LEGAL AND ADMINISTRATIVE STUDIES, www.jlas.upit.ro.
e-ISSN: 2344-6900, ISSN-L: 1583-0772
No.1 (32), Year XXIV, 2025, pp. 83-92

ARTIFICIAL INTELLIGENCE AND CRIMINAL LAW: CHALLENGES, OPPORTUNITIES AND PERSPECTIVES

Andreea CORSEI
ORCID ID: 0000-0001-5688-3701
E-mail: office.corsei@yahoo.co.uk
Affiliation: "Petre Andrei" University in Iasi,
Vice-Dean of the "College of Legal Advisers Suceava" Association,
General secretary of the "Order of Legal Advisers from Romania" Federation

Abstract: *Artificial intelligence (AI) is increasingly penetrating the field of criminal law, offering solutions for streamlining investigations, judicial decision-making and crime prevention. However, the use of AI raises complex issues regarding criminal liability, respect for fundamental rights and transparency of automated decisions.*

The main risks include algorithmic discrimination, lack of human control and the legislative vacuum regarding the regulation of AI in justice. In order to avoid abuses and protect the rights of persons involved in criminal proceedings, clear regulation is needed, ensuring transparency, fairness and mandatory human intervention in critical decisions.

Thus, AI offers important opportunities for the modernization of the criminal justice system, but these must be managed within a well-defined legal and ethical framework.

Keywords: *artificial intelligence; criminal law; discrimination; control.*

Introduction

In the last decade, artificial intelligence (AI) has become a factor of profound transformation in many fields, including justice and, in particular, criminal law. The accelerated development of technologies based on machine learning algorithms, automatic natural language processing and facial recognition raises fundamental questions related to the application and interpretation of criminal norms, but also to the respect for the fundamental rights and freedoms of individuals. In this context, the use of AI within the criminal system is not only a matter of technological efficiency, but also a deeply legal, ethical and constitutional one.

Criminal law, as a branch of public law, regulates the most serious forms of antisocial behavior and involves sanctions with a major impact on individual freedom. Therefore, the principles governing criminal law — the legality of incrimination and sanction, culpability, presumption of innocence, individualization of punishment — are fundamental and relatively rigid, designed to guarantee the protection of the individual against state power. Any integration of AI technology in this area must be carefully assessed in light of these principles.

On the one hand, AI offers undeniable opportunities in supporting criminal investigations, in analyzing digital evidence or in managing the growing volume of information relevant to criminal cases. Through its ability to identify patterns, relationships and anomalies in large data sets, AI can help criminal prosecution bodies to detect fraud, organized crime networks or terrorist activities more quickly. Also, in courts, the use of AI for the automatic organization of files, drafting of decisions or even assisting in the assessment of the risk of recidivism seems to increase the efficiency and coherence of the act of justice.

On the other hand, these applications raise major legal issues. A first obstacle is the determination of criminal liability in the situation where a crime is committed with the help of or through an AI system. According to classical criminal law, a criminal act presupposes the existence of an active subject — a natural person or, in certain situations, a legal entity — who acts with guilt. In the case of autonomous systems, lacking consciousness, intention, or will, the question arises: who is responsible for the damages caused? Current jurisprudence and criminal law do not provide a clear answer to this dilemma.

A second problematic aspect concerns the respect for fundamental rights. Algorithms used in the assessment of defendants may perpetuate or amplify pre-existing prejudices in the data on which they were trained, generating discriminatory results based on race, gender, socio-economic status or other criteria. This runs counter to the principles of equality before the law and non-discrimination, enshrined in the Constitution, the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. Algorithmic opacity also affects the right to a fair trial, as the parties cannot challenge or understand the logic of automated decisions if it is inaccessible or impossible to explain.

Finally, from a legislative perspective, it is necessary to develop a specific regulatory framework to regulate the application of AI in criminal proceedings. Existing initiatives at the European Union level (such as the AI Act) and the recommendations of the Council of Europe underline the importance of a prudent and balanced approach, combining technological innovation with respect for the principles of the rule of law. It is essential that the national legislator adopts clear regulations on the limits of the use of AI in the criminal field, the criteria for validating algorithms and the related procedural guarantees.

The relationship between artificial intelligence and criminal law therefore represents a new and complex terrain, where the challenges of technology meet the demands of criminal justice. The objective of research in this area must be twofold: on the one hand, identifying ways in which AI can bring real benefits to the criminal justice system; on the other hand, building a robust legal framework that ensures that these innovations do not violate the fundamental rights of the individual and do not undermine trust in the act of justice.

1. The Use of Artificial Intelligence in the Criminal Field

Artificial intelligence (AI) is a set of technologies capable of performing human-like cognitive tasks, such as learning, reasoning, and decision-making. In the criminal field, AI is used in a variety of ways, from supporting investigations to assisting judicial decisions, generating both opportunities for improving the efficiency of the system and major legal challenges.

Practical uses of AI in criminal law

a) Data analysis and crime investigation

AI enables law enforcement agencies to process large amounts of data - for example, communication analysis, video surveillance with facial recognition or behavioral analysis on social networks - to identify suspects and prevent crimes (*European Parliamentary Research Service*, 2021, p. 12). This can lead to faster and more efficient detection of criminals, but raises issues related to the legality and proportionality of data collection methods.

b) AI-assisted judicial decisions

In some judicial systems, predictive algorithms assess the risk of recidivism of defendants to support decisions on pre-trial detention or conditional release (Angwin et al., 2016). Such tools can help judges make more informed decisions, but they can raise risks related to transparency, impartiality and control over automated decisions (Wachter, Mittelstadt & Floridi, 2017).

c) Crime prevention (predictive policing)

The police use algorithms that analyze historical data to predict areas with a high risk of crime (Wachter, Mittelstadt & Floridi, 2017). Although this method can make resource allocation more efficient, it can perpetuate stereotypes and lead to disproportionate surveillance of certain social groups, which violates the principles of non-discrimination and the right to privacy (Barocas & Selbst, 2016).

The major legal issues are:

a) Criminal liability in the context of AI

AI systems do not have legal consciousness or will, and traditional criminal law requires the existence of an active subject who intentionally or culpably commits a criminal act (Roxin, 2017, p. 230). Thus, difficulties arise in attributing criminal liability for actions determined or facilitated by AI - the central question being whether individuals who develop, implement or use these technologies should be sanctioned

(Pagallo, 2013, p. 89).

b) Respect for fundamental rights

The use of AI in criminal proceedings may endanger fundamental rights such as the presumption of innocence, the right to a fair trial and the protection of personal data (European Court of Human Rights, *S. and Marper v. the United Kingdom*, 2008). For example, algorithms can be “black boxes” whose decisions are not transparent, which makes it difficult to challenge automated decisions (Selbst & Barocas, 2018). Also, errors or coded biases can lead to systematic discrimination.

c) Proportionality and legality of the intervention

According to the principles of criminal law and data protection, any intervention restricting fundamental rights must be clearly provided for by law, necessary and proportionate to the aim pursued (Art. 52 of the Charter of Fundamental Rights of the European Union). Many AI technologies are still insufficiently regulated, which raises the risk of abuse or excessive use without a clear legal framework.

Therefore, in order to properly integrate AI into the criminal justice system, it is imperative to develop specific regulations that ensure:

- Transparency of algorithms and the possibility of auditing automated decisions (AI Act Proposal, European Commission, 2021).
- Guaranteeing human intervention in relevant decisions, in order to respect the procedural rights of defendants (Goodman & Flaxman, 2017).
- Protection mechanisms against algorithmic discrimination and systematic errors (Kroll et al., 2017).
- Training of legal specialists to understand and use AI technologies responsibly (Raso et al., 2020).

Initiatives such as the European Regulation on Artificial Intelligence (AI Act) reflect this regulatory trend and provide a general framework applicable also in criminal law, imposing standards of accountability and transparency.

2. Major Legal and Ethical Issues

2.1. Criminal liability in the context of the use of AI

One of the most complex legal aspects that has arisen in the context of the use of artificial intelligence in the criminal field is that of attributing criminal liability. Classical criminal law requires the existence of an active subject – a natural or legal person – who has committed the act with guilt (intention or fault), according to the principle of nullum crimen sine culpa (Romanian Penal Code, art. 16 para. (1); Roxin, 2017, p. 231).

If an autonomous AI system generates a result that leads to the commission of a crime (e.g. using an algorithm that systematically discriminates when recommending a criminal sanction or makes decisions with unforeseen negative effects), the question arises as to who is criminally liable for the damages caused. Since AI does not have self-awareness, intention or discernment, it cannot be considered a subject of criminal liability in the classical sense (Pagallo, 2013, p. 92).

Several theories have been formulated in the doctrine:

- The liability of the programmer or developer, if the algorithm is defective due to fault;
- Liability of the user (operator), if he used AI without the due diligence required by law;
- Institutional liability, similar to the criminal liability of a legal entity (Boroi, 2020, p. 445).

However, in the absence of clear regulation on autonomous AI, current criminal law has difficulties in framing such situations without the risk of abusive extension of liability or violation of the principle of legality of incrimination.

2.2. Non-discrimination and fairness of algorithmic decisions

Another major risk is related to algorithmic discrimination. AI learns from historical data sets, and this data may reflect pre-existing social or institutional biases. Thus, an algorithm used to assess the risk of recidivism may end up disadvantageing certain defendants based on their race, gender or socio-economic status (Barocas, & Selbst, 2016, pp. 671–

732).

A notorious case is that of the COMPAS system, used in the USA, which was accused of overestimating the risk of recidivism for black defendants and underestimating it for white ones (Angwin et al., 2016). Although the algorithm itself is not "racist", its results are influenced by historical data and training parameters.

This runs counter to the principles of:

- equality before the law (art. 16 of the Romanian Constitution);
- non-discrimination (art. 14 of the ECHR);
- the right to a fair trial (art. 6 ECHR), as the defendant cannot effectively challenge an automatic decision whose internal mechanisms are opaque (ECHR, case Hirsi Jamaa and others v. Italy, 2012 – principle of access to an effective remedy).

2.3. Lack of transparency and control

Many AI systems are "black boxes", meaning that their decision-making processes are not fully understood by either those who develop them or those who use them. This runs counter to the principle of transparency of the act of justice and the right to reasons for the decision.

According to Art. 6 of the ECHR, everyone has the right to know the reasons that underpinned a judicial decision. If this decision is influenced (or even taken) by an algorithm, but without the possibility of understanding or verifying its internal logic, the right to defence and to a fair trial are violate (Selbst, &Barocas, 2019).

Therefore, the need for explainable and auditable algorithms becomes crucial. The proposal for a European Regulation on Artificial Intelligence (AI Act) classifies AI applications in justice as high-risk applications, which implies strict obligations regarding transparency, human control and performance monitoring (European Commission, *Proposal for a Regulation on Artificial Intelligence (AI Act),* COM(2021) 206 final).

2.4. Proportionality and legality of technological intervention

AI intervention in criminal proceedings must respect the principle of proportionality (also provided for in Article 52 of the EU Charter of

Fundamental Rights): any restriction of a right must be provided for by law, pursue a legitimate aim and be necessary in a democratic society.

In many cases, AI technologies are introduced into criminal investigations or proceedings without a clear legal basis, in the absence of procedural safeguards, which risks leading to systematic violations of fundamental rights (European Union Agency for Fundamental Rights (FRA), "Getting the future right – Artificial intelligence and fundamental rights," 2020).

Conclusions

The intersection of artificial intelligence (AI) and criminal law is an emerging field with profound implications for the way in which criminal law norms are designed, applied and protected in a state governed by the rule of law. AI offers undeniable opportunities to streamline judicial activity - by accelerating evidentiary analyses, supporting investigations or even anticipating criminal behaviour - but these benefits cannot be dissociated from the associated legal and ethical risks and challenges.

First, from the perspective of the principle of legality of criminalisation and sanctioning, enshrined in art. 1 of the Criminal Code and art. 7 of the European Convention on Human Rights (ECHR), the use of AI raises difficulties related to the attribution of criminal liability. Autonomous systems, which can make decisions without direct human intervention, challenge the classic paradigm of the active subject of criminal law, which involves discernment and guilt. Thus, a doctrinal and legislative reassessment of the concepts of imputability and culpability in the context of the use of autonomous technologies is necessary.

Secondly, AI affects the fundamental rights of the person – such as the presumption of innocence (art. 6 §2 ECHR), the right to a fair trial and to defense (art. 6 §1 ECHR), as well as the principle of equality before the law (art. 16 of the Romanian Constitution). Automated, non-transparent decisions, based on incomplete or biased data sets, can lead to discrimination, miscarriages of justice or even the denial of effective access to justice. In a criminal system that operates with deprivation of liberty as the ultimate sanction, these risks must be treated with utmost caution.

At the same time, the lack of a clear legislative framework regarding the application of AI in criminal procedure entails the risk of violating the principle of proportionality provided for in art. 52 of the Charter of Fundamental Rights of the European Union. Any interference by technology with individual freedoms must be not only legal, but also necessary and appropriate to the intended purpose, which requires rigorous control of the applicability of AI in this sensitive area.

In this context, it is imperative to develop a coherent, specific legal framework that regulates the use of AI in criminal justice. This should include: standards of algorithmic transparency, auditability, human oversight and the guarantee of procedural rights. Also, actors in the judicial system must be properly trained to understand and apply these technologies responsibly.

In conclusion, although artificial intelligence brings multiple opportunities for improving the criminal system, its integration must be carried out in a way that respects the foundation of European legal values: legality, fairness, human dignity and the rule of law. Only in this way can technological efficiency be avoided from becoming a threat to criminal justice.

References

Angwin et al. (2016). *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*. ProPublica.

Barocas, Solon & Selbst, Andrew D. (2016). Big Data's Disparate Impact. *California Law Review,* vol. 104.

Boroi, Alexandru. (2020). *Criminal Law. General Part*. C.H. Beck.

Charter of Fundamental Rights of the European Union.

European Commission. (2021). *Proposal for a Regulation on Artificial Intelligence* (AI Act), COM 206 final.

European Court of Human Rights. (2008). *S. and Marper v. the United Kingdom*.

ECHR, Hirsi Jamaa and Others v. Italy, 2012 - the principle of access to an effective remedy.

European Parliamentary Research Service. (2021). *Artificial Intelligence and Law Enforcement*.

European Union Agency for Fundamental Rights (FRA). (2020). *Getting the future right - Artificial intelligence and fundamental rights*.

Goodman & Flaxman, “European Union Regulations on Algorithmic Decision-Making and a ‘Right to Explanation,’” *AI Magazine,* 2017.

Kroll et al., “Accountable Algorithms,” *University of Pennsylvania Law Review*, 2017.

Pagallo. (2013). *The Laws of Robots: Regulating Autonomous Artificial Agents*. Springer.

Perry et al. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Corporation.

Romanian Penal Code.

Raso et al.. (2020). AI Ethics, Governance, and Policy: Global Perspectives. *AI Ethics Journal*.

Roxin, Claus. (2017). *Drept penal. Partea generală* (*Criminal Law. General Part*). C.H. Beck.

Selbst, Andrew & Barocas, Solon. (2018). Intelligent Discrimination in Big Data. *California Law Review*.

Selbst, Andrew & Barocas, Solon. (2019). The Intuitive Appeal of Explainable Machines. *Fordham Law Review*, vol. 87.

Wachter, Mittelstadt & Floridi. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*.