

Vlad Barbat, PhD\*

DOI: 10.51204/Zbornik\_UMKP\_25135A  
Originalni naučni rad

## AI AND THE CRIMINAL LAW – MODERN PERSPECTIVES – LEGISLATION AND UNIFICATION IN EUROPE

*Abstract: European criminal law faces both tremendous opportunities and challenges as a result of the incorporation of artificial intelligence (AI) into contemporary society. European judicial systems are under increasing pressure to change as AI systems have a greater impact on fields including digital evidence processing, autonomous decision-making, predictive policing, and surveillance. With an emphasis on legislative responses and the EU's efforts to harmonize, this study examines current viewpoints on the relationship between AI and criminal law. It looks at how well current legal frameworks handle concerns about privacy, accountability, culpability, and due process in criminal scenarios including artificial intelligence. The current article also examines recent EU measures, such as the Digital Services Act and the Artificial Intelligence Act, and analyzes how they affect criminal justice systems. This study emphasizes the need for logical, future-proof regulations that strike a balance between innovation, fundamental rights, and justice by comparing national laws with European attempts at legal unification. The goal of the paper is to add to the continuing discussion about how Europe might create a single legal framework that effectively and morally regulates and uses AI in criminal law.*

**Keywords:** AI, fragmentation, unification, international criminal law standardization, uniformization of the European law, European criminal law future.

### 1. AI AND THE LAW – ORIGINS

AI has radically changed many facets of civilization and brought about previously unheard-of advancements in economics, technology, and social dynamics. Legal systems around the world have faced new difficulties as AI continues

---

\* Vice-Chairman of The Center for European and Interdisciplinary Studies, “Bogdan Voda” University, Romania, PhD in Comparative Law, [vlad\\_barbat@ubv.ro](mailto:vlad_barbat@ubv.ro).

to permeate every aspect of daily life, requiring adaptation and development. Examining early conceptual underpinnings, early regulatory reactions, significant court rulings, and theoretical discussions regarding artificial intelligence's position within preexisting legal frameworks are all necessary to comprehend the beginnings of the intersection of AI and the law.

Alan Turing's groundbreaking 1950 work, "Computing Machinery and Intelligence",<sup>1</sup> which established the Turing Test as a standard for machine intelligence, is largely responsible for the idea of artificial intelligence's inception in the middle of the 20th century. Turing's investigation prepared the way for further philosophical and theoretical discussions over the legal personhood and rights that may be attributed to intelligent machines. Important moral and legal issues pertaining to the accountability, independence, and decision-making abilities of intelligent systems also surfaced during this time.<sup>2</sup>

The name "Artificial Intelligence" was first coined by the Dartmouth Conference in 1956, solidifying AI as a separate academic and scientific field. However, serious legal issues only arose decades later as AI became realistically useful in a variety of fields, mainly in relation to responsibility, intellectual property, data protection, and human rights implications<sup>3</sup>.

### 1.1. Initial Regulatory Responses

AI applications in data-driven technologies, such as automated decision-making systems, were the main cause of the first regulatory measures. As computing and data processing capabilities improved in the 1970s and 1980s, the law started to acknowledge privacy and data protection concerns. The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were one of the first significant regulatory frameworks. They established fundamental ideas that later influenced privacy laws such as the General Data Protection Regulation (GDPR) of the European Union.

Regulatory bodies had to deal with new problems including bias, discrimination, and fairness as AI developed into useful commercial and governmental uses. Early requests for regulatory supervision to prevent unfair or biased outcomes were sparked by AI-driven technologies, particularly algorithmic decision-making and predictive analytics, which raised important questions about algorithmic transparency and accountability.

Important legal precedents were established in the early AI cases, which mostly concerned liability and intellectual property challenges. The legal world notably struggled with the patentability and copyright protection of AI-generated

1 A. Turing, *Computing Machinery and Intelligence*. *Mind*, 1950, 433–460.

2 *Ibid.*, 461.

3 J. McCarthy, M. Minsky, M. N. Rochester, C. E. Shannon, *Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Dartmouth College, 1955, 11–12.

outputs in the early 1990s. In order to challenge conventional ideas of authorship, courts and regulatory agencies engaged in a thorough debate over whether works produced by intelligent machines may be regarded as original intellectual creations worthy of legal protection. The 1996 U.S. Court battle surrounding “Creativity Machine<sup>4</sup>,” in which an inventor sought patent protection for an invention produced automatically by a neural network, was a milestone case in this respect. Despite being contentious at first, the case brought to light fundamental issues with the legal attribution of creativity and invention that are still being discussed today and have an impact.

In a similar vein, liability claims involving autonomous systems were increasingly prevalent in the late 20th and early 21st centuries, especially in the transportation and healthcare industries. Important conversations concerning liability, product responsibility, and safety rules controlling intelligent automated systems were sparked by the notorious “Therac-25” incidents in the 1980s,<sup>5</sup> which involved software failures in a radiation therapy device that led to patient injuries and fatalities. Later legal precedents and regulatory frameworks pertaining to medical gadgets, robotic systems, and driverless cars were impacted by these instances.

## 1.2. Theoretical Discourse and Academic Contributions

Scholars and legal theorists have actively participated in the discussion of AI’s legal ramifications by examining fundamental issues about the personhood, rights, and accountability of AI systems. Early theoretical contributions made by academics like Lawrence Lessig in the late 1990s and early 2000s had a big impact on how people understood the connection between law and technology. Lessig suggested that regulatory frameworks need to change to reflect the inherent features of digital technology, anticipating the need for legal frameworks that can handle the special qualities and dangers presented by sentient machines<sup>6</sup>. The consequences of autonomous decision-making, predictive analytics, and algorithmic biases were the main topics of discussion as academics started to openly address AI from legal and ethical viewpoints.

Theoretical discussions on AI’s revolutionary potential inside legal systems were advanced by the groundbreaking work of Ryan Calo, Jack Balkin, and Mireille

4 M. Csikszentmihalyi, *Creativity: Flow and the psychology of discovery and invention*, Harper/Collins, New York, 1996, 108–109. Article consulted online on the 18. 04. 2025, 1.27 p.m. Link: <https://digitalauthorship.org/wp-content/uploads/2016/01/csikszentmihalyi-chapter-flow-and-creativity.pdf>.

5 OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD Publishing, 1980.

6 L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, 1999, 101–103. Consulted online on the 18. 04. 2025, 1.49. p.m. Link: <https://lessig.org/images/resources/1999-Code.pdf>.

Hildebrandt. They emphasized the need for flexible legal frameworks that guarantee the accountability and transparency of intelligent systems.

Different countries around the world have adopted different strategies for regulating AI, influenced by political, economic, ethical, and cultural factors. The 2018 GDPR,<sup>7</sup> which addressed automated decision-making directly, is an example of how the European Union has become a regulatory leader. Additionally, one of the most thorough initiatives to govern AI technology is the European Commission's 2021 plan for an AI Act, which would classify systems based on risk categories and enforce strict compliance standards for high-risk AI applications.<sup>8</sup>

On the other hand, the United States initially took a more laissez-faire stance, placing a strong emphasis on economic growth and innovation, especially in accordance with directives from the National Institute of Standards and Technology (NIST). But recent increases in federal and state-level regulatory interventions have been spurred by growing privacy, discrimination, and safety concerns, indicating a move toward more monitoring and standardization.

From theoretical investigations to real-world regulatory and judicial conflicts, the history of AI's relationship with law shows a continual progression. As intelligent systems have grown to be essential parts of society, legal issues that were formerly peripheral have now become top policy considerations. The dynamic and intricate interaction between technical innovation and legal governance is shown in this historical review, which emphasizes the need for ongoing legal adaptation in light of AI's revolutionary influence. In an increasingly AI-driven society, the ability of the law to change in tandem with AI's quick developments will have a substantial impact on societal outcomes pertaining to privacy, security, equity, and justice.

## 2. AI AND CRIMINAL LAW – HELP INSTRUMENTS

The use of AI in criminal law began mostly in the intelligence and law enforcement fields. In order to find patterns in criminal behavior, early innovations, which date back to the late 20th century, required using computer methods for analyzing large datasets. More effective systems that could forecast criminal activity, allocate resources, and improve investigation precision were required due to the growing complexity and volume of criminal data. Following the devastating events of September 11, 2001, when governments throughout the world increased their spending in intelligent security technology to combat terrorism and organized crime, the development of AI-driven solutions surged dramatically. Law enforcement organizations now have previously unheard-of predictive

---

7 European Union. (2018). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679.

8 European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. COM/2021/206 final.

skills thanks to developments in machine learning and data analytics, which have produced advanced platforms like crime analytics software and predictive policing algorithms.

## 2.1. The Art of Predictive policing

One of the most hotly contested and extensively used AI-powered technologies in criminal law is predictive policing. This method forecasts possible crime hotspots and periods by utilizing algorithms that examine historical crime data, socioeconomic variables, geographic data, and real-time inputs. Predictive policing is demonstrated by systems such as PredPol<sup>9</sup> and HunchLab,<sup>10</sup> which direct patrol assignments and preventive measures.

To help police forces deploy resources in advance, PredPol, for example, uses statistical algorithms to forecast the areas where violent incidents, thefts, and burglaries are most likely to occur. In a similar vein, HunchLab integrates a variety of data sources, such as social events and weather, to provide detailed prediction insights meant to lower crime through preventative actions. However, there are serious moral and legal questions around the use of predictive policing. Critics contend that algorithmic biases have the potential to worsen socioeconomic and racial disparities by disproportionately affecting underprivileged groups and sustaining discriminatory cycles.<sup>11</sup> Therefore, ongoing human monitoring and transparency in algorithmic decision-making processes are essential for ethical deployment.

The ability of law enforcement to evaluate forensic evidence, decipher surveillance data, and effectively resolve complicated cases is greatly improved by AI-driven investigative analytics tools.<sup>12</sup> Digital forensics, speech analysis, and facial recognition are all supported by AI systems, which significantly improve the precision and effectiveness of investigations. Widely used in criminal investigations, facial recognition technology compares databases of known people with photos taken from surveillance footage. This technology is demonstrated by systems such as Amazon Rekognition and Clearview AI, which offer quick recognition skills that are essential for investigations. However, disputes involving misidentifications and privacy infractions highlight how crucial strict regulation and control are.

---

9 For more information, please consult Tim Lau, *Predictive Policing Explained*, article published and consulted online on the Brennan Center Platform. Link: <https://www.brennan-center.org/our-work/research-reports/predictive-policing-explained>, 18. 04. 2025.

10 For more information, please consult : <https://teamupturn.gitbooks.io/predictive-policing/content/systems/hunchlab.html>, 18. 04. 2025.

11 A. G. Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, NYU Press, 2017, 84–86.

12 S. Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing*, Oxford University Press, Oxford, 2021, 201–202.

Artificial intelligence (AI) algorithms assist investigators in digital forensics by processing large datasets taken from electronic devices and spotting connections and patterns that human analysts would miss. These methods significantly shorten investigation times and increase conviction rates in financial fraud cases, organized criminal networks, and cybercrime investigations.

## 2.2. Judicial decision support systems

AI is being used more and more in court settings to manage caseloads, evaluate risk factors, and guide sentence choices. Judges can make informed decisions about sentencing severity, bail, and parole restrictions by using algorithmic risk assessment tools like COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), which give them data-driven insights about recidivism risks.<sup>13</sup> COMPAS, which is extensively used in U.S. jurisdictions, estimates recidivism risks by using behavioral patterns, demographic data, and offender histories. Advocates contend that these instruments improve the efficiency, consistency, and objectivity of the legal system. Nonetheless, there are still a lot of issues with algorithmic accountability, fairness, and transparency. Racial disparities in COMPAS were brought to light by high-profile investigations, such ProPublica's.

Ongoing initiatives concentrate on improving algorithmic transparency, guaranteeing explainability of results, and requiring independent audits in order to lessen such biases. The need for AI technologies to supplement human judgment and judicial discretion rather than replace it is becoming more widely acknowledged by court systems.

## 2.3. Ethical considerations and regulatory challenges

There are unavoidably serious ethical concerns about privacy, discrimination, accountability, and transparency when AI is used in criminal law. Despite their efficiency, critics contend that automated decision-making technologies run the risk of dehumanizing legal institutions and fostering ingrained biases. There are serious moral and legal conundrums raised by the possibility of algorithmic discrimination, excessive surveillance, and loss of personal autonomy.

Strong legal frameworks, transparency standards, and supervision procedures that guarantee AI tools are used responsibly are necessary to address these issues. Laws like the planned European Union AI Act, which would define AI systems used in criminal justice as high-risk applications and subject them to strict inspection and compliance standards, aim to set clear guidelines.

---

13 J. Dressel, H. Farid, "The accuracy, fairness, and limits of predicting recidivism", *Science Advances*, 4(1)/2018.

The application of AI to criminal law is both a significant breakthrough and a formidable obstacle. It holds promise for improving criminal justice systems' precision, effectiveness, and equity.<sup>14</sup> However, implementation must be cautious, transparent, and morally led due to the potential of algorithmic biases, privacy invasions, and ethical quandaries. Legal institutions must constantly adjust as AI technologies develop, striking a balance between creativity and core human rights concepts.<sup>15</sup> In order to ensure that AI's revolutionary potential helps society without compromising justice and equity, regulatory regimes that prioritize human oversight, transparency, fairness, and accountability will unavoidably be crucial to the future of AI in criminal law.<sup>16</sup>

### 3. LEGISLATION OF AI IN EUROPE – APPLICABILITY TO CRIMINAL LAW

Artificial Intelligence (AI) has quickly progressed from abstract ideas to real technologies incorporated into everyday social processes, profoundly influencing European legal systems. The revolutionary potential of AI, especially in criminal law, has led European lawmakers to look for strong regulatory frameworks to oversee its ethical and responsible application. With a focus on its significance and implications for criminal law, this chapter examines the development, present state, and practical applicability of AI laws in Europe.

In the past, European legal frameworks have taken a proactive approach to technological advancements, placing a strong emphasis on privacy, data protection, and human rights. The Council of Europe Convention for the Protection of Individuals concerning Automatic Processing of Personal Data (Convention 108) was adopted in 1981 as one of the first legislative responses, highlighting Europe's leadership in technological regulation. Since the early 2000s, artificial intelligence (AI) has become more and more prevalent in criminal justice and law enforcement systems, and European politicians realized that specific legislation governing AI technology were desperately needed. Important issues regarding justice, accountability, transparency, and fundamental rights were brought to light by the changing environment, especially with regard to algorithmic decision-making and fundamental rights.

A landmark regulatory step was the European Union's General Data Protection Regulation (GDPR), enacted in 2018. Although not AI-specific, GDPR critically shaped AI deployment by establishing fundamental rules for data processing, particularly impacting automated decision-making tools.

14 ProPublica, Machine Bias, 2016. Retrieved from <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>, 18. 04. 2025.

15 M. Hildebrandt, "Algorithmic regulation and the rule of law", *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 2018, 376.

16 A. Završnik, *Big Data, Crime and Social Control*, Routledge, New York, 2019, 102–104.

GDPR Article 22 explicitly addresses automated individual decision-making, stipulating individuals' rights not to be subjected to purely automated decisions producing significant effects.<sup>17</sup> This provision directly applies to algorithmic profiling and decision-making used in criminal investigations, judicial decisions, and risk assessments, demanding transparency and explainability of AI decisions. Law enforcement and judicial authorities employing AI must therefore justify algorithmic outcomes and provide mechanisms for human oversight and intervention, ensuring procedural fairness and safeguarding fundamental rights.

Building on GDPR, the European Commission unveiled “Ethical Guidelines for Trustworthy AI” in 2019, defining fundamental rules to regulate AI applications, such as nondiscrimination, accountability, and transparency.<sup>18</sup> By highlighting ethical considerations that are essential for criminal law applications, like automated judicial decision-making systems and predictive police algorithms, these guidelines—while not legally binding—had a substantial impact on later legislative initiatives.

The rules place a strong emphasis on openness and call for AI systems used in criminal justice to be auditable, explicable, and subject to human supervision. The ethical deployment and legislative design of AI in law enforcement, correctional facilities, and judicial procedures have been greatly influenced by these concepts.

### 3.1. Proposal for an EU Artificial Intelligence Act (2021)

The European Commission's Proposal for an Artificial Intelligence Act (AI Act), which was released in April 2021,<sup>19</sup> was a significant turning point in the continent's AI regulatory history. This thorough legislative proposal divides AI systems into four risk categories: minimal, high, limited, and unacceptable. Applications of AI in criminal justice, such as forensic analytical tools, biometric identification, judicial decision-making, and predictive policing, are specifically classified as high-risk. As a result, the proposed AI Act imposes strict compliance requirements on them. Important clauses include obligatory risk assessments, thorough documentation specifications, transparency guidelines, stringent data governance procedures, and commitments to ongoing monitoring and human supervision.

The Council of Europe has been actively involved in developing AI regulations that apply to criminal justice systems in parallel to the EU.<sup>20</sup> The Council

17 Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

18 European Commission. (2019). *Ethical Guidelines for Trustworthy AI*. High-Level Expert Group on Artificial Intelligence.

19 European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. COM/2021/206 final.

20 Council of Europe. (2021). *Guidelines on Artificial Intelligence and Data Protection*. Directorate-General for Human Rights and Rule of Law.



released proposals in 2021 that placed a strong emphasis on human rights compliance in the application of AI, especially with relation to the use of AI by criminal courts and law enforcement.<sup>21</sup> The Council's recommendations promote openness, justice, accountability, and ongoing human oversight while highlighting strict moral and legal requirements. It is recommended that member nations enact clear legislative protections against algorithmic prejudice, discrimination, and infringement of due process rights. For European states using or preparing to use AI in criminal justice contexts, these suggestions offer crucial direction.

### 3.2. Applicability to Criminal Law: Practical Implications

The practical use of AI in criminal law is significantly impacted by the changing legal environment in Europe. Increased regulatory scrutiny of law enforcement agencies using facial recognition or predictive analytics systems necessitates thorough risk assessments, openness policies, and well-defined oversight procedures. When judicial systems use algorithmic risk assessments, like COMPAS-style tools for sentencing or parole decisions, they must make sure that the requirements for fairness, explainability, and openness set forth by the GDPR and the planned AI Act are met. This involves enabling appeals or human reconsideration of automated choices, as well as giving impacted parties clear information about AI's involvement in decisions that impact their rights.

In order to lower the possibility of biased or discriminatory results, correctional facilities using AI-driven surveillance or rehabilitation programs must record, audit, and guarantee data integrity and impartiality. Legislative emphasis on human control also guarantees that AI complements human judgment rather than replaces it, which is important in situations where liberty is restricted.<sup>22</sup>

Practical difficulties still exist in spite of extensive legislative advancements. The interpretability of intricate machine learning models, biases present in datasets, and algorithmic transparency continue to be major concerns. Furthermore, because national legal traditions and practices vary, it is practically challenging to harmonize national legislation throughout European countries. Furthermore, ongoing legislative adaptation becomes crucial as technological advancements progress at a rapid pace. Iterative evaluations and flexible legislative frameworks that may proactively address future difficulties are necessary as regulatory frameworks must strike a balance between encouraging innovation and upholding strict human rights standards.

The European legal framework for AI creates a strong, morally sound, and human rights-based framework that is directly applicable to criminal law. Criminal

21 G. Sartor, F. Lagioia, "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence", *European Data Protection Law Review*, 6(1)/2020, 96–108.

22 C. Engel, L. Linhardt, M. Schubert, "Code is law: how COMPAS Affects the way the judiciary handles the risk of recidivism", *Artificial Intelligence and Law Collective Journal*, Springer International, 2024, 6–8.

justice procedures are greatly impacted by laws like the GDPR and the proposed AI Act, which enforce accountability, openness, and equity. Europe's changing legal environment guarantees that fundamental rights and procedural justice remain paramount as AI technologies continue to infiltrate criminal justice systems, thereby transforming AI's revolutionary potential into beneficial societal outcomes.

#### 4. AI AND CRIMINAL LAW – WHAT BRINGS THE FUTURE?

The use of artificial intelligence (AI) into criminal law is a revolutionary development that will have a significant impact on justice systems around the globe. AI's potential influence on criminal law presents both tremendous prospects and formidable difficulties as it continues to develop at a rapid pace. This chapter examines the expected developments, opportunities, hazards, moral dilemmas, and new arguments pertaining to artificial intelligence's potential application in criminal law.

The ongoing improvement of predictive capacities in criminal justice contexts is one of the most important future trends. Many jurisdictions have already adopted predictive policing methods, which are expected to advance in sophistication. A wider variety of data, such as socioeconomic indicators, environmental elements, real-time social media feeds, and sophisticated behavioral analytics, may be incorporated into prediction algorithms in the future.<sup>23</sup> These advancements have the potential to reduce criminal behavior through focused interventions and offer previously unheard-of accuracy in crime predicting. However, there are serious ethical and social justice issues with future prediction skills.<sup>24</sup> There is a significant chance of past prejudices or socioeconomic inequalities being maintained in the absence of strong control. In order to provide open, auditable, and equitable prediction algorithms, along with strict human monitoring, politicians and criminal justice institutions will therefore probably need to tread carefully.<sup>25</sup>

Significant developments in AI-powered surveillance technology, especially in the areas of biometrics and face recognition, are probably in store for the future. Beyond basic identification tasks, AI-driven surveillance may also include behavioral prediction, emotion recognition, and micro-expression analysis. These technologies have a lot of potential to improve criminal investigations, security monitoring, and public safety. However, they also provide significant privacy

23 European Union Agency for Fundamental Rights (FRA). (2020). *Getting the Future Right: Artificial Intelligence and Fundamental Rights*. Publications Office of the EU.

24 R. Richardson, J. Schultz, K. Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice", *New York University Law Review Online*, 94/2019, 192–233.

25 B. E. Harcourt, *Exposed: Desire and Disobedience in the Digital Age*, Harvard University Press, 2018, 364–367.

hazards and the possibility of misuse. Increased societal surveillance could result from improved surveillance capabilities, compromising individual liberties and privacy. Legal frameworks and regulatory agencies must proactively address possible abuses as AI-enabled surveillance develops, striking a balance between security requirements and fundamental human rights, accountability, and openness.<sup>26</sup>

#### **4.1. Autonomous Decision-Making and Judicial AI**

AI-powered legal instruments, such as self-governing systems for parole, bail, and sentence, are probably going to become more popular. More consistent, effective, and supposedly impartial court decisions are anticipated with increased algorithmic complexity and comprehensive data analytics. In order to provide judges and lawyers with extremely accurate suggestions, future judicial AI systems may use machine learning and natural language processing to evaluate enormous databases, court decisions, and legal texts.

However, it is still quite controversial to fully delegate judicial decision-making to AI systems. Accountability, transparency, and fairness concerns imply that a hybrid model will be prioritized in future systems. Instead of autonomous adjudication, these models use AI to support decisions, guaranteeing ongoing human scrutiny to uphold ethical standards and procedural justice.

In correctional systems, future AI applications will likely revolutionize inmate rehabilitation and institutional management. AI-powered predictive analytics could optimize inmate classification, predict violent incidents, manage facility logistics, and personalize rehabilitation programs. Tailored educational and vocational training delivered via AI-driven platforms could significantly reduce recidivism rates and facilitate successful reintegration into society.

However, the future application of AI in corrections raises ethical questions about data privacy, inmate autonomy, and potential manipulation through overly intrusive monitoring or predictive profiling. Balancing AI's rehabilitative potential with ethical safeguards will necessitate robust legislative frameworks and clear ethical guidelines governing AI's correctional deployment.

#### **4.2. Privacy, Data Protection, and Ethical Regulation**

Existing standards for data protection and privacy will unavoidably be put under pressure by AI's exponential expansion. Increased capacity for data processing, analysis, and monitoring increases the risk of illegal data use and invasive surveillance. Future legal frameworks must therefore aggressively improve privacy safeguards, specify precisely what applications of AI are acceptable, and set up strong accountability procedures. A viable regulatory paradigm is offered by the

---

26 *Ibidem*, 368.

European Union's proposed AI Act, which would impose strict compliance requirements and transparency standards on high-risk AI applications, particularly those used in criminal law contexts.<sup>27</sup> Future frameworks must, however, continue to be flexible in order to quickly address new dangers, developing technology, and societal expectations around ethical and privacy standards.

### 4.3. International Cooperation and Standardization

International collaboration and standards will become more and more important given AI's worldwide influence. Harmonized regulatory standards, shared criminal databases, and cross-border data exchanges will greatly increase the efficacy of international law enforcement. Diverse national legal traditions and ethical considerations will need to be reconciled by international frameworks, which will require intensive diplomatic efforts and the development of global stakeholder agreement.<sup>28</sup>

Future legal professionals will need to be more technologically proficient as AI changes criminal law. AI literacy, ethics instruction, and data analytics abilities must all be incorporated into legal school curricula as it develops. Algorithmic literacy will probably be emphasized in judicial training programs. This will allow judges and legal professionals to assess AI-generated outputs critically, guaranteeing fair, responsible, and well-informed decision-making.<sup>29</sup>

## 5. IN CONCLUSION

In the end, public trust and societal acceptability will be crucial to AI's future success in criminal law. Building societal consensus on the use of AI will need open communication, inclusive public discourse, and responsive legislation. Institutions of criminal justice must proactively address public concerns by openly recognizing and reducing dangers while showcasing AI's beneficial possibilities.

Future criminal law applications of AI hold revolutionary potential to improve public safety, speed, accuracy, and fairness. However, major cultural, legal, and ethical issues necessitate careful handling, proactive policymaking, and strict ethical supervision. It will take constant attention, flexibility, and a

27 L. Floridi, J. Cowls, "A unified framework of five principles for AI in society", *Harvard Data Science Review*, 1(1)/2019, 5–7.

28 K. Yeung, A. Howes, G. Pogrebna, "AI governance by human rights-centered design, deliberation, and oversight: An end to ethics washing", *The Oxford Handbook of Ethics of AI*, Oxford University Press, Oxford, 2020, 80–82.

29 F. Pasquale, *New Laws of Robotics: Defending Human Expertise in the Age of AI*, Belknap Press, 2020, 220–222.

strong dedication to openness, responsibility, and core human rights values to guarantee AI's future has a good impact on criminal justice.

## BIBLIOGRAPHY

- Brayne S., *Predict and Surveil: Data, Discretion, and the Future of Policing*, Oxford Oxford, University Press, 2021.
- Csikszentmihaly M., *Creativity: Flow and the psychology of discovery and invention*, Harper/Collins, New York, 1996.
- Dressel J., Farid H., "The accuracy, fairness, and limits of predicting recidivism", *Science Advances*, 4(1)/2018.
- Ferguson A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, NYU Press, 2017.
- Floridi L., Cows J., "A unified framework of five principles for AI in society", *Harvard Data Science Review*, 1(1)/2019.
- Harcourt B. E., *Exposed: Desire and Disobedience in the Digital Age*, Harvard University Press, 2015.
- Hildebrandt M., "Algorithmic regulation and the rule of law", *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2128)/2018.
- Lau T., "Predictive Policing Explained", article published and consulted online on the Brennan Center Platform.
- Lessig L., *Code and Other Laws of Cyberspace*, Basic Books, 1999.
- McCarthy J., Minsky M., Rochester N., Shannon C. E., *Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Dartmouth College, 1995.
- Pasquale F., *New Laws of Robotics: Defending Human Expertise in the Age of AI*, Belknap Press, 2020.
- Richardson, R., Schultz, J., Crawford K., "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice", *New York University Law Review Online*, 94/2019.
- Sartor G., Lagioia F., "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence", *European Data Protection Law Review*, 6(1)/2020.
- Turing A., *Computing Machinery and Intelligence*. *Mind*, 59(236)/1950.
- Yeung K., Howes A., Pogrebna G., "AI governance by human rights-centered design, deliberation, and oversight: An end to ethics washing", In *The Oxford Handbook of Ethics of AI*, Oxford University Press, Oxford, 2019;
- Završnik A., *Big Data, Crime and Social Control*, Routledge, 2019.

**Dr. Vlad Barbat\***

## **AI ȘI DREPTUL PENAL – PERSPECTIVE MODERNE – LEGISLAȚIE ȘI UNIFICARE ÎN EUROPA**

### *Rezumatul de la sfârșitul lucrării*

*Dreptul penal european se confruntă atât cu oportunități, cât și cu provocări extraordinare ca urmare a încorporării inteligenței artificiale (IA) în societatea contemporană. Sistemele judiciare europene sunt supuse unei presiuni din ce în ce mai mari de a se schimba, deoarece sistemele AI au un impact mai mare asupra domeniilor, inclusiv procesarea dovezilor digitale, luarea autonomă a deciziilor, controlul predictiv și supravegherea. Cu accent pe răspunsurile legislative și pe eforturile UE de armonizare, acest studiu examinează punctele de vedere actuale cu privire la relația dintre IA și dreptul penal. Acesta analizează cât de bine cadrele legale actuale tratează preocupările legate de confidențialitate, responsabilitate, culpabilitate și proces echitabil în scenarii criminale, inclusiv inteligența artificială. Articolul actual examinează, de asemenea, măsurile recente ale UE, cum ar fi Digital Services Act și Artificial Intelligence Act, și analizează modul în care acestea afectează sistemele de justiție penală. Acest studiu subliniază necesitatea unor reglementări logice, rezistente la viitor, care să atingă un echilibru între inovație, drepturi fundamentale și justiție, comparând legile naționale cu încercările europene de unificare juridică. Scopul lucrării este să adauge la discuția în curs despre modul în care Europa ar putea crea un cadru juridic unic care să reglementeze și să utilizeze AI în mod eficient și moral în dreptul penal.*

*Savanții și teoreticienii juridici au participat activ la discuția despre ramificațiile juridice ale AI, examinând aspecte fundamentale despre personalitatea, drepturile și responsabilitatea sistemelor AI. Contribuțiile teoretice timpurii făcute de academicieni precum Lawrence Lessig la sfârșitul anilor 1990 și începutul anilor 2000 au avut un impact mare asupra modului în care oamenii au înțeles legătura dintre drept și tehnologie. Lessig a sugerat că cadrele de reglementare trebuie să se schimbe pentru a reflecta caracteristicile inerente ale tehnologiei digitale, anticipând nevoia de cadre legale care să poată face față calităților și pericolelor speciale prezentate de mașinile sensibile.*

**Cuvinte cheie:** AI, fragmentare, unificare, standardizarea dreptului penal internațional, uniformizarea dreptului european, viitorul dreptului penal european.

\* Director-adjunct al Centrului de Studii Interdisciplinare, Universitatea „Bogdan Voda”, România, Doctor in Drept Comparat, e-mail: [vlad.barbat@ubv.ro](mailto:vlad.barbat@ubv.ro).