models of best practice, could adopt similar measures.

In all cases, safeguarding the integrity of fact-finding remains paramount: AI must not become a “black box” through which evidence is introduced into court without being subjected to the same adversarial scrutiny as evidence produced by human means.

7 CONCLUSION

The introduction of artificial intelligence into criminal justice is a delicate undertaking, as illustrated by the approaches taken in Germany and Ukraine. Both countries are introducing AI incrementally—Germany through carefully controlled initiatives emphasising infrastructure and administrative efficiency, and Ukraine through targeted tools combined with explicit ethical restrictions. In neither jurisdiction is there any rush to delegate core judicial powers to algorithms. On the contrary, there is a clear commitment to maintaining a “human-in-the-loop” approach, consistent with European values and international recommendations. This reflects the shared understanding that, regardless of their sophistication, algorithmic systems lack the moral judgment, accountability, and contextual reasoning that human judges and officials bring to the judicial process.

The challenges, however, remain substantial. Germany’s experience shows that even seemingly narrow applications such as predictive policing can raise complex questions of oversight and rights protection, while Ukraine’s early adoption of a risk-assessment tool highlights the difficulties of ensuring transparency and public trust under conditions of limited resources. Both jurisdictions must translate high-level principles into practice: Germany by carrying out audits and evaluations, potentially restricting or recalibrating tools that fail to meet legal standards, and Ukraine by reinforcing its framework through legislation and independent oversight to prevent gaps as technologies expand. The entry into force of the EU Artificial Intelligence Act is likely to accelerate these developments by establishing a regulatory structure that underpins many of the issues discussed in this article.

What emerges is that AI-based technologies carry both promise and peril, particularly with respect to the protection of human rights. Their introduction requires a precise and optimal balance.

The comparative analysis of Germany and Ukraine underscores that the responsible integration of AI in criminal justice requires a principled, thematic approach. The following recommendations, grouped under core themes, provide a practical framework for policymakers and judicial actors:

1. Human-Centred Justice. AI may support information processing, but must never substitute for judicial reasoning. Decisions affecting rights and liberties must remain attributable to human judges or officials, ensuring dignity, accountability, and individualised reasoning.

2. Transparency and Explainability. The deployment and operation of AI tools should be publicly documented, with clear model cards or equivalent documentation. In court proceedings, parties must receive case-specific explanations of AI outputs to allow meaningful contestation. Black-box systems are incompatible with the criminal justice system.

3. Accountability and Oversight. Every AI tool should have a designated authority responsible for its operation, subject to regular internal and external audits. Independent oversight bodies—such as data protection authorities or ethics councils—must have powers to investigate and enforce recommendations. Logs of AI processes should be preserved for potential review.

4. Data Protection and Privacy. Given the sensitivity of personal and biometric data in criminal justice, systems must comply with the highest standards of data minimisation, anonymisation, and cybersecurity. Secondary use of judicial data, particularly for commercial training purposes, should be strictly prohibited unless expressly authorised.

5. Scope and Proportionality. AI programs must be legally authorised for a defined purpose and not repurposed without renewed scrutiny. Predictive policing or surveillance tools should be deployed only as pilot projects, subject to proportionality tests and democratic authorisation.

Ultimately, the comparative analysis of Germany and Ukraine underscores that “intelligent” criminal justice is not about replacing human judgment with machine calculations but about finding safe and effective ways to assist judges, lawyers, and law enforcement. Thoughtfully implemented, AI can indeed enhance efficiency by filtering data, reducing delays, and promoting consistency. Implemented carelessly, however, it risks undermining rights and eroding trust in the justice system. The way forward, as both countries demonstrate, lies in a balanced approach: embracing innovation while embedding every step in oversight, transparency, and an unwavering commitment to the values of justice.

This perspective resonates with broader global debates: UNESCO’s ethical frameworks and interdisciplinary AI governance research converge on the same imperative—embedding transparency, fairness, and human accountability at the heart of judicial innovation.⁴³ This alignment is further reinforced by the OECD/G20 AI Principles⁴⁴ and interdisciplinary analyses from political science and philosophy, which emphasise the broader societal risks of opacity, accountability gaps, and the erosion of trust.⁴⁵ These perspectives extend the comparative findings of this article into the wider global conversation on responsible AI governance. In an era of rapid technological change, preserving a human-centred judiciary and respect for rights is both the most significant challenge and the ultimate goal.

43 UNESCO (n 7); Floridi and Cowls (n 9).

44 G20 (n 10); OECD (n 10).

45 Joanna J Bryson, ‘The Past Decade and Future of AI’s Impact on Society’ in *Towards a New Enlightenment?: A Transcendent Decade* (Turner 2019); Corinne Cath, ‘Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges’ (2018) 376(2133) *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20180080. doi:10.1098/rsta.2018.0080.

REFERENCES

1. Angwin J and others, 'Machine Bias' (*ProPublica*, 23 May 2016) <<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>> accessed 10 August 2025
2. Antsupova T and Koziakov S, 'News Digest No 2 on Ukraine Judiciary: (research project The Dynamicsof the Judiciary in Ukraine in the Context of the Rule of Law and the EU Accession Aspirations, September 15 – October 15, 2024)' (*Bingham Centre for the Rule of Law*, 19 August 2025) <<https://binghamcentre.biicl.org/newsitems/185/news-digest-no-12-on-ukraine-judiciary>> accessed 10 August 2025
3. Bernaziuk I, 'Artificial Intelligence and the Judicial System of Ukraine: Results of Cooperation in the Past Year: Presentation' (JAR-Association Conference "Judicial Systems in Transition: Reforms, Innovations and Justice", JAR-Association, OMIJ, Faculty of Law University of Limoges, 11 June 2025) <https://court.gov.ua/storage/portal/supreme/prezentacii_2025/AI_Ukraine_bernaziuk.pdf> accessed 10 August 2025
4. Bryson JJ, 'The Past Decade and Future of AI's Impact on Society' in *Towards a New Enlightenment?: A Transcendent Decade* (Turner 2019)
5. Cath C, 'Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges' (2018) 376(2133) *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20180080. doi:10.1098/rsta.2018.0080
6. Floridi L and Cowls J, 'A Unified Framework of Five Principles for AI in Society' (2019) 1(1) *Harvard Data Science Review* 1. doi:10.1162/99608f92.8cd550d1
7. Halahan O and others, 'Digitalization of the Criminal Process: Is for the Better?' (2023) 38 *IDP Revista de Internet, Derecho y Política* 1. doi:10.7238/idp.v0i38.408495
8. Izarova I and others, 'Advancing Sustainable Justice Through AI-Based Case Law Analysis: Ukrainian Experience' (2024) 7(1) *Access to Justice in Eastern Europe* 127. doi:10.33327/AJEE-18-7.1-a000123
9. Jacobson J, 'Algorithmic Risk Assessment Tools in Criminal Proceedings: An Analysis in Light of Articles 6 and 14 of the European Convention on Human Rights' (Master's thesis, Uppsala University 2022).
10. Kaplina O and others, 'Application of Artificial Intelligence Systems in Criminal Procedure: Key Areas, Basic Legal Principles and Problems of Correlation with Fundamental Human Rights' (2023) 6(3) *Access to Justice in Eastern Europe* 147. doi:10.33327/AJEE-18-6.3-a000314
11. Kiesow Cortez E and Maslej N, 'Adjudication of Artificial Intelligence and Automated Decision-Making Cases in Europe and the USA' (2023) 14(3) *European Journal of Risk Regulation* 457. doi:10.1017/err.2023.61

12. Mittelstadt B, 'Principles Alone Cannot Guarantee Ethical AI' (2019) 1 Nature Machine Intelligence 501. doi:10.1038/s42256-019-0114-4
13. Moskvityn Yu and Limante A, 'Integrating Artificial Intelligence in Ukraine's Courts: State of Play and Future Prospect' (*Verfassungsblog*, 12 December 2024) <<https://verfassungsblog.de/ai-ukraine-judiciary/>> accessed 10 August 2025
14. Shi C, Sourdin T and Li B, 'The Smart Court – A New Pathway to Justice in China?' (2021) 12(1) International Journal for Court Administration 4. doi:10.36745/ijca.367
15. Spell A, 'The Use of Predictive Policing in German Law Enforcement: A Discourse Analysis' (Bachelor's thesis, University of Twente 2023)
16. Sprenger J and Brodowski D, "'Predictive Policing", "Predictive justice", and the Use of AI in the Administration of Justice in Germany' [2023] e-Revue Internationale de Droit Pénal 117. doi:10.22028/D291-39980
17. Vepřek LH and others, 'Legitimising Predictive Policing in Germany' (2020) 2(3) Kriminologie 1. doi:10.18716/ojs/krimoj/2020.3.3
18. Zhukevych I and others, 'Analysis of Issues Related to the Legalization of Artificial Intelligence, Its Use in Legal Proceedings, Legal Consultation and Law Enforcement' (2024) 27 Legal Scientific Journal 17

AUTHORS INFORMATION

Lidiia Moskvych*

Dr Sc (Law), Professor, Associate Professor of the Department of Criminal Procedure, Faculty of Prosecutor's Office, Yaroslav Mudryi National Law University, Kharkiv, Ukraine
l.m.moskvych@nlu.edu.ua

<https://orcid.org/0000-0001-7339-3982>

Corresponding author, responsible for research methodology, writing and management.

Competing interests: No competing interests were reported.

Disclaimer: The author declares that her opinions and views expressed in this manuscript are free from any influence of any organization, including the Constitutional Court of Ukraine, despite the fact that she is a member of the Scientific Advisory Council of the Constitutional Court.

Iryna Borodina

Cand. of Science of Law (Equiv. Ph.D.), Associate Professor, Associate Professor of the Department of Criminal Procedure, Faculty of Prosecutor's Office, Yaroslav Mudryi National Law University, Kharkiv, Ukraine

i.v.borodina@nlu.edu.ua

<https://orcid.org/0009-0008-7611-6575>

Co-author, responsible for data collection and writing.

Competing interests: No competing interests were announced by the author.

Disclaimer: The author declares that her opinion and views expressed in this manuscript are free of any impact of any organizations.

Olga Ovsiannikova

Cand. of Science of Law (Equiv. Ph.D.), Associate Professor, Associate Professor of the Department of Criminal Procedure, Faculty of Prosecutor's Office, Yaroslav Mudryi National Law University, Kharkiv, Ukraine
o.o.ovsiannikova@nlu.edu.ua

<https://orcid.org/0000-0001-7773-6487>

Co-author, responsible for data collection and writing.

Competing interests: No competing interests were announced by the author.

Disclaimer: The author declares that her opinion and views expressed in this manuscript are free of any impact of any organizations.

RIGHTS AND PERMISSIONS

Copyright: © 2025 Lidiia Moskvych, Iryna Borodina and Olga Ovsiannikova. This is an open access article distributed under the terms of the Creative Commons Attribution License, (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

EDITORS

Managing editor – Mag. Bohdana Zahrebelna. **English Editor** – Julie Bold.

Ukrainian language Editor – Lilia Hartman.

ABOUT THIS ARTICLE

Cite this article

Moskvych L, Borodina I and Ovsiannikova O, ‘Artificial Intelligence in Criminal Justice in Germany and Ukraine: A Comparative Legal Study’ (2025) 8(Spec) Access to Justice in Eastern Europe 210-32 <<https://doi.org/10.33327/AJEE-18-8.S-a000155>> P

DOI: <https://doi.org/10.33327/AJEE-18-8.S-a000155>

Summary: 1. Introduction. – 2. Methodology. – 3. Legal and Political Foundations in Europe. – 4. Germany: Use Cases, Regulation, and Development Pathways. – 5. Ukraine: Use Cases, Regulation, and Development Pathways. – 6. Safeguarding Rights, Evidence, and Fair Trial Standards. – 7. Conclusion.

Keywords: *Artificial Intelligence; Criminal Justice; Predictive Policing; Risk Assessment; Explainability; Data Protection; Human Oversight.*

DETAILS FOR PUBLICATION

Date of submission: 03 Sep 2025

Date of acceptance: 01 Oct 2025

Date of Publication: 30 Dec 2025

Whether the manuscript was fast tracked? - No

Number of reviewer report submitted in first round: 2 reports

Number of revision rounds: 1 round with minor revisions

Technical tools were used in the editorial process:

Plagiarism checks - Turnitin from iThenticate <https://www.turnitin.com/products/ithenticate/>

Scholastica for Peer Review <https://scholasticahq.com/law-reviews>

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ШТУЧНИЙ ІНТЕЛЕКТ У КРИМІНАЛЬНОМУ ПРАВОСУДДІ НІМЕЧЧИНИ ТА УКРАЇНИ: ПОРІВНЯЛЬНО-ПРАВОВЕ ДОСЛІДЖЕННЯ

Лідія Москвич, Ірина Бородіна та Ольга Овсяннікова

АНОТАЦІЯ

Вступ. Штучний інтелект (ШІ) швидко переходить від допоміжних адміністративних інструментів до застосувань, які безпосередньо впливають на функціонування систем кримінального правосуддя. У Європі цей процес відбувається в межах обережного, правоорієнтованого підходу, покликаного поєднати інновації з дотриманням принципів незалежності суду, справедливості та верховенства права. Дослідження пропонує порівняльно-правовий аналіз впровадження ШІ у системи кримінального правосуддя Німеччини та України в контексті Акту ЄС про штучний інтелект (2024), стандартів

Ради Європи та конституційних гарантій. Структурований і скоординований на федеральному рівні підхід Німеччини контрастує з більш точковою, але етично обмеженою моделлю України, що відображає відмінності інституційних спроможностей і правових традицій.

Методи. Робота ґрунтується на порівняльно-правовому підході, що поєднує функціональний та контекстуальний аналіз. Функціональний аспект виявляє, як Німеччина та Україна застосовують ІІІ для вирішення подібних проблем — підвищення ефективності, прозорості та захисту прав. Контекстуальний аспект розглядає вплив конституційних, інституційних та соціально-політичних чинників, зокрема умов воєнного стану в Україні. Такий комбінований підхід дає змогу оцінювати подібності й відмінності не абстрактно, а в контексті європейської та національних правових культур.

Аналіз базується на законодавстві, офіційних звітах, судовій практиці та наукових джерелах. Емпіричну базу становлять, зокрема, німецькі пілотні проекти у сфері прогностичної поліцейської діяльності (PRECOBS, KLB-operativ), інструменти фільтрації слідчих даних і адміністративні ІІІ-рішення в судах, а також український алгоритм оцінки ризиків у пробації Cassandra та ІІІ-інструменти для правничих досліджень і перекладу. Досвід Сполучених Штатів щодо алгоритмічної оцінки ризиків використовується як застережливий орієнтир.

Результати та висновки. Дослідження показує, що обидві юрисдикції обмежують використання ІІІ як заміни у процесі прийняття рішень. Водночас у Німеччині використання ІІІ координується на федеральному рівні та обмежується допоміжними функціями — передусім у сфері адміністративної оптимізації й аналітичної підтримки. Натомість в Україні впровадження ІІІ є більш вибірковою і підпорядкованим чітким етичним обмеженням, але ускладнюється нестачею прозорості та об'єктивними обмеженнями, зумовленими воєнним станом. Аналіз виявляє спільні проблеми, зокрема алгоритмічну упередженість, пояснюваність рішень, допустимість доказів і забезпечення гарантій справедливого судового розгляду, та формулює рекомендації з урахуванням національного контексту. Серед них — запровадження обов'язкових зовнішніх аудитів, законодавче закріплення процесуальних прав на оскарження даних, згенерованих ІІІ, чіткі правила доказового використання таких даних, а також підвищення обізнаності суддів щодо технологій ІІІ.

Дослідження підкреслює, що сталий розвиток ІІІ у кримінальному правосудді можливий лише за умови його допоміжного характеру, прозорості, можливості аудиту та збереження людського контролю, що є необхідним для відповідності європейським правовим стандартам і захисту основоположних прав.

Ключові слова. Штучний інтелект, кримінальне правосуддя, прогностичні алгоритми у поліцейській діяльності, оцінка ризиків, пояснюваність, захист даних, людський контроль.