

AI in Big Data in Criminal Investigation: Procedural Safeguards and Human Rights Risks*

Matanat Pasha Asgarova¹

¹ National Aviation Academy of the Republic of Azerbaijan



[10.15408/jch.v13i3.46856](https://doi.org/10.15408/jch.v13i3.46856)

Abstract

The purpose of the study is to develop recommendations for improving procedural safeguards when using AI and big data in criminal investigations in Azerbaijan, considering the existing safeguards and risks that exist in the Azerbaijani legal system. This normative-legal study examines national and international laws about artificial intelligence in criminal justice using comparative and black-letter legal techniques. Due to the dearth of local research, it synthesizes scholarly material and adapts international approaches to the Azerbaijani setting. In results It has been demonstrated that the application of AI influences the development of human rights hazards, including the denial of access to algorithms, the possibility of discrimination, and the restriction of appeal procedures. The establishment of unique control and supervision mechanisms for the use of AI, as well as compatibility with international norms, is necessary due to the notable gaps in Azerbaijani legislation. Therefore, to enhance procedural guarantees in Azerbaijan, it is suggested that: establish and approve ethical standards for the use of AI in criminal proceedings; codify the rights of parties to transparency in algorithmic decisions and access to information about how AI works; and introduce legislative norms governing appeal procedures for AI-based decisions. In conclusion, it is shown that a significant prospective direction is the study of the interaction between technological innovations and legal institutions to shape modern regulatory frameworks.

Keywords: Artificial intelligence; Criminal proceedings; Big Data; Appeal Mechanisms; Azerbaijan

* Received: June 25, 2025, revised: July 24, 2025, accepted: July 29, 2025, published: December 30, 2025.

¹ Doctor of Law, National Aviation Academy of the Republic of Azerbaijan, Baku, Republic of Azerbaijan, Email: asgarovamatanatpasha@gmail.com ORCID: <https://orcid.org/0000-0003-1419-9519>

A. INTRODUCTION

Over the past decade, artificial intelligence (AI) and big data analytics technologies have been actively used in criminal investigations. Facial recognition systems, predictive analytics, social network analysis algorithms, and automated evidence sorting are used by law enforcement agencies in current countries around the world. For example, in the US, the police use predictive policing technologies. This allows them to predict crime. At the same time, China uses extensive AI-supported video surveillance systems that allow real-time identification of individuals. Such technologies have already had a vital impact on the tactics and success of criminal investigations (Ziobroń, 2021).

In the regional space of Azerbaijan, the issue of introducing digital technologies into law enforcement is also gaining importance (Yusifov, 2021). Although publicly available information indicates that certain steps have been taken towards the digitization of processes in the Ministry of Internal Affairs and the Prosecutor's Office, the large-scale implementation of AI systems, in particular facial recognition or algorithmic behaviour analysis, currently lacks a clearly regulated legal framework.

Therefore, the significance of the issue is determined not only by the potential advantages of using AI, but also by the identification of serious risks that they may cause. Scientific articles highlight violations of the right to privacy, discrimination based on race or social status, false accusations due to imperfect algorithms, and the lack of proper control over their use (Quezada-Tavárez et al., 2021). In Azerbaijan, as in many countries, the existing legal system does not yet provide sufficient procedural guarantees for the use of such technologies in criminal proceedings. Thus, the main problem of the study is the lack of adequate regulatory control over the use of AI and big data analytics in criminal investigations, which creates a potential threat of human rights violations through non-compliance with standards of procedural justice.

The purpose of the study is to develop recommendations for improving procedural safeguards when using AI and big data in criminal investigations in Azerbaijan, considering the existing safeguards and risks that exist in the Azerbaijani legal system.

Research questions: 1. What procedural safeguards are applied when using AI and big data in criminal investigations in different jurisdictions? 2. What risks to human rights arise from the use of AI in criminal investigations and what gaps exist in Azerbaijan's legal system? 3. What recommendations can

be developed based on the identification of key risks and gaps in current legislation? Thus, this work will have a direct impact on the process of forming a legal approach that will ensure a stability between technological efficiency and respect for fundamental rights in the system of criminal proceedings.

Literature Review

The development of artificial intelligence (AI) and big data analytics technologies is changing the criminal justice paradigm around the world. Various tools are actively used by law enforcement agencies: crime prediction tools, automatic facial recognition, social behavior recognition. This review aims to systematize the results of leading scientific research reports from international organizations.

1. The use of AI and big data in criminal investigations

The active use of AI in criminal investigations has been documented in global scientific literature. In the US, algorithmic systems, particularly PredPol, are used based on machine learning to predict areas and time windows of likely crime. Other works also highlight the use of other systems, such as COMPAS, to effectively assess the likelihood of recidivism (McKay, 2019). Other works indicate that these systems influence decisions on preventive measures (Greenstein, 2021). Similar tools are also used in the United Kingdom, France, and Australia.

Looking at scientific sources, the use of biometric data plays a special role. In particular, the article states that China has one of the world's largest facial recognition systems, integrated with a surveillance network and a social rating system (Asgarov & Mustafayev, 2024). This may give rise to certain ethical and legal dilemmas. In Europe, on the other hand, a more cautious approach is observed — technologies are used in narrow areas, such as tracking organized crime, but with clear restrictions imposed by GDPR and decisions of the European Court of Human Rights (Mitrou, 2018).

The dearth of rigorous empirical research on the efficacy of these tools is another issue raised by recent scientific papers. The works specifically highlight the primary dangers of automated systems, which can strengthen preexisting prejudices if algorithms are trained on data that has been skewed in the past. Additionally, there is a methodological flaw in the research on how these technologies affect various demographic groups.

2. Procedural guarantees: transparency, accountability, appeal

The use of AI in criminal proceedings requires a rethinking of classic procedural guarantees. The scientific community is debating how to effectively ensure the right to a fair trial in the context of algorithmic justice (Neiva, 2023). One of the key challenges is ensuring transparency of decisions that can be made using an AI system.

At the same time, as noted, the issue of responsibility for decisions made with the participation of AI remains unclear (Blount, 2022). As noted in other articles, the complexity of the algorithmic decision-making chain (from data collection to automated conclusion) leads to a blurring of responsibility between developers, software providers, and judicial authorities (Caianiello, 2021). This complicates the protection of the rights of the accused, especially in cases of misinterpretation of data.

In the context of the GDPR, there is also significant discussion regarding whether algorithmic choices adhere to fundamental legal concepts like the right to defend oneself and the presumption of innocence. The right of persons to not be subject to decisions based exclusively on automated data processing is guaranteed under Article 22 of the General Data Protection Regulation (GDPR) (Buchholtz, 2019). The article highlights the current exceptions to this rule's application and the reality that these guarantees are frequently implemented formally in practice, with little to no influence on the algorithmic decision's content.

Special attention in literature is paid to the problem of appealing decisions that are partially or entirely based on AI. According to scientists, algorithmic participation in the investigation or decision-making process can directly complicate or even prevent effective appeals (Kilian, 2022). This can happen if the defense does not have access to the internal logic of the system's functioning. This creates a risk of violating the principle of equality of the parties.

3. Risks to human rights

Scientific articles also indicate that AI in criminal proceedings affects the formation of risks to human rights, primarily to confidentiality, freedom of travel, and not being discriminated against (Truby, 2020). According to a Human Rights Watch report, the use of algorithms in criminal proceedings is often accompanied by a lack of control. This can lead to false accusations,

especially in the case of marginalized groups. In addition, recent reports by Amnesty International also express concern about the use of biometric systems in countries with unstable democratic institutions (Raso et al., 2018). These reports emphasize that AI can serve as a device for mass surveillance or even political persecution.

Researchers also pointed to the limited number of legal remedies available in cases of rights violations due to AI actions (Ramos, 2024). In this sense, it is important that most scientific works focus on countries with a high level of digitalization. Therefore, countries such as the Caucasus or Central Asia are outside the analytical focus. This contributes to the formation of blind spots in contemporary international scientific discourse.

Therefore, as can be seen from the review, there is a significant gap in thorough research that would adapt international experience to the realities of the Azerbaijani legal system. In addition, in terms of methodology, there are many studies that examine specific cases of AI use in criminal investigations in the US and the EU, but there are significantly fewer articles devoted to the experience of countries with transitional legal systems. At the same time, the mechanisms for adapting procedural guarantees to the conditions of modern automated justice remain insufficiently studied. As can be seen from this review, there is limited research on Azerbaijan. Further research is not only of academic but also of practical importance, as it is aimed at the legal modernization of criminal procedure in Azerbaijan.

B. METHODS

This research is normative-legal and has an analytical-recommendatory character. The focus of this doctrinal article is to develop well-founded recommendations for regulating the use of artificial intelligence (AI) in law enforcement activities in Azerbaijan. The research is based on the analysis of current legal norms, international standards, and scientific literature. Special attention is paid to ensuring procedural guarantees (in particular, transparency, appeal, compliance, and accountability) in the digitized criminal process. The research is not empirical and does not involve the collection of primary sociological or biometric data; instead, it employs desk methods characteristic of legal science and comparative law.

This study exclusively uses open sources that meet scientific, legal, and ethical criteria for use. The sources cover both national and international legal acts, analytical reports, peer-reviewed publications, and official statements.

Data collection was conducted based on the principle of relevance to the topic of using artificial intelligence in criminal proceedings, specifically considering aspects of transparency, accountability, appeal, and compliance with legal standards.

Official databases of legal acts of Azerbaijan: e-qanun.az ("On Personal Data", Law No. №998-IIIQ, 2010); "On Requirements for the protection of personal data", Law, 2010; "On the Prosecutor's Office", Law No. 767-IQ, 1999). Criminal Procedure Code of the Republic of Azerbaijan (Criminal Procedure Code of the Republic of Azerbaijan, Code, 2000); EUR-Lex, Council of Europe Legal Instruments, UN Treaties Database; EU General Data Protection Regulation (GDPR, 2016/679); European Convention on Human Rights ("On Human Rights", Convention, 1950); Council of Europe Convention "On the Automatic Processing of Personal Data" ("On data protection", Convention No. 108, 1981); Council of Europe Recommendations on the Ethical Use of AI in the Justice System (*Special file publication 2018 Edition of the CEPEJ report: "European judicial systems - Efficiency and quality of justice"*, 2018).

Peer-reviewed publications from databases such as SpringerLink, Cambridge University Press, Oxford Academic, SSRN, Scopus, Web of Science. The study also utilized information from news publications and official statements from government authorities.

Only sources that meet the following criteria are included in the study: 1). Sources directly related to the legal regulation or enforcement of AI in criminal proceedings (national or international law). 2). Preference is given to normative acts, official reports, and publications from peer-reviewed academic journals. 3). Scientific articles and other sources published no earlier than 2015, except for classic acts or doctrinal works that are of systemic importance.

The main method used in the study was black-letter analysis, which is used to study and interpret international and national law provisions relating to the use of artificial intelligence technologies in criminal proceedings. At the international level, the following were analyzed: The General Data Protection Regulation (GDPR), in particular Articles 22, 13–15 on automated decision-making and the right to explanation. The European Convention on Human Rights (ECHR), with particular emphasis on Article 6 (right to a fair trial) and Article 8 (right to privacy). The Council of Europe's guidelines on the ethical use of AI in justice

At the national level, legislative acts relating to the use of technology in Azerbaijan, in particular: the Criminal Procedure Code of the Republic of

Azerbaijan and other relevant subordinate legislation and regulations of state authorities (in particular, the Ministry of Internal Affairs and the Ministry of Justice). This analysis made it possible to determine the extent to which Azerbaijan's current legislation considers the challenges associated with algorithmic justice and whether there are mechanisms to control the use of automated systems in criminal cases.

A comparative legal method was used to identify gaps in national regulation. In particular, the main legal regimes and practices of countries where AI is already actively used in criminal justice were analyzed: the European Union (France, Germany) and Canada, the United States (Predictive Policing, algorithmic risk scoring in bail decisions), and, to some extent, Israel as an example of a country with a transitional economy that is already developing institutional strategies for the digital transformation of the security sector. This comparison made it possible to conclude relevant models of legal regulation that can be adapted to Azerbaijani laws. Particular attention should be paid to the analysis of mechanisms for ensuring the transparency of decisions, the right to appeal, and procedural equality of the parties.

Given the limited availability of comprehensive legal analyses and case studies on the use of AI in criminal proceedings in Azerbaijan, the study is partly based on adapting international experience to the local context. This approach is due to the lack of specialized reports or publications on the regulation of algorithmic justice within the Azerbaijani law enforcement system. At the same time, a review of digital initiatives in the judicial sphere (electronic document management, automatic case distribution) revealed potential for further regulation.

The study follows the rules of academic honesty and lawful behavior. The article did not involve the collection of personal data, did not interfere with personal or criminal information, and is based entirely on the analysis of open legal, scientific, and government sources. All documents used are publicly available and do not require special permission for citation or analysis.

C. RESULT AND DISCUSSION

The using of artificial intelligence or big data in criminal investigations requires a review of traditional procedural safeguards. Fundamental safeguards — the right to a fair trial, transparency, appeal, and equality of arms — must be adapted to the challenges of algorithmic justice (Završnik, 2020). An analysis of international and national legislation has made it possible to identify legal

mechanisms in place in leading jurisdictions and outline standards that can be adapted to Azerbaijan. Explainability and transparency in decision-making are crucial. Article 22 of the GDPR, which is part of the international legal system, says that people have the right to not have choices made about them based purely on automated data processing, including profiling, if those decisions have legal consequences (Mitrou, 2018). At the same time, Articles 13–15 of the GDPR also oblige the controller to provide understandable information about the logic of the algorithm, data categories, and the possibility of human intervention (Mitrou, 2018). Article 6 of the European Convention on Human Rights guarantees the right to a fair trial, which includes requirements for the comprehensibility and reasonableness of evidence ("On Human Rights", Convention, 1950). The Council of Europe's (CEPEJ) recommendations on the ethics of AI use in justice include the principle of explainability and human oversight (*Special file publication 2018 Edition of the CEPEJ report: "European judicial systems - Efficiency and quality of justice"*, 2018).

Among the fundamental principles, equality of the parties in access to algorithms also plays an important role. Article 6(3) of the ECHR allows the state to ensure the right to defense. This implies access to all evidence, even if it is generated automatically. In most jurisdictions, this requirement is not met because algorithms are often protected by copyright or trade secrets. As a result, the defense does not have equal access to AI analysis, which in turn violates the principle of equality of arms. At the same time, the principles of accountability and transparency are enshrined in the White Paper on Artificial Intelligence. This document states that modern states are obliged to implement a register of high-risk AI systems and a system of independent oversight. Table 1 shows the main procedural guarantees, relevant regulatory acts or precedents, jurisdictions, and the level of implementation of guarantees in practice.

Table 1.

Comparative characteristics of procedural guarantees when using AI in criminal investigations in different jurisdictions

Procedural guarantees	Source of law / regulatory framework	Implementation in practice
Right to algorithm transparency	GDPR (art. 13–15, 22); French Digital Republic Act (2016); Directive on ADM (Canada, 2019)	High: obligation to explain, access to decision-making logic in state structures
Right to appeal	Precedent <i>State v. Loomis</i> ; DMCA (copyright, USA)	Low: algorithms are often closed, transparency is limited by copyright
Equality of arms	ECHR (art. 6); <i>R (Bridges) v. South Wales Police</i> (UK, 2020); US Constitution (5th, 14th amendments)	Limitedly implemented: appeal is possible, but difficult without access to the logic of AI decisions

Accountability and independent audit	Constitution of Canada (art. 7, 11); Directive on ADM	Implemented: possibility of appeal in case of violation of procedural rights
Prevention of discrimination	ECHR (art. 6.3); US Constitution; AI Ethics Guidelines (EU AI Ethics Guidelines, 2019)	Violated: defense parties do not have equal access to algorithms and data sets
Access to information	Israel Criminal Procedure Law (amendments to 2020)	Partially ensured: lawyers can request technical documentation, but do not always receive full access
Ethical standards for the use of AI	White Paper on AI (EU, 2020); CEPEJ Guidelines (2018); Directive on ADM (Canada); Digital Charter Implementation Act (Canada)	High: independent control bodies (AI observatories, audit boards), public reporting mechanisms have been established
Procedural guarantees	EU Charter of Fundamental Rights (art. 21); German Anti-Discrimination Act; US Civil Rights Law	Partially implemented: discriminatory impact of algorithms remains difficult to prove
Right to algorithm transparency	French Law (2016); Canadian Algorithm Transparency Act; Freedom of Information Act (US)	Depends on the area: administrative data is available, and criminal data is limited or not at all
Right to appeal	CEPEJ Ethical Charter (2018); OECD AI Principles (2019); AI Ethics Guidelines (EU); AI Bill of Rights (US, 2022, draft)	Developed, but not always implemented: ethical standards often do not have legal force

Source: obtained from primary data

The integration of AI into criminal justice poses serious challenges to the protection of fundamental human rights. The risks center around algorithmic opacity, data bias, privacy violations, discrimination, restrictions on the right to defense, and threats of unlawful interference in private life. In some countries these challenges are exacerbated by insufficient regulation, weak institutional oversight, and a lack of independent control mechanisms.

The lack of algorithmic explainability poses a significant risk to human rights (Rahimova, 2025). Most AI systems used in criminal proceedings (from video surveillance analytics to offender behavior prediction) have a closed architecture. This makes it impossible to analyze how judgments about searches, arrests, and indictments are reached. Article 6 of the European Convention on Human Rights (the right to a fair trial) and Article 22 of the GDPR both ban fully automated decision-making. This means that citizens do not have access to the logic behind decisions, making effective appeal impossible.

At the same time, systems based on big data can often inherit social biases present in the original data sets. For example, AI may more often associate certain ethnic or social groups with the risk of committing crimes (Asgarova et al., 2022). COMPAS systems have demonstrated racial bias in predicting recidivism in the United States. However, no official studies of this kind have been conducted in Azerbaijan. Accordingly, this contributes to the

risk of hidden discrimination. It is also worth noting that modern algorithmic tools involve the mass collection and processing of personal data. At the same time, Azerbaijan's Law on the Protection of Personal Data does not contain clear provisions on biometric and automated profiles. There are also no requirements for storage, anonymization, or restriction of data use in criminal proceedings. In addition, the Azerbaijani Code of Criminal Procedure does not contain any provisions requiring the disclosure of algorithms or data processing methods used in evidence.

There is also a noticeable lack of independent oversight, like an AI Ombudsman or supervisory authority, which would oversee the use of algorithms in law enforcement agencies. This makes external audits impossible. Azerbaijan's Criminal Procedure Code does not contain provisions on automated systems, big data, or algorithms in the evidence process (Criminal Procedure Code of the Republic of Azerbaijan, Code, 2000). At the same time, the legislation does not provide for the right to verify the origin of digital evidence, AI logic, or analytical processing methods. Practical aspects are also not regulated in Azerbaijani law. No regulatory act requires ethical evaluation of algorithms or prior testing for discriminatory effects (See Table 2).

Table 2.
The main risks and gaps in Azerbaijani legislation

Risk Category	Risks identified	Gaps in Azerbaijan
Transparency	No access to algorithm logic	No legislative requirements for explainability and openness of algorithms
Privacy	Mass collection of sensitive data	2010 law ("On Personal Data") does not cover modern realities, no norms on biometrics
Discrimination	Data bias	No mechanisms for assessing the impact of algorithms, no ethical requirements
Appeal and Redress	Inability to challenge results	The CPC does not provide procedures for verifying or excluding algorithmic evidence
Accountability and Audit	Lack of external control	No oversight bodies, no obligation for state bodies to report

Source: obtained from primary data

The recognized concerns to human rights related with the use of AI in criminal processes, as well as loopholes in Azerbaijani legislation, need the formulation of comprehensive, normatively and institutionally sound guidelines. It is critical to develop legislation governing the use of AI in law enforcement. This can be accomplished by creating a distinct law governing the

use of AI in criminal procedures, which would include: 1). Defining the legal status of automated decisions; 2). Mandatory explainability of algorithms; 3). Obligation to conduct human rights impact assessments. It is also worth amending the Criminal Procedure Code to include provisions on: 1). The right of the parties to familiarize themselves with the logic of AI functioning if it is used as part of the evidence base; 2). The possibility of appealing algorithmic conclusions.

Another important aspect is the formation of transparency requirements for government agencies. They should provide protocols for explaining decisions made using AI. The introduction of ethical standards also plays an important role, in particular, it is worth developing a Code of Ethics for the use of AI in jurisprudence, consistent with: 1). CEPEJ Ethical Charter; 2). OECD AI Principles; 3). AI Bill of Rights draft. Finally, the professional development of law enforcement officers and judges plays an important role. In the future, effective training programs on digital legal ethics and algorithmic justice should be developed.

The study found that modern procedural guarantees, in particular transparency, appeal, equality of parties, and accountability, are not adequately enshrined in Azerbaijani law in the context of the use of AI in criminal proceedings. This contributes to the risk of violating the principle of fair trial (Article 6 of the ECHR), particularly about access to algorithms that may be used as evidence. In the international context, especially in EU countries and Canada, such guarantees are not only declared but also have institutional and procedural safeguards. For example, researchers have pointed out that leading countries have Algorithmic Impact Assessments in place to assess risks. EU countries also have transparency mechanisms in place in accordance with Article 22 of the GDPR (Nagy, 2023). At the same time, scientific works indicate that European legislation obliges authorities to use “explainable” algorithms. Thus, the data obtained confirm the relevance of the need to harmonize Azerbaijan's national legislation with international standards, about procedural access to data, the right of appeal, and the transparency of algorithmic decisions (Aliyeva, 2023).

The study identifies the main risks and gaps in Azerbaijan's national legislation. It notes that Azerbaijan's legal system lacks specific laws or regulations governing the use of AI in criminal investigations and defining the legal status of automated decisions. Furthermore, Azerbaijan's Code of Criminal Procedure does not contain provisions on automated systems, big data, or algorithms in the process of evidence gathering (Criminal Procedure

Code of the Republic of Azerbaijan, 2000). Summarizing the scientific positions, it can be noted that several authors point to the structural opacity of algorithmic systems as an important challenge for the law (Consulich, 2023). Moreover, Azerbaijan's Law on the Protection of Personal Data is not adapted to the challenges of the big data era and does not contain an equivalent to Article 22 of the GDPR, which allows a person not to comply with a decision made solely based on automated processing ("On Personal Data", The Law No. №998-IIIQ, 2010). This is consistent with research findings that demonstrate a lack of mechanisms for accessing code, training samples, and decision-making logic in Azerbaijan's national legal system. In particular, the authors emphasized that even with the existence of regulations, the practical implementation of safeguards may remain formal without oversight and transparency (Mikayilov, A. oğlu., 2023). Our findings confirm this, as there is no specific supervisory body or independent procedure for evaluating AI systems used in investigations in Azerbaijan. Other works also examine the phenomenon of "automated discrimination," which is difficult to challenge given limited access to algorithms. An identical risk has been identified in other studies, which point to cases of unequal access to technology by the parties (Leheza et al., 2021). This, in turn, violates the fundamental principle of equality of the parties. Moreover Azerbaijan's Law on the Protection of Personal Data ("On Personal Data," The Law No. №998-IIIQ, 2010) does not address the challenges of the big data era and lacks an equivalent to Article 22 of the GDPR, which allows individuals to object to automated processing decisions.

Based on a comparative analysis and the identified gaps, it is proposed to codify procedural guarantees in criminal proceedings that consider the challenges of algorithmic justice. It is also envisaged to amend the Criminal Procedure Code of Azerbaijan to provide for: the right of parties to access algorithms and training models, and a mechanism for appealing AI evidence. It is also proposed to create an independent supervisory body on digital justice and the use of AI in law enforcement and to introduce new educational programs for judges, prosecutors, and investigators on AI ethics and bias detection. These results are consistent with other authors who have emphasized the need to develop clear regulations governing access to code and data for parties to criminal proceedings. In addition, other works also mention the creation of specialized supervisory bodies with broad powers to control and audit algorithmic systems. Contemporary authors have emphasized the implementation of ethical standards and principles of transparency, fairness, and continuous monitoring, which is consistent with the motives behind the data obtained.

Despite attempts at in-depth analysis, the study has the following limitations. Notably, empirical data from Azerbaijan is lacking. This can be explained by the lack of public information on the use of AI in criminal cases, so the analysis is based on open sources and analogies with international practice. Another significant drawback is the focus on a normative rather than an empirical approach. This limits the consideration of the practical implications of the use of algorithms in real court cases.

D. CONCLUSIONS

The research revealed that procedural guarantees (transparency of algorithms, the right to appeal, and equality of parties) have varying levels of implementation worldwide. It has been proven that the use of AI affects the formation of risks for human rights, particularly the lack of access to algorithms, potential discrimination, and the limitation of appeal mechanisms. It is noted that Azerbaijani legislation contains significant gaps that require harmonization with international standards and the implementation of special control and oversight procedures for the use of AI. For this reason, to improve procedural guarantees in Azerbaijan, it is proposed to: codify the rights of parties to transparency in algorithmic decisions and access to information about the functioning of AI, introduce legislative norms regulating appeal procedures for AI-based decisions, develop and approve ethical criteria for the use of AI in criminal processes, and establish an independent oversight body or commission to oversee the use of AI in law enforcement activities.

Therefore, by identifying and systematizing regulatory limitations in the use of AI in the criminal process, the research significantly advances the field of legal science in Azerbaijan. The empirical examination of the effects of AI on Azerbaijani legal procedures should be the main subject of future studies. Examining instances and customs that take place in Azerbaijan is worthwhile. Methodologies for evaluating algorithmic bias in the national context should receive particular emphasis. Examining how legal institutions and technical advancements interact to create contemporary regulatory frameworks is another important future direction.

REFERENCES

Aliyeva, Z. "State Policy of Preventing Crimes Against a Person: Which Best Practices Should Be Used by Azerbaijan?" *Problems and Perspectives in*

Management 21, no. 4 (2023): 771–789.
[https://doi.org/10.21511/ppm.21\(4\).2023.57](https://doi.org/10.21511/ppm.21(4).2023.57).

Asgarov, B. M., and M. H. Mustafayev. "Systematic Analysis of the Use of Innovative Approaches in Operational and Investigative Activities: The Republic of Azerbaijan Case." *Futurity Economics & Law* 4, no. 3 (2024): 34–46. <https://doi.org/10.57125/fel.2024.09.25.03>.

Blount, K. "Using Artificial Intelligence to Prevent Crime: Implications for Due Process and Criminal Justice." *AI & Society* 39 (2022): 359–368. <https://doi.org/10.1007/s00146-022-01513-z>.

Buchholtz, G. "Artificial Intelligence and Legal Tech: Challenges to the Rule of Law." In *Regulating Artificial Intelligence*, 175–198. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-32361-5_8.

Caianiello, M. "Dangerous Liaisons: Potentialities and Risks Deriving from the Interaction Between Artificial Intelligence and Preventive Justice." *European Journal of Crime, Criminal Law and Criminal Justice* 29, no. 1 (2021): 1–23. <https://doi.org/10.1163/15718174-29010001>.

Consulich, F. "Criminal Law and Artificial Intelligence: Perspective from Italian and European Experience." *European Criminal Law Review* 13, no. 3 (2023): 270–307. <https://doi.org/10.5771/2193-5505-2023-3-270>.

Criminal Procedure Code of the Republic of Azerbaijan. 2000. https://e-qanun.az/framework/46950#_edn1.

Greenstein, S. "Preserving the Rule of Law in the Era of Artificial Intelligence (AI)." *Artificial Intelligence and Law*, 2021. <https://doi.org/10.1007/s10506-021-09294-4>.

Kilian, W. "Legal Tech: Artificial Intelligence and Legal Decisionmaking." *Computer Law Review International* 23, no. 4 (2022): 127–128. <https://doi.org/10.9785/cr-2022-230407>.

Leheza, Y., V. Len, O. Shkuta, O. Titarenko, and N. Cherniak. "Foreign Experience and International Legal Standards for the Application of Artificial Intelligence in Criminal Proceedings." *Revista de la Universidad del Zulia* 13, no. 36 (2021): 276–287. <https://doi.org/10.46925/rdluz.36.18>.

McKay, Carolyn. "Predicting Risk in Criminal Procedure: Actuarial Tools, Algorithms, AI and Judicial Decision-Making." *Current Issues in*

- Criminal Justice* 32, no. 1 (2019): 22–39.
<https://doi.org/10.1080/10345329.2019.1658694>.
- Mitrou, Lilian. "Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?" *SSRN Electronic Journal*, 2018.
<https://doi.org/10.2139/ssrn.3386914>.
- Nagy, Norbert. "Humanity's New Frontier: Human Rights Implications of Artificial Intelligence and New Technologies." *Hungarian Journal of Legal Studies* 64, no. 2 (2023): 236–267.
<https://doi.org/10.1556/2052.2023.00481>.
- Neiva, Luísa. "Big Data Technologies in Criminal Investigations: The Frames of the Members of Judiciary Police in Portugal." *Criminology & Criminal Justice*, 2023. <https://doi.org/10.1177/17488958231192767>.
- Mikayılov, A. oğlu. "Innovations in the Criminal Procedure of the Republic of Azerbaijan: Prospects for the Implementation of Modern Methods and Technologies in the Work of Specialists." *Futurity Economics & Law* 3, no. 4 (2023): 190–208. <https://doi.org/10.57125/fel.2023.12.25.12>.
- Council of Europe.** *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* ("Convention No. 108"), January 28, 1981. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=108>.
- Council of Europe.** *Convention for the Protection of Human Rights and Fundamental Freedoms* ("European Convention on Human Rights"), November 4, 1950.
https://www.echr.coe.int/documents/d/echr/convention_ENG.
- Republic of Azerbaijan.** *Law on Personal Data*, Law No. 998-IIIQ, 2010. <https://e-qanun.az/framework/19675>.
- Republic of Azerbaijan.** *Law on Requirements for the Protection of Personal Data*, 2010. https://e-qanun.az/framework/20046#_edn1.
- Republic of Azerbaijan.** *Law on the Prosecutor's Office*, Law No. 767-IQ, 1999. https://e-qanun.az/framework/5229#_edn1.
- Asgarova, M. P., Aliev, B. A., Khalilov, F. Y., & Hasanaova, I. Z. (2022). The use of electronic evidence in court: a comparative legal analysis in the world practice. *Cuestiones Políticas*, 40(72), 385-394.

<https://doi.org/10.46398/cuestpol.4072.21>

Quezada-Tavárez, K., P. Vogiatzoglou, and S. Royer. "Legal Challenges in Bringing AI Evidence to the Criminal Courtroom." *New Journal of European Criminal Law* 12, no. 4 (2021): 531–551. <https://doi.org/10.1177/20322844211057019>.

Ramos, A. "AI and Its Application in Criminal Investigation." In *Artificial Intelligence Approaches to Sustainable Accounting*, 26–33. Hershey, PA: IGI Global, 2024. <https://doi.org/10.4018/979-8-3693-0847-9.ch002>.

Rahimova, K. "Artificial Intelligence as a Remedy for Economic Crimes Through the Application of the Labeling Theory." *Scientific Work* 19, no. 2 (2025): 140–144. <https://doi.org/10.36719/2663-4619/111/140-144>.

Raso, F., H. Hilligoss, V. Krishnamurthy, C. Bavitz, and L. Y. Kim. "Artificial Intelligence & Human Rights: Opportunities & Risks." *SSRN Electronic Journal*, 2018. <https://doi.org/10.2139/ssrn.3259344>.

Council of Europe. *European Judicial Systems – Efficiency and Quality of Justice: Special File Publication 2018 Edition of the CEPEJ Report*, 2018. <https://www.coe.int/en/web/cepej/special-file-publication-2018-edition-of-the-cepej-report-european-judicial-systems-efficiency-and-quality-of-justice>.

Truby, J. "Governing Artificial Intelligence to Benefit the UN Sustainable Development Goals." *Sustainable Development* 28, no. 4 (2020): 946–959. <https://doi.org/10.1002/sd.2048>.

Yusifov, F. "Using Public Registers for Development of Electronic Demography System: The Case of Azerbaijan." *International Journal of Computing and Digital Systems* 10, no. 1 (2021): 1251–1261. <https://doi.org/10.12785/ijcds/1001112>.

Završnik, A. "Criminal Justice, Artificial Intelligence Systems, and Human Rights." *ERA Forum* 20, no. 4 (2020): 567–583. <https://doi.org/10.1007/s12027-020-00602-0>.

Ziobron, A. "Artificial Intelligence in the Context of Crime and Criminal Justice System – A Threat for the Rights of the Accused?" In *Artificial Intelligence and Human Rights*, 403–415. Madrid: Dykinson, 2021. <https://doi.org/10.2307/j.ctv282jgff.29>.