LEGAL AND ADMINISTRATIVE STUDIES, www.jlas.upit.ro.
e-ISSN: 2344-6900, ISSN-L: 1583-0772
No.1 (32), Year XXIV, 2025, pp. 93-106

USING ARTIFICAL INTELLIGENCE IN FIGHTING CRIME AND RESPECTING HUMAN RIGHTS

Loredana TEREC-VLAD
ORCID ^{ID}: 0000-0002-6984-3482
E-mail: Loredanaterec@gmail.com
Affiliation: Assistant Professor at the "Ștefan cel Mare" University of Suceava,
Principal at the Secondary School No. 4 Suceava,
Associate Researcher - Romanian Academy - Family Sociology Laboratory

Abstract: *The use of artificial intelligence (AI) in the field of public safety represents a major evolution in the way authorities prevent and investigate crime. Through predictive analytics, facial recognition, big data processing and automation of judicial processes, AI can contribute to making police and judicial activities more efficient. This technology offers significant benefits, such as faster identification of criminals, anticipating crimes and reducing the burden on courts.*

According to the European Convention on Human Rights (ECHR) and the General Data Protection Regulation (GDPR), the use of AI must respect fundamental principles such as legality, proportionality and non-discrimination. In particular, Article 8 of the ECHR protects privacy, Article 14 prohibits discrimination and Article 6 guarantees the right to a fair trial.

In this context, the EU Regulation on Artificial Intelligence (AI Act), currently in the process of being adopted, proposes a classification of the risks associated with AI systems and sets strict requirements for applications used in the field of public safety.

In conclusion, the use of AI in the fight against crime must be carried out within a clear legal framework, ensuring the balance between public safety and the protection of fundamental human rights. Any application of AI in this area must be transparent, humanly controlled and subject to effective oversight and legal accountability mechanisms.

Keywords: *technology; artificial intelligence; regulation; law.*

Introduction

In the context of rapid technological transformations of the 21st century, artificial intelligence (AI) has become an increasingly used tool in various sectors of society, including in the field of public security and criminal justice. Law enforcement agencies and judicial institutions increasingly resort to automated systems to prevent, detect and investigate criminal acts. From predictive analysis of criminal behavior to facial recognition and real-time monitoring of public space, AI promises to increase efficiency, reduce human errors and optimize decision-making processes.

However, this technological evolution raises serious challenges from the perspective of fundamental human rights. The implementation of algorithms and automated systems in activities that involve the restriction of individual freedoms requires a rigorous assessment of the compliance of these practices with the norms of national, European and international law. Essential rights, such as the right to privacy (art. 8 ECHR), the right to a fair trial (art. 6 ECHR) and the principle of non-discrimination (art. 14 ECHR) can be seriously affected in the absence of solid procedural guarantees and clear legal regulation.

In this context, the analysis of the use of artificial intelligence in combating crime must take into account both the perspective of practical efficiency and the imperatives of the rule of law and the protection of human rights. A balanced approach is required, which capitalizes on the technological potential, without compromising the fundamental principles of justice and democracy. This is why it is rightly stated that human rights issues are of international concern and do not fall under the domestic jurisdiction of states, which legitimizes not only the right of intervention of international bodies, but also their obligation to intervene whenever violations of human rights, which characterize any human community, are at issue (Corsei & Ștefãnoaia, 2022, p. 73).

The present study aims to critically analyze the use of AI in the criminal field, assessing the risks, benefits and applicable legal framework, with a focus on the compatibility of these practices with international human rights standards.

1. Arguments for using artificial intelligence in fighting crime

In a context marked by the complexity of forms of crime, the digitalization of society and the pressure on law enforcement institutions, artificial intelligence (AI) is emerging as a modern and efficient tool in preventing and combating crime. The use of AI in this field responds to a systemic need to increase efficiency, reduce costs and anticipate risks, but also requires strict compliance with national and international legal standards regarding the fundamental rights and freedoms of the individual.

1.1. Operational efficiency and big data analysis

The first major argument in favor of using AI in combating crime is the technology's ability to quickly and accurately process massive volumes of data, known as big data analytics. Machine learning algorithms can identify patterns of criminal behavior, correlate information from disparate sources (e.g. surveillance cameras, social networks, judicial databases) and generate alerts in real time, facilitating early intervention by law enforcement agencies (O'Neil, 2016).

This capability fundamentally transforms traditional investigative methods, giving authorities proactive insight into criminal dynamics. According to the literature, AI helps reduce response times in investigations and increase the rate of suspect identification, compared to conventional methods (Ferguson, 2017).

1.2. Crime prevention through predictive policing

Another important argument is the use of AI in predictive policing systems, which use algorithmic models to estimate the likelihood of crimes occurring in a given geographical area or time frame. Programs such as PredPol, implemented in the US, analyze historical crime data and generate recommendations for the allocation of police patrols (Brayne, 2020).

These systems allow for more efficient management of human and material resources, reducing risks and improving public safety. From a legal perspective, the use of this type of AI is not necessarily contrary to fundamental rights, as long as it does not lead to unlawful profiling or discrimination and is subject to appropriate procedural safeguards (European Union Agency for Fundamental Rights, 2020).

1.3. Automation of judicial and administrative processes

AI can also be used to automate repetitive tasks within the judicial system: drafting documents, managing files or sorting cases. For example, in Estonia a “robot judge” system has been developed to resolve minor civil cases, while other European countries use AI to automatically generate standardized decisions (Susskind, 2019).

In a criminal context, AI can assist in assessing the risk of recidivism or social dangerousness, supporting courts in making decisions on conditional release or preventive detention. However, these applications must be used with caution, as they may affect the right to a fair trial, enshrined in Article 6 of the European Convention on Human Rights (ECHR), if the algorithms are not transparent and if human control mechanisms are missing (European Court of Human Rights Hirsi Jamaa and Others v. Italy, App no. 27765/09, 2012).

1.4. Combating cybercrime and terrorism

One area in which AI is almost indispensable is the fight against cybercrime and terrorism. AI algorithms can detect cyberattacks in real time, monitor darknets and identify radicalizing language online, thus helping to prevent attacks and subversive activities (Europol, Internet Organised Crime Threat Assessment, 2023).

According to the case law of the European Court of Human Rights, states have a positive obligation to protect the life and security of citizens (art. 2 and 3 ECHR), which justifies, under certain conditions, the use of advanced technological means to prevent major dangers (ECtHR, Osman v. the United Kingdom, App no. 23452/94, 1998).

The use of artificial intelligence in combating crime represents a significant technological advance, capable of radically transforming police and judicial activity. The efficiency, speed and analytical capacity offered by AI bring real benefits in the fight against crime, especially in the context of emerging threats such as cyber terrorism or cross-border crime. However, these benefits must be balanced with respect for the principles of the rule of law and fundamental human rights. It is essential that the implementation of AI in the criminal field be carried out within a clear legal framework, with transparency, human control and legal accountability, in accordance with European and international standards. Therefore, the rigor of respecting fundamental rights and freedoms goes beyond the framework of the Communities, becoming a strong point in the external relations existing at the Union level (Corsei, Zisu & Țoncu, 2023, p. 55).

2. Legal challenges and human rights risks

The use of artificial intelligence (AI) technologies in law enforcement has brought significant improvements in the prevention and investigation of crime. However, this technological development raises numerous legal challenges and risks to fundamental human rights, requiring rigorous regulation and critical analysis from a human rights perspective.

2.1. Violation of the right to privacy and protection of personal data

One of the most obvious risks derives from the widespread use of AI for mass surveillance and the collection of sensitive personal data, including biometrics (facial recognition, voiceprints). This raises major issues of compliance with Article 8 of the European Convention on Human Rights (ECHR), which guarantees the right to respect for private and family life (European Convention on Human Rights, Art. 8, Respect for private and family life).

The processing of biometric data is also strictly regulated in the European framework by the General Data Protection Regulation (Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data - GDPR), which imposes principles such as lawfulness, purpose limitation, data minimisation and data security. The uncontrolled use of

AI can lead to mass surveillance, affecting individuals' rights to anonymity and freedom of movement, and can create a chilling effect on free expression (Tufekci, 2015, pp. 203-218).

2.2. Algorithmic discrimination and social inequalities

A major risk associated with the use of AI in justice and policing is algorithmic discrimination, caused by biases in historical data or algorithms. Criminal risk prediction algorithms, such as COMPAS in the United States, have been accused of overestimating the risk of recidivism for minority groups, thereby amplifying social inequalities (Angwin, Larson, Mattu & Kirchner, 2016).

This phenomenon runs counter to the principle of equality before the law and the prohibition of discrimination enshrined in Article 14 of the ECHR (Prohibition of discrimination). The lack of transparency of algorithms and the possibility of challenging automated decisions amplifies the negative effects on the right to a fair trial and equal protection before the law.

2.3. Lack of transparency and accountability

AI-based automated decisions, especially in criminal matters, can affect fundamental rights, but algorithms often remain opaque ('black boxes') and affected individuals do not have access to clear explanations of the decision-making criteria (Pasquale, 2015). This runs counter to the right to a fair trial under Article 6 of the ECHR, which includes, among others, the right to a defence and to effective judicial review.

Furthermore, the lack of clear mechanisms for accountability and human scrutiny of AI decisions can lead to miscarriages of justice or abuse. The absence of uniform regulation and sound technical and ethical standards increases the risk of arbitrary use of technology (Mittelstadt et al., 2016).

2.4. Threat to freedom of expression and association

AI-based surveillance can be used to monitor social movements, protests and online discussions, threatening fundamental civic freedoms, including freedom of expression and freedom of association (Articles 10 and 11 of the ECHR). In the absence of clear limits, this surveillance can induce self-censorship and the repression of political opposition or social criticism (Gilliom & Monahan, 2013).

2.5. Respect for the principle of legality and proportionality

Any interference with fundamental rights must respect the principles of legality, proportionality and necessity, as laid down in both national legislation and the case law of the ECHR (S. and Marper v. United Kingdom, Appeal no. 30562/04 and 30566/04, 2008). The implementation of AI in the criminal field must be strictly regulated by law, pursue a legitimate aim and be proportionate to the danger sought to be avoided.

In the absence of clear regulations, the use of AI can generate arbitrary or disproportionate interference, in particular through the use of invasive surveillance technologies in public spaces or through automated decisions without adequate human control (Goodman & Flaxman, 2017, pp. 50-57).

In conclusion, the use of artificial intelligence in the fight against crime offers undeniable opportunities, but it also entails significant risks for fundamental human rights. The regulation of the use of AI must be carried out rigorously, to ensure respect for the principles of privacy protection, non-discrimination, transparency and the right to a fair trial. Without such guarantees, AI risks transforming law enforcement institutions into an opaque, unfair and potentially abusive system, endangering the rule of law and democracy.

3. The international and European legal framework on the use of artificial intelligence in combating crime

Artificial intelligence (AI) technologies are increasingly being used in the fields of public security, criminal justice and crime prevention. However, the use of these technologies raises numerous legal questions regarding their compatibility with fundamental human rights and democratic principles enshrined in international and European treaties. This analysis examines the main legal regulations and standards applicable at international and European level, providing a systemic perspective on the obligations of states.

3.1. The European Convention on Human Rights (ECHR) and the case law of the Strasbourg Court

The ECHR, concluded under the auspices of the Council of Europe, is the main regional instrument for the protection of fundamental rights. In the context of the use of AI, several articles of the Convention are relevant:

Art. 8 – Right to private and family life: Applicable in cases of surveillance, facial recognition, collection of biometric data or predictive profiling. The European Court of Human Rights (ECHR) established in the case of S. and Marper v. v. the United Kingdom (2008) that the long-term retention of biometric data of unconvicted persons constitutes a violation of Article 8 (S. and Marper v. UK, Appl. Nos. 30562/04 and 30566/04, 2008).

Art. 6 – Right to a fair trial: This right may be violated if judicial decisions are influenced by algorithmic assessments that are not transparent or cannot be effectively challenged by litigants.

Art. 14 – Prohibition of discrimination: If AI algorithms reproduce or amplify systemic biases (racial, ethnic, social), this may lead to violations of equal treatment.

The ECHR imposes negative obligations on states (not to interfere arbitrarily with rights) and positive obligations (to protect rights through appropriate legislation and administrative measures). Thus, any use of AI by state authorities must be provided for by law, necessary in a democratic society and proportionate to the aim pursued (Uzun v. Germany, Appl. No. 35623/05, 2010, on GPS surveillance).

3.2. Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union (CFREU), legally binding under the Treaty of Lisbon (Article 6 TEU), reiterates and develops the standards of the ECHR. Among the relevant articles:

Art. 8 – Protection of personal data: The Charter establishes an autonomous right to data protection, distinct from private life. Any automated processing of data by AI systems must respect the principles of lawfulness, transparency and individual control (EU Charter of Fundamental Rights, Art. 8, in force since 2009, legally binding).

Art. 21 – Non-discrimination: In accordance with EU secondary legislation (Directive 2000/43/EC on equal treatment), discrimination is prohibited, including on grounds of race, ethnic origin, gender or political orientation, which is relevant in the context of AI used in the assessment of suspects.

Art. 47 – Right to a fair trial and access to justice: Affirms the right to an effective remedy before a court, including against decisions taken automatically.

3.3. General Data Protection Regulation (GDPR)

The GDPR (Regulation (EU) 2016/679) provides a detailed framework for the protection of personal data, including in relation to AI systems. Article 22 of the GDPR provides for the right of any individual not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects the data subject (Automated individual decisions, including profiling).

The regulation also requires:

- Data Protection Impact Assessments (DPIAs) for high-risk technologies.
- Principles such as purpose limitation, data minimisation, transparency and controller accountability.
- The right of the data subject to explanations of the AI decision logic and to human intervention.

3.4. UN Human Rights Conventions and UNESCO/OECD Documents

At the international level, several treaties and recommendations cover issues related to AI and crime:

- International Covenant on Civil and Political Rights (ICCPR): Protects the right to privacy (art. 17), to a fair trial (art. 14) and prohibits discrimination (art. 26). The UN Human Rights Committee has emphasized that digital technologies should not be misused by authorities to track or control the population (General Comment No. 16 on Article 17, 1988).
- UNESCO – Recommendation on the Ethics of Artificial Intelligence (2021): Framework document that promotes the responsible, ethical and non-discriminatory use of AI. Recommends impact assessments, transparency, explainability and democratic oversight of AI.
- OECD – Principles on AI (2019): Also adopted by the Council of Europe and the EU, they encourage the development of AI that is human-centred, transparent and accountable (accepted by 42 states).

3.5. Council of Europe initiatives and proposal for EU-level AI regulation

The Council of Europe is currently working on a binding legal framework on AI, in the form of an international convention (AI Convention), which would establish common safeguards for the use of AI in relation to human rights, democracy and the rule of law.

In parallel, the European Commission proposed in 2021 a Regulation on Artificial Intelligence (AI Act) (European Commission, Proposal for a Regulation on a Harmonised Approach to AI, COM/2021/206 final), which is in the process of adoption, which introduces:

- Classification of AI systems according to risk: unacceptable risk, high risk, limited risk, minimal risk;
- Bans for systems with unacceptable risk (e.g. real-time facial recognition in public spaces);
- Strict transparency, auditing and conformity assessment requirements for high-risk systems (e.g. AI used in criminal justice).

This regulation will constitute the first comprehensive legal framework for AI in the world, providing a reference for the responsible regulation of advanced technologies in the public and private sectors.

The international and European legal framework provides a solid foundation for the responsible use of artificial intelligence in the fight against crime. The changes that occurred domestically mainly took into account the changes that appeared in EU law regarding the applicable domestic law, starting from the idea that the legal order applicable at the level of each EU member state is subsumed under the legal order at the European level (Corsei & Ștefănoaia, 2022, p. 98). Documents such as the ECHR, the GDPR, the EU Charter and the UN treaties impose clear obligations on states to respect fundamental rights, data protection and prevent discrimination. At the same time, recent initiatives by the EU and the Council of Europe demonstrate a growing commitment to the balanced regulation of AI, so that it is compatible with democratic values and the rule of law. In this regard, the use of AI must be transparent, legally justifiable, proportionate, auditable and subject to human control, in order to ensure a balance between security and freedom.

Conclusions

The use of artificial intelligence in the fight against crime is a complex challenge that requires a balance between technological efficiency and the protection of fundamental human rights. The international and European legal framework provides essential principles and norms to guide the implementation of these technologies, ensuring respect for the rights to privacy, non-discrimination, fair trial and the protection of personal data.

The European Convention on Human Rights, the Charter of Fundamental Rights of the European Union and the General Data Protection Regulation impose clear standards on the legality, transparency and proportionality of the use of AI-based systems. At the same time, the case law of the European Court of Human Rights emphasizes the need for strong guarantees against arbitrary surveillance and non-transparent automated decisions.

At the international level, UNESCO recommendations and OECD principles add ethical and responsible governance dimensions, guiding states towards a use of AI that serves the public interest without compromising fundamental freedoms.

Recent legislative initiatives by the European Union, in particular the proposed AI Act, reflect a progressive effort to harmonise and regulate AI, with an emphasis on risk assessment, the prohibition of dangerous uses and the introduction of control and accountability mechanisms. These steps are indispensable to prevent abuse, discrimination and human rights violations, while ensuring that technology effectively contributes to security and democratic justice.

The European and international legal framework thus constitutes both a protective instrument and an ethical compass for the development and application of artificial intelligence in the field of crime. Compliance with these rules is essential to maintain public trust, strengthen the rule of law and ensure a fair balance between innovation and fundamental rights.

References

Angwin J., Larson J., Mattu S. & Kirchner, L. (2016). *Machine Bias*. ProPublica.

Brayne, S., Predict and Surveil. (2020). *Data, Discretion, and the Future of Policing*. Oxford University Press.

Corsei, A, Zisu, M.A., & Țoncu, S. (2023). The European Union and fundamental human rights. *AGIR Bulletin* no. 4.

Corsei, A., & Ștefănoaia, M.A. (2022). Respect for the Right to a Fair Trial in the Light of the Case Law of the Court of Justice of the European Union. *Anuarul Universităţii "Petre Andrei" din Iaşi Fascicula: Drept, Ştiinţe Economice, Ştiinţe Politice*.

Corsei, A., & Ștefănoaia, M.A. (2022). Romania and Human Rights According to European Regulations. *Acta Universitatis Danubius* Vol. 18, No. 2.

ECtHR, Osman v. the United Kingdom. (1998). App no. 23452/94, on the state's positive obligation to protect life.

ECtHR, S. and Marper v. United Kingdom. (2008). Appeal no. 30562/04 and 30566/04.

ECtHR, Uzun v. Germany. (2010). Appl. No. 35623/05, on GPS surveillance.

EU Charter of Fundamental Rights, Art. 8, in force since 2009, legally binding.

European Commission, Proposal for a Regulation on a Harmonised Approach to AI (COM/2021/206 final).

European Convention on Human Rights, Art. 14, Prohibition of discrimination.

European Convention on Human Rights, Art. 8, Respect for private and family life.

European Court of Human Rights (ECtHR). (2012). Hirsi Jamaa and Others v. Italy, App no. 27765/09.

European Union Agency for Fundamental Rights (FRA), Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2020.

Europol, Internet Organised Crime Threat Assessment (IOCTA), 2023.

Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press.

Gilliom, J., & Monahan, T. (2013). *SuperVision: An Introduction to the Surveillance Society*. University of Chicago Press.

Goodman, B., & Flaxman, S. (2017). European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation'. *AI Magazine*, 38(3).

Mittelstadt, B. D., et al. (2016). The Ethics of Algorithms: Mapping the Debate. *Big Data & Society*, 3(2).

OECD, Principles on Artificial Intelligence. (2019). Accepted by 42 states.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group.

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR).

Susskind, R. (2019). *Online Courts and the Future of Justice*. Oxford University Press.

Tufekci, Z. (2015). Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency. *Colorado Technology Law Journal*, 13(203).

UN Human Rights Committee. (1988). General Comment No. 16 on Article 17.

UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence.