

ARTIFICIAL INTELLIGENCE IN FORENSIC INVESTIGATIONS. DOCTRINAL GAPS, FUNDAMENTAL RIGHTS AND THE RULE OF LAW

Anca Florina Moroșteș*

"Vasile Goldiș" Western University of Arad, Romania

E-mail: anca_moro@yahoo.com

(Received: October 2025; Accepted: November 2025; Published: November 2025)

Abstract: The article examines the growing tension between the use of Artificial Intelligence (AI) in criminal investigations and the protection of fundamental rights. While AI technologies such as facial recognition, predictive policing, and digital forensics promise greater efficiency in law enforcement, they simultaneously raise serious concerns related to privacy, equality, non-discrimination, and the right to a fair trial. The analysis demonstrates that the current legal and doctrinal framework remains insufficiently developed to address these challenges, creating the risk of fragmented practices and undermining legal certainty. Drawing on European and international standards, as well as recent doctrinal debates, the article highlights the main risks: algorithmic opacity, indirect discrimination, automation bias, and the lack of consolidated jurisprudence regarding AI-generated evidence. The article contributes to filling this gap by identifying doctrinal lacunae and proposing research and regulatory directions. These include the need for clear procedural standards, mandatory algorithmic audits, minimum safeguards for digital evidence, strict limitations on the use of predictive technologies, and investment in digital literacy for justice professionals. AI should not be rejected as a threat, but integrated responsibly into the legal system, ensuring both security and respect for the rule of law.

Keywords: Artificial Intelligence; Fundamental Rights; Digital Forensics; Privacy and Data Protection; Fair Trial; Rule of Law.

1. Introduction

In recent years, artificial intelligence (AI) has become one of the central topics of international legal debate, due to its impact on fundamental rights and the functioning of democratic institutions. The adoption of the Artificial Intelligence Act by the European Union in 2024 confirms both the urgency of regulating this field

* Corresponding author: Anca Florina Moroșteș. E-mail: anca_moro@yahoo.com

Moroștes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

and the difficulty of finding a balance between technological innovation and the protection of constitutional values.

In the field of criminal forensics, the use of AI promises a radical transformation: facial recognition algorithms, predictive analysis tools, and digital evidence processing technologies can significantly enhance the efficiency of investigations and crime prevention. However, these instruments also pose major risks to fundamental rights — from the right to privacy and equality before the law to the right to a fair trial. Algorithmic opacity (the so-called “black box”), the potential for discrimination, and the lack of uniform standards regarding the admissibility of evidence raise serious concerns for the rule of law.

Although the legal literature has extensively analyzed the impact of AI on fundamental rights and, to some extent, on justice in general, the field of criminal forensics remains largely neglected. There is a clear doctrinal gap regarding how new technological tools can be employed in criminal investigations without undermining fundamental safeguards. In the absence of coherent legal reflection, practice risks developing in a fragmented manner, with ad hoc and potentially abusive solutions.

The article argues that the use of AI in criminal investigations generates both significant opportunities for security and serious risks of violating fundamental rights, in the absence of clear and coherent normative frameworks. Its contribution lies in identifying existing doctrinal gaps and proposing research and regulatory directions capable of balancing technological innovation with the rule of law.

2. Fundamental Rights and Artificial Intelligence – Privacy, Equality, Fair Trial

2.1. Privacy and Data Protection

One of the fundamental rights most directly affected by the use of artificial intelligence is the right to privacy, enshrined in Article 8 of the European Convention on Human Rights [1] and in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union [2]. The expansion of AI-based technologies in the fields of public security and forensics involves the collection and processing of massive amounts of personal data, including highly sensitive biometric data such as facial images and fingerprints.

The central issue lies in the fact that facial recognition algorithms and similar technologies can be used not only for the specific identification of suspects but also for the generalized surveillance of the population. Such practices raise serious concerns regarding the principles of proportionality and necessity, as established in the case law of the European Court of Human Rights. [3], where the Court has condemned the unlimited retention of biometric data by public authorities.

Moros̃tes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

Moreover, recent jurisprudence confirms that states are under an obligation to provide adequate safeguards against abuses of digital surveillance [4].

A further risk derives from algorithmic opacity. When authorities use AI tools to generate matches or profiles, the individuals concerned may face decisions that significantly affect their rights, without having the possibility to understand the logic and criteria underlying the processing. This situation runs counter to the principle of transparency and to the right to an effective remedy, fundamental elements enshrined in the General Data Protection Regulation (GDPR, Article 22) and elaborated in legal scholarship [5].

Furthermore, the issue of data storage and reuse raises questions related to purpose limitation and retention periods. A database initially created for counter-terrorism purposes may later be reused for other objectives, thereby amplifying the risk of abuse and of disproportionate expansion of surveillance. In this regard, the European Data Protection Board (EDPB) has emphasized in several opinions the need for strict limitations on the use of AI in the field of public security [6].

Therefore, the use of AI in forensic activities requires additional legal safeguards: strict limitation of purposes, independent audit mechanisms for algorithms, an obligation to inform data subjects, and the possibility to challenge the outcomes generated by automated systems. Without these instruments, the right to privacy risks being excessively subordinated to security considerations.

2.2. Equality and Non-Discrimination

Another fundamental right affected by the use of artificial intelligence in forensic investigations is the right to equality and non-discrimination, enshrined in Article 14 of the European Convention on Human Rights, Article 21 of the Charter of Fundamental Rights of the European Union, and numerous international instruments, including Article 26 of the International Covenant on Civil and Political Rights.

Facial recognition algorithms and predictive models used in criminal investigations may reflect and even amplify biases present in the data on which they are trained. Numerous studies have shown that facial recognition systems exhibit significantly higher error rates for women and ethnic minorities [7]. In the forensic context, such errors may lead to wrongful identifications, abusive investigations, and even unjust convictions.

The risk of algorithmic profiling further exacerbates these issues. Predictive policing models may associate certain neighborhoods or social groups with a higher probability of criminality, generating a spiral of structural discrimination: the targeted areas become subject to disproportionate surveillance, leading to a greater number of reported crimes, which in turn reinforces the algorithm's initial biases.

From a legal perspective, these practices may infringe the principle of equality of arms and undermine the right to a fair trial. The European Court of Human Rights

Moros̃tes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

has consistently emphasized the importance of avoiding indirect discrimination, including in the field of law enforcement. In the case of AI-based decision-making, discrimination may become harder to identify due to the technical and opaque nature of algorithms.

To mitigate these risks, legal scholarship has proposed mechanisms of algorithmic accountability, independent audits, transparency regarding the datasets used, and an obligation for authorities to justify the deployment of AI tools in criminal cases [8]. At the European level, the AI Act introduces the classification of certain AI applications as "high-risk," which entails strict requirements concerning non-discrimination and data quality [9]. However, the practical applicability of these standards within the field of criminal forensics remains a major challenge.

2.3. The Right to a Fair Trial

Another essential fundamental right brought into question by the use of artificial intelligence in forensic investigations is the right to a fair trial, enshrined in Article 6 of the European Convention on Human Rights and Article 47 of the Charter of Fundamental Rights of the European Union. The central issue concerns how evidence generated or supported by AI algorithms can be used in criminal proceedings without compromising the principles of adversarial process, equality of arms, and access to an effective remedy.

The use of facial recognition algorithms or predictive systems in identifying suspects raises questions regarding the admissibility and reliability of such evidence. For instance, the European Court of Human Rights has consistently emphasized that evidence obtained through intrusive means must be subject to strict safeguards and must not compromise the overall fairness of the trial. In the case of AI, the main difficulty lies in the lack of transparency: the defense does not have access to the internal logic of algorithms, which limits its ability to challenge the validity of the evidence.

This situation contradicts the principle of equality of arms, which requires that each party be given a reasonable opportunity to present its case under conditions of parity. When the prosecution relies on results produced by AI systems without allowing the defense access to the algorithm's parameters or training data, there is a risk of a fundamental imbalance. Legal scholarship has already highlighted that "black box" algorithms can undermine the right to defense, as they introduce into the proceedings non-transparent and unverifiable elements [10].

Moreover, Article 22 of the GDPR generally prohibits decisions producing legal effects based solely on automated processing, which raises the question of whether courts may accept AI-based evidence as the sole or decisive basis for determining guilt. Even when AI is used merely as an auxiliary tool, there remains the danger

Moroștes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

that judges and prosecutors may exhibit an "automation bias," an excessive trust in algorithmic outputs [11].

To ensure respect for the right to a fair trial, additional legal safeguards are required: mandatory independent auditing of AI systems used in investigations, transparency regarding relevant algorithmic parameters, the defense's right to request independent technical expertise, and the exclusion of evidence obtained through systems that fail to meet standards of verifiability and contestability.

3. Digital Forensics and Artificial Intelligence

3.1. Facial Recognition and the Identification of Suspects

Automated facial recognition is among the most widely used applications of artificial intelligence in forensic investigations. This technology promises enhanced efficiency in identifying suspects by comparing video footage or photographs from databases with pre-existing biometric profiles. While its practical utility is undeniable, facial recognition raises serious concerns regarding reliability and proportionality.

Recent studies have demonstrated that commercial facial recognition systems display disproportionately high error rates for women and ethnic minorities [12]. In the context of criminal investigations, such errors may lead to false identifications, unjustified inquiries, and even wrongful convictions. Moreover, the use of facial recognition in public spaces often amounts to a form of mass surveillance, contrary to the case law of the European Court of Human Rights concerning the proportionality of interferences with the right to privacy.

At the European level, the Artificial Intelligence Act (2024) classifies facial recognition in public spaces as a "high-risk" technology and imposes strict restrictions, including limiting its use to exceptional cases such as the fight against terrorism. However, the effective application of these standards depends on their transposition into national legislation and on the existence of robust judicial oversight mechanisms.

Thus, while facial recognition can serve as a valuable tool for forensic purposes, its use must be conditioned upon clear legal safeguards, such as restriction to exceptional circumstances, prior judicial authorization, independent audits of algorithmic accuracy, and the defense's right to challenge the reliability of such evidence.

3.2. Predictive Analysis and Anticipated Criminality

An emerging domain of artificial intelligence use in forensic investigations is predictive analysis, also known as predictive policing. This approach involves the use of algorithms to identify areas, time frames, or individuals with a high probability of involvement in criminal activities. Although proponents argue that such tools can

Moroștes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

increase the efficiency of police resource allocation and prevent crimes before they occur, their effects on fundamental rights remain deeply controversial.

In practice, predictive algorithms risk creating a spiral of structural discrimination. Historical crime data often reflect institutional or social biases, and their integration into predictive models leads to the reinforcement of these biases. Studies conducted in the United States have shown that programs such as PredPol resulted in disproportionate surveillance of neighborhoods inhabited by minorities, without any significant reduction in crime rates. This situation contravenes the principle of proportionality and may give rise to indirect discrimination prohibited under Article 14 of the ECHR and Article 21 of the Charter of Fundamental Rights of the European Union.

Another major risk concerns the excessive automation of policing decisions. When police officers rely mechanically on algorithmic recommendations, there is a danger of diminishing human judgment and transforming law enforcement into a mere executor of "black box" decisions. From a legal perspective, this affects not only the fundamental rights of the individuals concerned but also public trust in the impartiality of law enforcement institutions.

At the European level, debates on predictive policing remain limited; however, the Artificial Intelligence Act (2024) explicitly classifies profiling models aimed at criminal prevention as "high-risk" applications, subject to strict requirements of transparency, accuracy, and algorithmic auditing. Nevertheless, the lack of clear mechanisms for verifying compliance with these standards raises questions regarding their actual effectiveness.

A concrete example is the PredPol system, initially used in U.S. cities such as Los Angeles and Chicago. This algorithm purported to identify "crime hotspots" based on historical data. In practice, however, journalistic and academic investigations revealed that the system led to disproportionate surveillance of minority neighborhoods without any real reduction in reported crime. This situation illustrates the risk of structural discrimination, as the algorithm merely reproduced and amplified pre-existing biases embedded in police data. From a legal standpoint, such mechanisms would contravene the principles of proportionality and the prohibition of indirect discrimination, as enshrined in Article 14 of the ECHR and Article 21 of the Charter of Fundamental Rights of the EU.

Thus, predictive analysis may serve as a useful instrument for security resource planning, but its use must be accompanied by strict legal safeguards: independent

Moros̃tes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

audits, a prohibition on the exclusive use of AI in decisions affecting individual liberty, and effective mechanisms for challenging algorithmic determinations.

3.3. Digital Evidence and Its Admissibility in Court

Another sensitive aspect of the use of artificial intelligence in forensic investigations concerns the admissibility and validity of digital evidence generated or supported by algorithms. In an era when electronic data already constitutes a significant part of the evidentiary material in criminal proceedings, the role of AI is becoming increasingly prominent — from metadata analysis and communication pattern detection to the identification of suspicious transactions within blockchain networks. The main issue lies in the reliability and verifiability of digital evidence. According to the case law of the European Court of Human Rights, the fairness of a trial must be assessed as a whole, and evidence obtained through intrusive or questionable means must not compromise the overall fairness of the proceedings. In the case of AI-generated evidence, the major difficulties stem from the lack of algorithmic transparency and the limited ability of the defense to request independent expertise on the technical mechanisms that produced the evidence.

Recent legal scholarship emphasizes that AI-based digital evidence risks creating an asymmetry of power between prosecution and defense: the accused party lacks access to the training data or the internal logic of the system, which contravenes the principle of adversarial proceedings [13]. Furthermore, courts have begun to debate whether there is a distinction between digital evidence explicitly recognized as AI-generated and that which is not labeled as such. A 2025 study shows that judges fluctuate between accepting such evidence as auxiliary technical proof and rejecting it in the absence of methodological transparency.

Another contemporary issue concerns the standards of integrity applicable to digital evidence. In 2025, UNESCO and the International Association of Prosecutors issued a dedicated guideline emphasizing that the chain of custody for digital evidence must include verification of any AI technologies used in the collection and analysis process. This recommendation reflects a growing tendency to tighten requirements on traceability and technical auditing of evidence, in order to prevent manipulation and algorithmic errors [14].

Therefore, to ensure respect for the right to a fair trial, national legislation and judicial practice should impose minimum standards of transparency and verifiability for AI-generated evidence. In the absence of such standards, there is a risk of divergent practices among jurisdictions and of judicial decisions based on evidence that cannot be effectively challenged.

In Romania, litigation concerning the use of body cameras (body-cams) by public authorities has raised similar concerns. In 2023, the National Authority for the Supervision of Personal Data Processing (ANSPDCP) prohibited the processing and ordered the deletion of data collected by the National Authority for Consumer

Moros̃tes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

Protection (ANPC) through body-cams, finding that there was no legal basis for processing facial images and voice recordings. Subsequently, the Bucharest Court of Appeal and the Constanța Court of Appeal confirmed similar solutions in cases involving local police authorities, emphasizing that the lack of a clear legal framework affects the admissibility and probative value of digital evidence. This jurisprudence demonstrates how, in the absence of explicit legal safeguards, digital evidence can become contestable before courts.

Recent jurisprudence also confirms the practical difficulties faced by courts. In the United States, judges have had to decide on the admissibility of AI-generated evidence, particularly in cases involving digital analysis and facial recognition. A 2025 report indicates that courts tend to accept evidence explicitly acknowledged as AI-generated (such as automated image analysis), but impose stricter standards for evidence not formally recognized as such, precisely due to the lack of methodological transparency [15]. This trend illustrates that, in the absence of general principles, judicial practice risks becoming fragmented and unpredictable, thereby undermining legal certainty.

4. Risks and Doctrinal Gaps

4.1. Lack of a Coherent Normative Framework

Although the European Union adopted the Artificial Intelligence Act in 2024, the regulation focuses primarily on classifying AI applications according to their level of risk and on general technical requirements. In the criminal and forensic domain, its provisions remain vague and fragmented, without establishing clear procedural standards concerning the admissibility of evidence, the rights of the defense, or mechanisms for contestation. Legal scholarship highlights that, at this stage, the underdeveloped regulatory framework may foster divergent practices among Member States, thereby undermining legal certainty and the principle of foreseeability [16].

4.2. Algorithmic Opacity (the “Black Box Problem”)

One of the most significant doctrinal risks lies in the impossibility of verifying how an algorithm has generated a specific conclusion. Unlike traditional forensic methods, which can be subject to expert examination and replication, AI systems—particularly those based on machine learning—operate through statistical correlations that are difficult to explain. This may create a structural asymmetry between prosecution and defense, calling into question the principles of adversarial proceedings and equality of arms.

4.3. Indirect Discrimination and Lack of Effective Oversight

Although recent literature has documented numerous cases of algorithmic bias, the current doctrinal framework still fails to provide clear solutions for identifying and

Moros̃tes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

sanctioning indirect discrimination produced by AI systems. The problem is further exacerbated by the absence of mandatory audit mechanisms and by the voluntary nature of many best-practice guidelines issued by international bodies. In the absence of effective oversight, AI risks reproducing and amplifying pre-existing social inequalities.

4.4. The Danger of the "Automation of Justice"

Another risk identified by legal scholarship is the tendency to grant algorithms excessive authority, a phenomenon known as automation bias. Criminal justice practitioners — police officers, prosecutors, and even judges- may display disproportionate trust in AI-generated outcomes, perceiving them as more objective than human decisions. In reality, these results are deeply dependent on the quality of the data and the parameters of system design. This tendency threatens to erode the role of human judgment and to transform AI from an auxiliary tool into a quasi-determinative decision-making factor.

4.5. Lack of Consolidated Jurisprudence

Although there are already relevant judgments of the European Court of Human Rights concerning digital surveillance and the right to privacy (*S. and Marper v. the United Kingdom*, *Big Brother Watch v. the United Kingdom*), there is not yet a consolidated body of case law regarding AI-generated evidence or predictive policing. National courts oscillate between accepting and rejecting such evidence, creating an area of doctrinal and practical uncertainty. Recent legal scholarship has observed that courts tend to approach these cases in a fragmented manner, avoiding the formulation of general principles applicable to AI-based evidence.

5. Conclusions

The present analysis has highlighted the structural tension between the forensic efficiency brought by artificial intelligence and the necessity of protecting fundamental rights. On the one hand, AI provides significant opportunities for the investigation and prevention of crime through facial recognition, predictive analysis, and the processing of digital evidence. On the other hand, these instruments raise major concerns related to privacy, non-discrimination, and the right to a fair trial.

The main contribution of this article lies in identifying the doctrinal gap concerning the use of AI in forensic investigations and in proposing directions for regulation and research aimed at ensuring a balance between security and liberty. Among these are: strengthening the European regulatory framework through clear procedural standards, introducing mandatory algorithmic auditing, developing standards for digital evidence, restricting the use of facial recognition and predictive analysis to strictly regulated situations, and investing in the training of justice professionals.

Rather than being viewed as a threat, AI should be understood as a legal and ethical challenge. The solution is not to reject innovation, but to integrate it within a

Moroștes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

normative and institutional framework capable of safeguarding the fundamental values of the rule of law. In this respect, dialogue between legal scholarship, legislators, and practitioners becomes essential.

Thus, the balance between security and fundamental rights is not a utopian goal but a realistic course of action, provided that AI regulation remains proportional, transparent, and oriented toward the protection of human dignity.

Acknowledgments

The author thanks the anonymous reviewers and editor for their valuable contributions.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not – for – profit sectors.

Author Contributions

The entire article was written by Anca Florina Moroșteș.

Disclosure Statement

The author does not have any competing financial, professional, or personal interests from other parties.

References

1. Abdulai, A.G., Sackeyfio, N. (2022). Introduction: The uncertainties of Ghana's 2020 elections. *African Affairs*, 121(484), e25–e53.
2. Artificial Intelligence Act (UE), (2024). Dispozițiile privind sistemele „high-risk”.
3. Barocas, S., Selbst, A.D. (2016). Big Data's Disparate Impact. *California Law Review*, 104(3), 671–732.
4. Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, 81, 1–15.
5. Carta Drepturilor Fundamentale a Uniunii Europene, art. 7–8.
6. CEDO, Big Brother Watch and Others v. United Kingdom, hotărârea din 25 mai 2021.
7. CEDO, Gillan and Quinton v. United Kingdom, hotărârea din 12 ianuarie 2010.
8. CEDO, Khan v. United Kingdom, hotărârea din 12 mai 2000.
9. CEDO, S. and Marper v. United Kingdom, hotărârea din 4 decembrie 2008.
10. Cary Coglianese, D., Lehr, D. (2017). Regulating by Robot: Administrative Decision Making in the Machine-Learning Era. *Georgetown Law Journal*, 105, 1147–1223.
11. Convenția Europeană a Drepturilor Omului, art. 8.

Moroștes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

12. European Data Protection Board (EDPB) (2021). Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR, adopted la 18 noiembrie 2021.
13. Ferguson, A.G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press.
14. G.F. Lendvai, G., Gosztonyi, G. (2025). Algorithmic Bias as a Core Legal Dilemma in the Age of Artificial Intelligence: Conceptual Basis and the Current State of Regulation. *Laws*, 14(3), 1–20.
15. Hildebrandt, M. (2015). *Smart Technologies and the End(s) of Law*. Edward Elgar.
16. Hildebrandt, M. (2016). Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics. *University of Toronto Law Journal*, 68(1), 12–34.
17. Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence (2025). *Artificial Intelligence Trends Report*, eDiscovery Today, 27 mai 2025.
18. Joshua A. Kroll, J.A., Huey, J., Barocas, S., Felten, E.W., Reidenberg, J.R., Robinson, D.G., Yu, H. (2017). *Accountable Algorithms*. *University of Pennsylvania Law Review*, 165(3), 633–705.
19. UNESCO & International Association of Prosecutors (2025). *Guidelines for Prosecutors on Digital Evidence*. Paris.
20. Wachter, S., Mittelstadt, B., Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99.
21. Wang, X. (2024). Algorithmic Discrimination: Examining Its Types and Regulatory Responses. *Frontiers in Artificial Intelligence*, 7, 1–12.

Notes:

- [1] European Convention on Human Rights, art. 8.
- [2] Charter of Fundamental Rights of the European Union, art. 7–8.
- [3] CEDO, S. and Marper v. United Kingdom, hotărârea din 4 decembrie 2008.
- [4] CEDO, Big Brother Watch and Others v. United Kingdom, hotărârea din 25 mai 2021
- [5] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, Edward Elgar, 2015; Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, *International Data Privacy Law*, vol. 7, nr. 2, 2017.
- [6] European Data Protection Board (EDPB), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers under Chapter V of the GDPR*, adopted on 18 November 2021.
- [7] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, *Proceedings of Machine Learning Research*, vol. 81, 2018.
- [8] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, *California Law Review*, vol. 104, nr. 3, 2016.
- [9] *Artificial Intelligence Act (EU), 2024*, the provisions concerning "high-risk" systems.
- [10] Mireille Hildebrandt, *Law as Computation in the Era of Artificial Legal Intelligence. Speaking Law to the Power of Statistics*, *University of Toronto Law Journal*, vol. 68, nr. 1,

Moroștes, A.F., (2025)

Artificial Intelligence in Forensic Investigations. Doctrinal Gaps, Fundamental Rights and the Rule of Law

2016; Joshua A. Kroll et al., *Accountable Algorithms*, University of Pennsylvania Law Review, vol. 165, nr. 3, 2017.

[11] Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, Georgetown Law Journal, vol. 105, 2017.

[12] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research, vol. 81, 2018.

[13] Xintong Wang, *Algorithmic Discrimination: Examining Its Types and Regulatory Responses*, Frontiers in Artificial Intelligence, 2024.

[14] UNESCO & International Association of Prosecutors, *Guidelines for Prosecutors on Digital Evidence*, Paris, 2025.

[15] *Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence*, Artificial Intelligence Trends Report, eDiscovery Today, 27 mai 2025.

[16] G.F. Lendvai & G. Gosztonyi, *Algorithmic Bias as a Core Legal Dilemma in the Age of Artificial Intelligence: Conceptual Basis and the Current State of Regulation*, Laws, vol. 14, nr. 3, 2025.