

Legal challenges of regulating artificial intelligence in law enforcement, taking into account the interdisciplinary approach to socio-legal transformations

Rauan Zhaltyrbayeva

Senior Lecturer

K. Zhubanov Aktobe Regional University

030000, 34 A. Moldagulova Ave., Aktobe, Republic of Kazakhstan

<https://orcid.org/0009-0009-1394-0863>

Arailym Jangabulova*

PhD in Law, Associate Professor

Al-Farabi Kazakh National University

050040, 71 Al-Farabi Ave., Almaty, Republic of Kazakhstan

<https://orcid.org/0000-0002-4150-5393>

Saule Suleimenova

Doctor of Law, Professor

Al-Farabi Kazakh National University

050040, 71 Al-Farabi Ave., Almaty, Republic of Kazakhstan

<https://orcid.org/0000-0002-6754-9255>

Sholpan Saimova

PhD in Law

“Institute of Parliamentarism” of the Department of Material and Technical Support

010000, 8 Mangilik El Ave., Astana, Republic of Kazakhstan

<https://orcid.org/0000-0002-9000-6136>

Zhanna Tlembayeva

PhD in Law, Professor

Astana Medical University

010000, 49A Beibitshilik Str., Astana, Republic of Kazakhstan

<https://orcid.org/0000-0003-4088-1087>

Abstract. This study examined the legal challenges associated with regulating artificial intelligence in law enforcement, considering its broader socio-legal transformations. Using an interdisciplinary approach, the research conducted a comparative legal analysis of AI regulations across multiple jurisdictions, assessing statutory frameworks, judicial decisions, and policy initiatives. The study identified key regulatory gaps, including the absence of clear statutory definitions, issues of accountability in AI-driven policing, and the risk of algorithmic bias. Through a comparative analysis of different jurisdictions, the study highlighted significant disparities in AI governance. The European Union adopts a precautionary and rights-based regulatory approach, classifying law enforcement AI as high-risk and imposing strict compliance requirements. The United States relies on decentralised governance, where state-level initiatives and judicial oversight shape AI deployment, leading to inconsistent enforcement. China prioritises state control, rapidly integrating AI surveillance into law enforcement without independent oversight, raising concerns about due process and human rights protections. In contrast, emerging jurisdictions like Kazakhstan and Kyrgyzstan are in the early stages of AI regulation, implementing AI-driven policing technologies while relying on general legal provisions. The study found

Suggested Citation

Article's History: Received: 25.02.2025 Revised: 21.05.2025 Accepted: 25.06.2025

Zhaltyrbayeva, R., Jangabulova, A., Suleimenova, S., Saimova, Sh., & Tlembayeva, Zh. (2025). Legal challenges of regulating artificial intelligence in law enforcement, taking into account the interdisciplinary approach to socio-legal transformations. *Social & Legal Studios*, 8(2), 118-130. doi: 10.32518/sals2.2025.118.

*Corresponding author



Copyright © The Author(s). This is an open access Article distributed under the terms of the Creative Commons Attribution License 4.0 (<https://creativecommons.org/licenses/by/4.0/>)

that AI's integration into law enforcement presents both opportunities and risks. While AI enhances policing efficiency and resource allocation, it also reinforces systemic biases, compromises data privacy, and challenges traditional accountability structures. The absence of regulatory harmonisation further complicates cross-border AI cooperation and liability determination. These findings underscored the need for clearer legal frameworks, international coordination, and ethical AI governance to balance security imperatives with fundamental rights. Given the rapid pace of AI adoption, future research should focus on empirical assessments of AI's real-world impact on legal systems, public trust, and law enforcement transparency, ensuring that regulatory approaches remain adaptive and equitable

Keywords: algorithmic accountability; biometric surveillance; data protection; automated decision-making; digital rights; public trust

Introduction

The integration of artificial intelligence (AI) into law enforcement has become an increasingly debated issue, shaped by legal, ethical, and societal considerations. Across different jurisdictions, AI-driven policing technologies reflect broader discussions on privacy, accountability, and the balance between public safety and civil rights. Legal frameworks governing AI applications in law enforcement vary significantly, influenced by constitutional principles, regulatory structures, and public concerns about surveillance and discrimination.

The relevance of this study is determined by the growing reliance on AI technologies in law enforcement and the challenges in ensuring transparency, fairness, and human rights protections. The legal and ethical issues surrounding AI-driven policing are particularly acute in jurisdictions where regulatory frameworks are underdeveloped, leading to concerns about mass surveillance, data privacy violations, and wrongful arrests. The increasing use of facial recognition, predictive policing, and automated decision-making tools has sparked legal disputes regarding due process, discrimination, and the right to challenge AI-generated decisions (Kovalchuk *et al.*, 2024). While AI-driven law enforcement promises efficiency and crime prevention, its risks necessitate a comprehensive legal and ethical examination of its impact on justice, public trust, and governance.

A review of existing research demonstrates a broad spectrum of approaches to AI regulation, highlighting the complexity of legal oversight and the ethical dilemmas associated with AI-driven policing. R.A. Berk (2021) examined the role of AI in predictive policing, demonstrating how algorithmic bias often reinforces racial and socioeconomic disparities. The study found that predictive crime mapping tools disproportionately classify low-income and minority communities as high-risk areas, leading to over-policing and systemic discrimination. P. Pokhariyal *et al.* (2024) explored AI-based decision-making in digital forensics, highlighting how AI-powered forensic analysis may perpetuate stereotypes, raising concerns about its role in judicial processes. Meanwhile, M.S. Kabir and M.N. Alam (2023) analysed facial recognition technologies, demonstrating that error rates in AI-based suspect identification are significantly higher for racial minorities, increasing the likelihood of wrongful arrests. Their findings underscore the urgent need for regulatory oversight to prevent AI from reinforcing structural inequalities in policing.

Further research has explored the transparency and accountability of AI-driven law enforcement. A. Chukaieva and S. Matulienė (2023) examined the legal implications of AI decision-making, emphasising how black-box algorithms obstruct due process by making it difficult to contest AI-generated outcomes. Meanwhile, A. Taeiagh (2021)

explored AI regulation in democratic societies, warning that unchecked AI surveillance could expand state power and threaten civil liberties. Another critical issue in AI policing is the conflict between mass surveillance and privacy rights. T. Singh (2023) examined the implications of AI-driven surveillance systems, noting how law enforcement agencies increasingly rely on real-time facial recognition and biometric tracking.

The ethical concerns surrounding AI in law enforcement also extend to public perception and trust in AI-driven policing. K. Wiek (2023) examined how AI's expansion in law enforcement affects public trust, finding that citizens in jurisdictions with strong AI oversight express higher confidence in law enforcement, while those in countries with minimal regulations are more skeptical. Y. Ezsedine *et al.* (2023) conducted a comparative study on public attitudes toward AI policing, revealing that younger populations tend to be more accepting of AI-driven law enforcement, whereas historically over-policed communities express greater distrust due to concerns about racial profiling and biased decision-making. Their research suggests that public engagement and transparency initiatives are necessary to build trust in AI-driven policing technologies.

Despite extensive research on AI regulation in law enforcement, gaps remain in understanding how AI governance models influence policing practices and civil rights protections. While various legal frameworks address AI accountability, their implementation and enforcement remain inconsistent, leading to uncertainties in oversight and potential human rights violations (Iklassova *et al.*, 2024). Existing studies document disparities in policy application, often influenced by political shifts, regulatory ambiguities, and evolving societal attitudes toward AI surveillance. The fragmented nature of AI regulation creates challenges in ensuring transparency, preventing bias, and maintaining due process protections across different legal systems (Lyndyuk *et al.*, 2024).

While international human rights standards advocate for ethical AI deployment, enforcement remains uneven, resulting in variations in civil liberties protections across jurisdictions. Some countries have introduced transparency and fairness requirements, while others lack clear guidelines on AI oversight in law enforcement. This divergence underscores the need for a more harmonised approach that balances technological advancements with fundamental rights protections.

This article aimed to contribute to the discussion by critically analysing the legal and ethical challenges of AI-driven policing, focusing on its implications for policy-making and justice. The research tasks included:

- examining AI regulatory frameworks and their effectiveness in mitigating algorithmic bias;

- analysing ethical principles that should guide AI adoption in law enforcement to ensure fairness and accountability;

- proposing policy recommendations that align AI governance with human rights protections and democratic principles.

Materials and methods

This study examined the legal challenges associated with the regulation of AI in law enforcement through an interdisciplinary approach, integrating legal analysis, ethical evaluation, and policy assessment. The research focused on international, regional, and national regulatory frameworks governing AI-driven law enforcement technologies, as well as their practical implications for policing, civil liberties, and human rights. The selection of legal frameworks and policy models was based on jurisdictional diversity, legislative precedents, and contemporary regulatory relevance to ensure a comprehensive evaluation of AI governance.

The theoretical component of the study was grounded in comparative legal analysis of international treaties, national legislation, constitutional provisions, judicial rulings, and policy guidelines that regulate AI deployment in law enforcement. This included a systematic examination of the Regulation of the European Parliament and of the Council No. 2024/1689 (2024), the General Data Protection Regulation (2016), the Algorithmic Accountability Act (2023), Interim Measures for the Management of Generative Artificial Intelligence Services (2023), Digital Code of the Kyrgyz Republic: Concept (2024), and the Law of the Republic of Kazakhstan No. 94-V “On Personal Data and their Protection” (2013). The selection of countries and regions for analysis was based on their distinctive approaches to AI regulation, reflecting a balance between global legal standards, regional regulatory frameworks, and national governance models.

The theoretical component of the study was grounded in a detailed comparative legal analysis of international treaties, national legislation, constitutional provisions, judicial rulings, and policy guidelines that regulate AI deployment in law enforcement. The comparison focused on several key aspects of AI regulation, including transparency and accountability mechanisms, the prevention of algorithmic bias, judicial and administrative oversight of AI-driven policing, data privacy protections, and the alignment of national AI policies with international human rights standards. By systematically examining these elements across different legal systems, the study identified patterns of convergence and divergence in AI governance.

Ethical considerations were explored through academic literature on data privacy, algorithmic accountability, non-discrimination, transparency, and due process in AI regulation, allowing for an in-depth assessment of how different legal models address fundamental rights and democratic accountability. The analysis considered the extent to which AI-driven law enforcement technologies align with ethical principles such as fairness, proportionality, and autonomy. Particular attention was given to issues of algorithmic bias, the right to contest AI-generated decisions, and the potential for AI surveillance to infringe on civil liberties.

The data analysis integrated comparative legal analysis, ethical evaluation, and thematic content analysis. The legal analysis focused on fundamental principles of AI

accountability, due process, privacy rights, and non-discrimination, comparing regulatory approaches across jurisdictions. Ethical evaluation assessed the extent to which existing AI governance frameworks align with principles of fairness, autonomy, transparency, and proportionality in law enforcement applications. Thematic content analysis was applied to policy documents, legal rulings, and empirical studies, allowing for the identification of recurring themes, challenges, and regulatory gaps. To enhance reliability and validity, multiple sources were cross-referenced, and legal interpretations were verified against primary legal texts. The study also incorporated an evaluation of judicial decisions and legal disputes surrounding AI use in law enforcement, providing an empirical dimension to the legal analysis. This approach ensured that the research was not only grounded in normative legal principles but also reflected the practical implications of AI governance in real-world policing scenarios.

Results

Legal challenges in regulating AI in law enforcement.

The findings of this study revealed that the regulation of artificial intelligence in law enforcement presents a series of complex legal challenges that stem from the rapid evolution of AI technologies, the opacity of AI decision-making processes, and the fragmented regulatory landscape governing AI applications. While AI has the potential to enhance policing efficiency, reduce human error, and optimize resource allocation, its deployment raises significant concerns regarding compliance with legal and constitutional principles. These concerns include the absence of clear accountability mechanisms, the risk of algorithmic bias, data privacy violations, and the lack of transparency in AI-generated decisions. The growing reliance on AI in criminal justice processes requires urgent legal and policy interventions to ensure that fundamental rights are not compromised under the pretext of technological progress.

A comparative assessment of AI regulations across different jurisdictions highlights the inconsistent approaches taken by governments and regulatory bodies, revealing significant disparities in how artificial intelligence is governed in law enforcement. These variations stem from different constitutional traditions, data protection laws, and judicial interpretations of fundamental rights, leading to legal uncertainty regarding AI accountability, bias mitigation, and law enforcement transparency.

The Regulation of the European Parliament and of the Council No. 2024/1689 (2024) represents the most comprehensive attempt at AI regulation globally. The Regulation classifies AI applications into four risk categories – unacceptable risk, high risk, limited risk, and minimal risk – each with corresponding compliance requirements. AI systems used in law enforcement, such as biometric surveillance, predictive policing, and automated risk assessments, fall under the high-risk category, requiring human oversight, mandatory transparency reports, and conformity assessments before deployment (Zaroff, 2022). Paragraph 33 of the Regulation explicitly prohibits AI applications that involve social scoring or real-time biometric identification in public spaces, except in strictly defined circumstances such as national security investigations.

However, despite its strong regulatory ambitions, challenges remain regarding its enforcement across 27 European Union member states. Article 65 of the Regulation of the Eu-

European Parliament and of the Council No. 2024/1689 (2024), which will oversee compliance and harmonisation across member states. P. Friedl and G.G. Gasiola (2024) argued that differences in national implementation, reliance on self-assessment for compliance, and potential loopholes in biometric surveillance exemptions may undermine the Act's effectiveness. Furthermore, the Regulation impact on cross-border AI cooperation and law enforcement data sharing within Europol and Schengen Area security frameworks remains uncertain.

In addition to the Regulation No. 2024/1689 (2024), the Regulation of the European Parliament and of the Council No. 2016/679 (2016) plays a critical role in limiting AI-driven data collection in law enforcement. This Regulation in Paragraph 71 mandates that individuals must not be subjected to fully automated decision-making with legal consequences unless specific exemptions apply, a provision highly relevant to AI-based risk assessment tools and predictive policing algorithms. Despite these legal safeguards, enforcement varies across member states, particularly when national security exemptions are invoked. For instance, France's AI-powered facial recognition system (PARAFE) has been criticised for lacking proportionality and independent oversight, highlighting the tension between AI-driven public security initiatives and fundamental rights under EU law (Poirson, 2021).

Unlike the EU's centralised AI governance, the United States relies on a fragmented regulatory approach, with AI oversight primarily occurring at the state level. The Illinois Biometric Information Privacy Act (BIPA) (2024) serves as one of the most stringent biometric regulations, requiring informed consent before collecting biometric identifiers such as facial recognition data. Court cases such as "Stacy Rosenbach" (Opinion of the Supreme Court of State of Illinois No. 123186, 2019) have reinforced BIPA's applicability to AI-driven surveillance tools, enabling individuals to sue companies for privacy violations without proving direct harm. At the federal level, the Algorithmic Accountability Act (2023) seeks to establish mandatory AI risk assessments for high-impact automated systems, including those used by federal law enforcement agencies. The Act would require the Federal Trade Commission (FTC) to audit AI models for bias and unfair decision-making, yet as of 2024, it remains a legislative proposal without enforcement mechanisms.

Judicial decisions continue to shape AI accountability in law enforcement. In case "State of Wisconsin, Plaintiff-Respondent, v. L. Loomis, Defendant-Appellant. On Certification from the Court of Appeals" (2016), the Wisconsin Supreme Court ruled that AI-generated risk scores in sentencing decisions must not be the sole determinant of judicial outcomes, citing due process concerns under the Fourteenth Amendment. Similarly, case "Williams v. City of Detroit, Michigan, A Municipal Corporation" (2021) exposed the flaws of AI-based facial recognition, as an incorrect algorithmic match led to a wrongful arrest, prompting legislative discussions on algorithmic transparency and liability in criminal justice.

China has emerged as a global leader in AI-driven law enforcement, deploying facial recognition, predictive policing, and social credit algorithms as part of its national security framework (Pisani, 2021). The Interim Measures for the Management of Generative Artificial Intelligence Services (2023) regulate AI-powered public surveillance,

deepfake technology, and automated content generation, requiring security assessments and government registration before deployment.

China's regulatory model prioritises state control over algorithmic accountability, which mandate compulsory AI data sharing with government agencies (Dong & Chen, 2024). Unlike the EU or U.S., China lacks independent oversight mechanisms, leading to concerns about mass surveillance, lack of judicial recourse, and potential human rights violations. Reports from Amnesty International (2020) have criticised China's Skynet AI surveillance system, which integrates real-time facial recognition with behavioral prediction models, for targeting ethnic minorities in Xinjiang.

The disparity in these regulatory approaches indicates that AI-driven law enforcement operates in a largely unregulated or inconsistently regulated space, raising concerns about international legal harmonisation and the extraterritorial effects of AI governance. The United Nations High Commissioner for Human Rights has called for a moratorium on AI-driven surveillance technologies, citing potential violations of Article 12 of the Universal Declaration of Human Rights (1948). However, there remains no binding international treaty specifically regulating AI in law enforcement, making it difficult to establish global standards for AI ethics and lawful use.

A major challenge in AI policing is lack of transparency in algorithmic decision-making. Black-box models – especially deep learning architectures used in facial recognition – are often non-interpretable, making it difficult for defendants, lawyers, and judges to challenge AI-generated evidence (Custers, 2022). Bias in AI policing remains a critical legal issue, as historical crime data reinforce systemic racial and socioeconomic disparities. In the UK case *R v. the Chief Constable of South Wales Police* (2020), the Court of Appeal ruled that AI-powered facial recognition disproportionately targeted racial minorities, violating the Equality Act 2010 (2013).

Kazakhstan has developed a structured legal framework for AI-related data practices, particularly in law enforcement, through its existing Law of the Republic of Kazakhstan No. 94-V "On Personal Data and their Protection" (2013) and the Resolution of the Government of the Republic of Kazakhstan No. 592 (2024). These documents outline key regulatory approaches to AI governance, with a focus on data security, transparency, and ethical use in automated decision-making. The first Law provides the foundation for AI-related data governance. This law defines the principles for the collection, processing, and protection of personal data, including biometric data, which are integral to AI-driven law enforcement technologies. Article 9 of the law permits law enforcement agencies to collect and process personal data without an individual's consent for purposes such as criminal investigations, judicial proceedings, and national security. However, it lacks explicit provisions on algorithmic accountability, AI bias mitigation, and due process guarantees for individuals affected by automated decision-making. This raises concerns about the potential for AI-driven mass surveillance and the lack of mechanisms for contesting AI-generated decisions.

In an effort to modernize AI governance, Kazakhstan adopted the Resolution of the Government of the Republic of Kazakhstan No. 592 (2024), which includes a dedicated section on AI regulation and legal frameworks. This plan emphasises the need for an adaptive regulatory environment

that ensures AI systems comply with ethical standards and international best practices. One of its key provisions is the establishment of oversight mechanisms for AI-driven law enforcement, including mandatory risk assessments, independent audits, and the introduction of legal standards for algorithmic transparency. The plan also acknowledges the necessity of integrating AI governance into Kazakhstan's broader digital transformation strategy, aiming to strike a balance between innovation and human rights protection.

Despite these advancements, Kazakhstan's AI regulatory landscape still faces gaps in ensuring fairness, transparency, and accountability. Unlike the Regulation of the European Parliament and of the Council No. 2024/1689 (2024), which imposes strict risk-based classifications for AI applications, Kazakhstan's approach remains largely focused on data security rather than comprehensive AI governance. Additionally, the absence of an independent regulatory body specifically overseeing AI in law enforcement presents challenges in enforcing compliance and addressing algorithmic bias.

Kazakhstan's approach to AI regulation in law enforcement contrasts with that of Kyrgyzstan, where legal discussions around AI governance are still in the conceptual phase. Kyrgyzstan has also initiated the process of developing legal regulations for artificial intelligence in law enforcement, focusing on broader principles of digital legislation. The primary regulatory document shaping the country's approach to digital governance is the Digital Code

of the Kyrgyz Republic (2024). This document outlines key directions for the development of digital technologies, including the application of algorithms and automated decision-making in public administration and law enforcement. The Concept emphasises the need for legal certainty, transparency, data protection, and alignment with international standards in AI governance.

Although Kyrgyzstan does not yet have specialised legislation explicitly regulating AI in law enforcement, the Digital Code Concept lays out fundamental principles that could shape future regulatory developments in this area. One of its core provisions is the necessity of restricting the use of automated algorithms in criminal prosecution to prevent discriminatory practices and the risks associated with algorithmic decision-making without human oversight. Additionally, the Concept proposes the introduction of mechanisms for independent auditing and ethical supervision of AI tools used in law enforcement and judicial systems, as well as mandatory risk assessments before AI technologies are deployed in policing and security operations.

Table 1 summarised a comparative analysis of AI regulatory frameworks across five jurisdictions – the European Union, the United States, China, Kazakhstan, and Kyrgyzstan – focusing on their legal approaches to AI governance in law enforcement. The differences in AI oversight reflect distinct legislative priorities, ranging from structured risk-based classifications in the EU to state-controlled AI governance in China.

Table 1. Comparative analysis of AI regulatory frameworks in law enforcement

Jurisdiction	Primary AI regulation	Risk classification approach	Enforcement mechanism	Transparency & accountability
European Union	Regulations of the European Parliament and of the Council No. 2024/1689 (2024) GDPR (2016)	Structured risk levels (unacceptable, high, limited, minimal)	European AI Board and national regulators	Mandatory audits, human oversight
United States	Algorithmic Accountability Act (2023), BIPA (2024)	State-driven, no federal standard	State-level oversight, FTC involvement	Case-based regulation, court challenges
China	Interim Measures for the Management of Generative Artificial Intelligence Services (2023)	State-controlled, lacks independent oversight	Government-mandated compliance, no independent review	Opaque decision-making, no public recourse
Kazakhstan	Law of the Republic of Kazakhstan No. 94-V (2013), Resolution of the Government of the Republic of Kazakhstan No. 592 (2024)	Data protection-focused, lacks AI-specific risk classification	Government regulatory agencies, limited AI oversight	Data transparency provisions, but no AI accountability framework
Kyrgyzstan	Digital Code of the Kyrgyz Republic: Concept (2024)	Developing regulatory framework, lacks specificity	Emerging legal structure, potential oversight gaps	Conceptual stage, undefined oversight

Source: compiled by the authors

The findings of this study confirm that AI regulation in law enforcement remains fragmented, with gaps in accountability, algorithmic bias protections, and cross-border regulatory coherence. While the Regulation of the European Parliament and of the Council No. 2024/1689 (2024) offers a structured risk-based approach, the U.S. relies on state-level governance, and China prioritises national security over individual rights. Addressing these challenges requires a combination of legislative reform, judicial oversight, and interdisciplinary collaboration among legal scholars, policy-makers, and AI ethicists. Without comprehensive regulation, AI-driven law enforcement risks compromising fundamental rights and undermining public trust in justice systems (Apostolakis *et al.*, 2022).

The text provides a comparative overview of AI governance in law enforcement across several countries, highlighting Kazakhstan's recent regulatory efforts and Kyrgyzstan's early-stage initiatives. Kazakhstan has introduced mechanisms like audits and risk assessments but still lacks comprehensive oversight, especially compared to the EU's structured, risk-based approach. Kyrgyzstan, while not yet implementing specific AI laws, outlines foundational principles in its Digital Code that emphasize transparency and human oversight. Overall, the analysis reveals a fragmented global landscape in AI regulation, with persistent gaps in accountability, fairness, and international coherence.

Socio-legal transformations resulting from AI in law enforcement. Beyond the immediate legal challenges, the

findings of this study also highlight broader socio-legal transformations that have emerged as AI becomes increasingly integrated into law enforcement. These transformations are reshaping the nature of policing, the relationship between law enforcement agencies and the public, and the role of judicial oversight in AI-assisted criminal justice procedures. AI's rapid adoption in law enforcement has altered traditional policing paradigms, creating new ethical, legal, and social considerations that require urgent regulatory attention.

One of the most profound transformations observed is the shift toward preemptive law enforcement, facilitated by AI-driven predictive policing (Kheira, 2024). Traditional law enforcement strategies have historically been reactive, focusing on responding to crimes after they have been committed. However, AI allows for data-driven crime prediction, where law enforcement resources are directed to locations or individuals deemed high-risk based on algorithmic assessments. This transformation fundamentally alters the role of police officers, shifting their focus from traditional investigation and response to preventive surveillance and intervention. The concept of “predictive justice” – where crimes are anticipated and preemptively addressed before they occur – has been widely debated among legal scholars and human rights advocates (Dhanya, 2024; Patra, 2024).

While predictive policing has been recognised for optimising resource allocation and reducing response times, its deployment has also led to self-reinforcing feedback loops that disproportionately impact marginalised communities (Chapman *et al.*, 2022). This occurs when AI models trained on historical crime data identify certain neighborhoods as high-crime areas, leading to increased law enforcement presence, which in turn results in higher recorded crime rates in those communities (Stensland, 2023). In the US, a study published in the journal *Social Problems* found that judges use algorithmic risk assessment tools selectively to inform their decisions, rather than relying entirely on the assessments provided (Felner, 2024). This suggests that such tools can legitimise existing biases and conceal deeper ones. In the UK, an Amnesty International report entitled “Automated Racism” criticised the use of predictive policing, stressing

that the practice is racist and disproportionately affects poor and black communities (Moy, 2021; Dodd, 2025). Report argued that predictive policing tools are based on biased data derived from discriminatory police practices such as stop and frisk, which leads to increased racial and socio-economic disparities in law enforcement. Furthermore, the Los Angeles Police Department's PredPol system, which was intended to predict crime hotspots based on historical arrest data, faced widespread criticism after reports revealed that it disproportionately flagged communities of color as high-crime areas, leading to over-policing and increased instances of racial profiling (Automating Banishment, 2021). The study suggests that this risk of AI-driven over-policing must be carefully balanced against fundamental rights, including due process, freedom of movement, and non-discrimination.

Public perception of AI-driven law enforcement represents a significant socio-legal transformation that will influence the long-term viability and legitimacy of AI adoption in policing. The data from Table 2 indicate a generational and demographic divide in attitudes toward AI policing across different national contexts. Younger populations, particularly in Germany, where 81.2% of participants were under 35 years old, tend to be more accepting of AI integration in law enforcement, seeing it as a means of enhancing efficiency, reducing human bias, and streamlining administrative processes. Conversely, in the UK, where a significant portion of respondents (27.3%) were over 55 years old, there is a greater emphasis on privacy concerns, reflecting a more cautious approach to AI surveillance and law enforcement tools. Moreover, cybersecurity expertise influences AI acceptance, as demonstrated by responses in the Netherlands, where 37.5% of participants fell within the 34-55 age range. Participants in this group exhibited a more analytical stance toward AI use in law enforcement, emphasising the importance of cybersecurity risks and regulatory safeguards. However, across all demographics, minority groups and historically over-policed communities continue to express significantly higher levels of distrust, citing concerns about AI reinforcing racial profiling, systemic discrimination, and mass surveillance.

Table 2. Public perception of AI in law enforcement

Country	Total participants	Average age	Gender distribution (female/male)	Participants < 35 years	Participants 34-55 years	Participants > 55 years	Predominant perspective
UK	11	33.4	72.7%/27.2%	63.6%	36.4%	27.3%	Privacy Concerns
Netherlands	16	32.3	43.7%/56.2%	62.5%	37.5%	0%	Cybersecurity Expertise
Germany	16	26.3	100%/0%	81.2%	18.7%	12.5%	Youth-Oriented AI Perception

Source: compiled by the authors based on Y. Ezsedine *et al.* (2023)

Distrust is not unfounded, as multiple reports and legal cases have demonstrated that AI-driven law enforcement tools often fail to provide equal protection under the law. In case “Williams v. City of Detroit, Michigan, A Municipal Corporation” (2021), a Michigan man was wrongfully arrested based on a false facial recognition match, raising questions about the reliability of AI in criminal identification. Similarly, in the United Kingdom, the case of R v. the Chief Constable of South Wales Police (2020) resulted in a

landmark ruling by the UK Court of Appeal, which found that the police's use of automated facial recognition technology violated privacy rights and data protection laws. This ruling underscores the growing legal scrutiny surrounding AI surveillance technologies and their impact on public trust in law enforcement.

The research findings suggest that public confidence in AI-assisted policing is directly correlated with the level of transparency and oversight applied to these systems. In

jurisdictions where law enforcement agencies provide clear public disclosures about AI deployment, including independent auditing, algorithmic transparency, and community engagement, trust in AI policing is notably higher. However, in jurisdictions where AI systems are deployed without clear legal safeguards, public skepticism remains widespread.

The EDPS statement in view of the 10th and last Plenary Meeting of the Committee on Artificial Intelligence (CAI) of the Council of Europe drafting the Framework Convention on Artificial Intelligence (2024) has warned that a lack of transparency in AI policing could undermine democratic values, particularly if AI-driven surveillance technologies are used to monitor political dissent or suppress civil liberties. The study emphasises that public engagement and community-based discussions must be prioritised when introducing AI-driven law enforcement tools to ensure social legitimacy, ethical compliance, and legal accountability.

Another significant transformation is the increasing reliance on AI in judicial decision-making, particularly in bail determinations, sentencing guidelines, and parole assessments. Some jurisdictions have begun implementing AI-powered risk assessment tools to assist judges in evaluating the likelihood of reoffending, but the study finds that these tools often lack transparency and fail to account for individual circumstances beyond statistical probabilities (PAI Staff, 2019).

For instance, in the U.S. criminal justice system, AI-driven risk assessment tools such as Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) have been used to predict recidivism rates, influencing bail and sentencing decisions. However, investigative report from J. Angwin *et al.* (2016) found that COMPAS exhibited racial bias, as Black defendants were disproportionately classified as high-risk compared to White defendants, even when controlling for similar criminal histories. This raises fundamental questions about the role of human discretion in legal decision-making and whether AI should be granted authority in matters of justice.

Kazakhstan is actively implementing the concept of smart policing by integrating advanced technologies such as AI and big data analytics into law enforcement operations (Kenawy, 2025). This approach aims to enhance efficiency and responsiveness in crime prevention. The use of AI enables law enforcement agencies to identify patterns in criminal activity, facilitating crime prediction and the optimal allocation of resources to prevent incidents.

The implementation of such technologies presents several legal challenges. It is necessary to develop a regulatory framework governing the use of AI in law enforcement, particularly concerning data protection, algorithmic transparency, and the prevention of discriminatory practices. Additionally, an interdisciplinary approach that combines legal, social, and technical perspectives is crucial to establishing a balanced and effective AI governance system in policing.

Kyrgyzstan has also begun integrating AI into law enforcement, with a particular focus on facial recognition and predictive analytics. The introduction of AI-powered facial recognition cameras under the “Safe City” initiative has already altered policing strategies, with over 50 AI-driven surveillance cameras deployed in Bishkek and other urban areas (Zhakshe kyzy & Shambetov, 2023). These cameras assist law enforcement in identifying suspects and enforcing traffic violations, with reports suggesting that the system has contributed to the identification of over 650 wanted

individuals and 500 missing teenagers in 2024 alone (Khan & Rizvi, 2021; 650 wanted people..., 2025;).

Public perception of AI policing in Kyrgyzstan reflects broader global concerns. Privacy advocates and civil society organisations have criticised the system’s potential for misuse, particularly in tracking activists and journalists (Wang, 2019). Kyrgyzstan has no specific AI law regulating law enforcement’s use of biometric surveillance, meaning that police can operate facial recognition tools under broad national security exemptions. This legal vacuum raises issues similar to those seen in other jurisdictions, where AI surveillance is deployed without clear accountability mechanisms. Critics warn that without strong oversight measures, AI policing in Kyrgyzstan may disproportionately impact vulnerable groups, leading to potential rights violations (Bolt Junusov, 2019).

The research suggests that while AI can serve as a supplementary tool for judicial analysis, human oversight and interpretability remain essential to maintaining fairness and individualised justice. Legal scholars have argued that AI-driven sentencing recommendations must be auditable, challengeable, and subject to judicial review to prevent unjust sentencing outcomes based on flawed predictive models. Finally, this study highlights the expansion of AI-driven surveillance, which has reshaped the balance of power between state authorities and civil liberties. AI-powered facial recognition, behavioral tracking, and biometric monitoring have significantly increased law enforcement’s surveillance capabilities, raising concerns about the potential erosion of privacy rights and the normalisation of mass surveillance.

The European Union has introduced restrictions on AI surveillance through the GDPR and the proposed Regulation of the European Parliament and of the Council No. 2024/1689 (2024), which aims to prohibit real-time facial recognition in public spaces except in cases of national security or serious crime investigations. However, countries such as China, the United Arab Emirates, and Russia have adopted AI surveillance on a vast scale, with limited oversight and legal constraints (Zeng *et al.*, 2021). The United Nations Special Rapporteur on the Right to Privacy has raised concerns about the use of AI surveillance to suppress political activism and freedom of expression, particularly in authoritarian regimes. The study concludes that regulatory frameworks must establish clear legal boundaries for AI surveillance, ensuring that law enforcement’s use of AI remains proportionate, necessary, and subject to independent oversight.

This research demonstrated that AI is fundamentally reshaping the legal and social landscape of law enforcement, requiring urgent regulatory and policy responses. The findings highlight that AI’s integration into predictive policing, judicial decision-making, and surveillance technologies has transformed law enforcement practices, but not without significant socio-legal consequences. Without comprehensive legal safeguards, AI in policing risks undermining civil liberties, reinforcing bias, and reducing accountability. The study underscored the need for a balanced regulatory approach that protects democratic values while allowing law enforcement to harness AI responsibly. AI-driven law enforcement must be guided by transparent policies, independent oversight, and public engagement to ensure that technological advancements serve the interests of justice rather than eroding fundamental rights.

Discussion

This study highlights the challenges of regulating AI in law enforcement, emphasising the rapid technological advancements that outpace existing legal frameworks. The analysis identifies three core issues: the absence of clear statutory definitions, concerns over accountability and bias in AI-based policing, and significant jurisdictional disparities in AI governance. The findings affirm that AI, while capable of enhancing efficiency and decision-making, also threatens fundamental rights and public trust when left unregulated. These results underscore the need for coherent, interdisciplinary regulatory approaches that integrate legal, technological, and societal perspectives.

The lack of explicit legal definitions and frameworks for AI in law enforcement emerged as a central issue. Many jurisdictions have yet to establish precise rules governing AI applications in policing, leading to legal uncertainties. This regulatory gap arises because technological innovations often outpace legislative processes, leaving law enforcement agencies to operate in a grey area. Without robust legal standards, fundamental principles such as transparency, accountability, and fairness remain aspirational.

Bias and accountability present persistent concerns in AI-driven policing. Predictive policing and facial recognition technologies can replicate and amplify historical biases, disproportionately targeting minority communities. The study found weak or absent oversight mechanisms in most jurisdictions, corroborating existing research that AI-based law enforcement tools often lack fairness and accuracy. The “black-box” problem, where proprietary AI systems obscure decision-making processes, exacerbates these issues. Interestingly, some police departments have begun implementing internal guidelines to mitigate bias, even in the absence of binding regulations. However, the lack of enforceable legal requirements for algorithmic transparency and accountability remains a major risk.

The study also reveals significant jurisdictional differences in AI governance. The European Union follows a precautionary, rights-driven regulatory approach, with the forthcoming Regulation of the European Parliament and of the Council No. 2024/1689 (2024) classifying law enforcement AI tools as high-risk and prohibiting certain applications, such as real-time biometric surveillance, except in limited scenarios (Yanyshivskiy, 2024). In contrast, the United States lacks federal AI laws specific to policing, relying on a fragmented mix of state laws, judicial rulings, and local bans on facial recognition. This reactive approach emphasises balancing innovation with civil rights, with courts playing a crucial role in defining AI’s legal boundaries. Meanwhile, China’s model prioritises rapid AI integration for national security and social management, governed by broad regulations rather than dedicated AI laws (Zeng, 2022). This approach enables rapid deployment but raises rule-of-law concerns due to limited oversight and avenues for public recourse. Kazakhstan is integrating AI-driven policing tools such as facial recognition and predictive analytics. While it lacks a dedicated AI law governing law enforcement applications, it relies on general data protection legislation and constitutional privacy rights (Saparbekova *et al.*, 2024). The country has taken early steps toward AI regulation through the Resolution of the Government of the Republic of Kazakhstan No. 592 (2024) and its participation in regional initiatives such as the CIS model AI law, signaling efforts toward legal

harmonisation. Findings from this research align with and extend previous studies on AI governance in law enforcement. K. Alikhademi *et al.* (2022) identified transparency, fairness, and accuracy as critical concerns in predictive policing and risk assessment, emphasising that these factors involve inherent trade-offs that cannot be entirely resolved through technical solutions. This is consistent with the conclusion that regulatory and policy interventions are essential to balancing effective policing with human rights protections. Similarly, the identification of bias and accountability challenges reinforces prior studies on algorithmic risk assessments, such as the COMPAS controversy, where racial disparities in recidivism predictions triggered legal debates on due process.

In terms of regulatory responses, the EU’s structured AI governance approach aligns with prior analyses of European digital rights policies, which emphasize ethical AI principles (Petrovskiy *et al.*, 2025). Studies on the Regulation of the European Parliament and of the Council No. 2024/1689 (2024) highlight its ambition as the world’s most comprehensive AI regulation, explicitly classifying police AI tools as high-risk or prohibiting them in sensitive applications. This study confirms this trajectory, showing that Europe prioritises fundamental rights and accountability over unfettered AI deployment. By contrast, P.G.R. De Almeida *et al.* (2021), suggested that American AI regulation will likely adapt existing legal doctrines rather than introduce comprehensive legislation. The findings support this perspective, as U.S. AI governance remains decentralised, driven by litigation and state-level initiatives rather than national policy.

This research also adds an international dimension that is underrepresented in existing studies by comparing AI governance in China and Central Asia. While Western scholarship frequently focuses on EU and U.S. models, the study examines how China’s state-driven AI adoption contrasts with rights-based frameworks. The findings align with prior critiques that Chinese AI governance prioritises state control over individual rights, raising concerns about surveillance and lack of recourse. Meanwhile, Kyrgyzstan’s nascent regulatory efforts illustrate the transnational influence of AI governance, as its adoption of Chinese-built facial recognition technology has triggered domestic privacy debates. This broadens the AI policing discourse beyond high-income democracies, highlighting regulatory challenges in emerging jurisdictions.

The examination of public perception further complements existing socio-legal research. L. Xia *et al.* (2023) found that citizen attitudes toward AI in policing vary based on demographic and cultural factors, balancing security benefits against privacy concerns. The findings confirm this complexity, showing that AI policing is met with skepticism, particularly among historically over-policed communities. The study emphasises that regulatory solutions must incorporate public trust considerations to ensure legitimacy and compliance. Overall, the results confirm and expand upon existing research, reinforcing known challenges such as bias, accountability, and legal fragmentation while introducing new insights on regional cooperation and emerging AI governance models.

This research contributes to AI regulation in law enforcement by integrating legal, technological, and social perspectives. The study underscores AI’s role as a socio-legal disruptor, reshaping policing norms, institutional practices, and public expectations. By framing AI regulation as more than a legal issue, this study contributes to a more holistic understanding of responsible AI governance. For policymakers,

the findings emphasize the urgent need for clear legal definitions and comprehensive regulatory frameworks for AI policing. Jurisdictions can learn from the EU's structured risk-based classification or consider emerging regional models, such as the CIS AI law initiative. Harmonised legal standards across jurisdictions can prevent regulatory arbitrage and enhance cross-border AI governance. For law enforcement and legal professionals, the study highlights the importance of internal AI policies and professional training. Police departments should develop ethical guidelines, establish bias-mitigation strategies, and implement independent oversight mechanisms to prevent AI-driven discrimination. Legal practitioners must be prepared to scrutinize AI-derived evidence, ensuring it meets due process and evidentiary standards. For technologists and AI developers, the research underscores the need to design AI tools with built-in transparency, explainability, and bias mitigation. Developers should anticipate emerging regulations by incorporating compliance-ready features, such as decision-logging and independent auditing capabilities. Engaging legal experts in AI development can help ensure adherence to ethical and legal standards. By providing these insights, the study bridges the gap between theory and practice, offering concrete recommendations for responsible AI governance in law enforcement.

The legal regulation of AI in law enforcement is at a pivotal moment. This study demonstrates that while AI offers potential benefits in crime prevention and resource optimisation, it also presents profound risks to privacy, due process, and non-discrimination. The findings emphasize that regulatory frameworks must evolve to address AI's socio-legal impact, ensuring that its integration into policing aligns with democratic values and human rights. Jurisdictional comparisons illustrate that while the EU is moving toward strict AI governance, the U.S. relies on judicial oversight, China emphasises state control, Kazakhstan and Kyrgyzstan are still defining their regulatory paths.

A forward-looking regulatory approach should balance innovation with accountability, incorporating interdisciplinary perspectives. Lawmakers must proactively establish legal safeguards, law enforcement agencies should implement responsible AI policies, and technologists should prioritize ethical AI design. Moving forward, future research should explore cross-jurisdictional regulatory harmonisation and assess the long-term impacts of AI policing on civil liberties. As AI continues to shape the legal and social landscape of law enforcement, ensuring transparent, accountable, and rights-respecting AI governance is imperative. Only through deliberate legal and policy clarity can societies harness AI's benefits while safeguarding fundamental freedoms.

Conclusions

This study explored the legal challenges of regulating artificial intelligence in law enforcement, focusing on the socio-legal transformations driven by AI adoption. The findings reveal significant gaps in existing legal frameworks, accountability issues, and jurisdictional differences in AI governance. While AI offers efficiency gains in policing, it also raises critical ethical and legal concerns related to transparency, fairness, and fundamental rights. Without clear regulations, these technologies risk undermining public trust and exacerbating systemic biases.

A key finding was the regulatory lag that prevents laws from keeping pace with AI advancements. Many jurisdictions

lack statutory definitions or oversight mechanisms, leading to inconsistent governance and enforcement. This absence of legal clarity allows AI to be deployed in ways that may conflict with constitutional rights, particularly in biometric surveillance and predictive policing. Although some regions are working toward AI legislation, progress remains slow, reinforcing concerns that technology is evolving faster than regulatory adaptation.

The study also highlights risks associated with algorithmic bias and AI opacity in law enforcement. Predictive policing models and facial recognition technologies often replicate and amplify historical biases, disproportionately impacting marginalised communities. Additionally, AI systems frequently operate as black boxes, making their decision-making processes difficult to interpret or challenge. While some police agencies have implemented internal guidelines to mitigate bias, the absence of legal mandates for algorithmic transparency and oversight remains a major concern.

A comparative analysis of regulatory approaches reveals considerable variation. The Regulation of the European Parliament and of the Council No. 2024/1689 adopts a precautionary framework, classifying law enforcement AI systems as high-risk and imposing strict compliance requirements. The Act's emphasis on accountability and human oversight reflects the EU's rights-based regulatory model. In contrast, the United States relies on a decentralised approach, with state-level legislation and judicial rulings shaping AI governance. This fragmented model results in uneven oversight and a reliance on constitutional litigation rather than comprehensive federal regulation. China, meanwhile, has rapidly expanded AI-driven policing under a state-controlled framework that prioritises security over individual rights. The lack of independent oversight in China's AI governance raises concerns about unchecked surveillance and limited legal recourse. Smaller jurisdictions, such as Kazakhstan and Kyrgyzstan, are in the early stages of AI regulation, relying on general legal provisions rather than AI-specific laws. While AI-driven surveillance initiatives are emerging, governance remains uncertain. These findings contribute to the broader discussion on AI regulation by illustrating how different legal models influence AI's role in law enforcement. The lack of international harmonisation complicates cross-border cooperation, data-sharing agreements, and liability frameworks for AI-driven decisions. As AI technology evolves, a coordinated approach integrating legal, ethical, and technological perspectives is essential to ensure that AI is deployed responsibly and equitably.

Overall, this study underscored the urgent need for clear, enforceable legal frameworks to govern AI in law enforcement. Without proper oversight, AI risks being deployed in ways that infringe on rights and erode public confidence. Moving forward, legal and policy efforts must prioritize regulatory clarity, international cooperation, and ethical AI governance to ensure a balanced approach that safeguards both security and civil liberties.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of interest

None.

References

- [1] 650 wanted people caught with help of facial recognition security cameras in Bishkek in 2024. (2025). Retrieved from <https://surl.lu/pgiikv>.
- [2] Algorithmic Accountability Act of 2023. (2023, September). Retrieved from <https://www.congress.gov/bill/118th-congress/house-bill/5628/text>.
- [3] Alikhademi, K., Drobina, E., Prioleau, D., Richardson, B., Purves, D., & Gilbert, J.E. (2022). A review of predictive policing from the perspective of fairness. *Artificial Intelligence and Law*, 30. doi: 10.1007/s10506-021-09286-4.
- [4] Amnesty International. (2020). *Out of control: Failing EU laws for digital surveillance export*. Retrieved from <https://www.amnesty.org.ua/wp-content/uploads/2020/09/out-of-control-amnesty-international-eur01-2556-2020.pdf>.
- [5] Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine bias: Risk assessments in criminal sentencing*. Retrieved from <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.
- [6] Apostolakis, K.C., Dimitriou, N., Margetis, G., Ntoa, S., Tzovaras, D., & Stephanidis, C. (2022). DARLENE – Improving situational awareness of European law enforcement agents through a combination of augmented reality and artificial intelligence solutions. *Open Research Europe*, 1, article number 87. doi: 10.12688/openreseurope.13715.2.
- [7] Automating banishment: The surveillance and policing of looted land. (2021). Retrieved from <https://automatingbanishment.org/>.
- [8] Berk, R.A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology*, 4, 209-237. doi: 10.1146/annurev-criminol-051520-012342.
- [9] Biometric Information Privacy Act. (2024). Retrieved from <https://law.justia.com/codes/illinois/chapter-740/act-740-ilcs-14/>.
- [10] Bolot Junusov. (2019). “Safe City”, facial recognition. Who is hindered by new technologies in Bishkek. Retrieved from <https://24.kg/vlast/135511-bezopasnyiy-gorod-raspoznvanie-lits-komu-meshayut-novyye-tehnologii-v-bishkeke/>.
- [11] Chapman, A., Grylls, P., Ugwu-dike, P., Gammack, D., & Ayling, J. (2022). A Data-driven analysis of the interplay between Criminological theory and predictive policing algorithms. In *Proceedings of the 2022 ACM conference on fairness, accountability, and transparency* (pp. 36-45). Seoul: Association for Computing Machinery. doi: 10.1145/3531146.3533071.
- [12] Chukaieva, A., & Matulienė, S. (2023). Possibilities of applying artificial intelligence in the work of law enforcement agencies. *Scientific Journal of the National Academy of Internal Affairs*, 28(3), 28-37. doi: 10.56215/naia-herald/3.2023.28.
- [13] Custers, B. (2022). AI in criminal law: An overview of AI applications in substantive and procedural criminal law. In B. Custers & E. Fosh-Villaronga (Eds.), *Law and artificial intelligence: Regulating AI and applying AI in legal practice* (pp. 205-223). Hague: T.M.C. Asser Press. doi: 10.1007/978-94-6265-523-2_11.
- [14] De Almeida, P.G.R., dos Santos, C.D., & Farias, J.S. (2021). Artificial intelligence regulation: A framework for governance. *Ethics and Information Technology*, 23, 505-525. doi: 10.1007/s10676-021-09593-z.
- [15] Dhanya, K.S. (2024). *Artificial intelligence in justice system and its ethical and legal implications: A comparative analysis*. Kochi: National University of Advanced Legal Studies.
- [16] Digital Code of the Kyrgyz Republic: Concept. (2024). Retrieved from <https://internetpolicy.kg/wp-content/uploads/2023/04/%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D1%8F-%D0%A6%D0%9A-eng-1.pdf>.
- [17] Dodd, V. (2025). *UK use of predictive policing is racist and should be banned, says Amnesty*. Retrieved from <https://www.theguardian.com/uk-news/2025/feb/19/uk-use-of-predictive-policing-is-racist-and-should-be-banned-says-amnesty>.
- [18] Dong, H., & Chen, J. (2024). Meta-regulation: An ideal alternative to the primary responsibility as the regulatory model of generative AI in China. *Computer Law & Security Review*, 54, article number 106016. doi: 10.1016/j.clsr.2024.106016.
- [19] EDPS statement in view of the 10th and last Plenary Meeting of the Committee on Artificial Intelligence (CAI) of the Council of Europe drafting the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. (2024). Retrieved from <https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-statement-view-10th-and-last-plenary-meeting-committee-artificial-intelligence-cai-council-europe-drafting-framework-convention-artificial-en>.
- [20] Equality Act 2010: Guidance. (2013, February). Retrieved from <https://www.gov.uk/guidance/equality-act-2010-guidance>.
- [21] Ezsedine, Y., Bayerl, P.S., & Gibson, H. (2023). Safety, privacy, or both: Evaluating citizens’ perspectives around artificial intelligence use by police forces. *Policing and Society*, 33(7), 861-876. doi: 10.1080/10439463.2023.2211813.
- [22] Felner, L. (2024). *Judges are using algorithms to justify doing what they already want/Algorithmic risk scores might be obscuring a broader issue with how the judicial system works*. Retrieved from <https://www.theverge.com/2024/10/30/24281924/pretrial-risk-assessment-algorithms-research>.
- [23] Friedl, P., & Gasiola, G.G. (2024). *Examining the EU’s Artificial Intelligence Act*. Retrieved from <https://verfassungsblog.de/examining-the-eus-artificial-intelligence-act/>.
- [24] Iklassova, K., Aitymov, A., Kopnova, O., Shaporeva, A., Abildinova, G., Nurbekova, Z., Almagambetova, L., Gorokhov, A., & Aitymov, Z. (2024). Ontology modeling for automation of questionnaire data processing. *Eastern-European Journal of Enterprise Technologies*, 5(2-131), 36-52. doi: 10.15587/1729-4061.2024.314129.
- [25] Interim Measures for the Management of Generative Artificial Intelligence Services. (2023, July). Retrieved from <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2023-08-07%20ITOW%20Interim%20Measures%20for%20the%20Management%20of%20Generative%20Artificial%20Intelligence%20Services.pdf>.
- [26] Judgment of the District Court of Michigan in Case No. 2:21-cv-10827 “Williams v. City of Detroit, Michigan, A Municipal Corporation”. (2021, April). Retrieved from <https://www.courtlistener.com/docket/59815822/williams-v-city-of-detroit-michigan-a-municipal-corporation/>.
- [27] Judgment of the UK Court of Appeal in Case No. C1/2019/2670 “R v. the Chief Constable of South Wales Police”. (2020, August). Retrieved from <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf>.
- [28] Kabir, S., & Alam, M.N. (2023). *IoT, big data and AI applications in the law enforcement and legal system: A review*. *International Research Journal of Engineering and Technology*, 10(5), 1777-1789.

- [29] Kenawy, F. (2025). *Smart policing revolution: How Kazakhstan is setting a global benchmark*. Retrieved from <https://sapsavvy.com/smart-policing-revolution-how-kazakhstan-is-setting-a-global-benchmark-2/>.
- [30] Khan, Z.A., & Rizvi, A. (2021). *AI based facial recognition technology and criminal justice: Issues and challenges*. *Turkish Journal of Computer and Mathematics Education*, 12(14), 3384-3392.
- [31] Kheira, B. (2024). Predictive policing and enhancing security performance through artificial intelligence applications. *Turkish Academic Research Review*, 9(4), 444-454. doi: 10.30622/tarr.1464788.
- [32] Kovalchuk, O., Banakh, S., Chudyk, N., & Drakokhrust, T. (2024). Machine learning models for judicial information support. *Law, Policy and Security*, 2(1), 33-45. doi: 10.62566/lps/1.2024.33.
- [33] Law of the Republic of Kazakhstan No. 94-V "On Personal Data and their Protection". (2013, May). Retrieved from <https://adilet.zan.kz/eng/docs/Z1300000094>.
- [34] Lyndyuk, A., Havrylyuk, I., Tomashevskii, Y., Khirivskiy, R., & Kohut, M. (2024). The impact of artificial intelligence on marketing communications: New business opportunities and challenges. *Economics of Development*, 23(4), 60-71. doi: 10.57111/econ/4.2024.60.
- [35] Moy, L.M. (2021). *A taxonomy of police technology's racial inequity problems*. *University of Illinois Law Review*, 2021(1), 139-193.
- [36] Opinion of the Supreme Court of State of Illinois No. 123186 in Case "Stacy Rosenbach, as Mother and Next Friend of Alexander Rosenbach, Appellant, v. SIX Flags Entertainment Corporation et al., Appellees". (2019, January). Retrieved from <https://law.justia.com/cases/illinois/supreme-court/2019/123186.html>.
- [37] Opinion of the Supreme Court of State of Wisconsin in Case No. 2015AP157-CR "State of Wisconsin, Plaintiff-Respondent, v. L. Loomis, Defendant-Appellant". (2016, July). Retrieved from <https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html>.
- [38] PAI Staff. (2019). *Report on algorithmic risk assessment tools in the U.S. criminal justice system*. Retrieved from <https://partnershiponai.org/paper/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system/>.
- [39] Patra, J. (2024). Cyber laws and emerging use of artificial intelligence: View from sociological perspectives. *Electronic Journal of Veterinary Medicine*, 25(1), 1308-1312. doi: 10.69980/redvet.v25i1.863.
- [40] Petrovskiy, A., Kyrdan, B., & Kutsyk, K. (2025). Implementation of artificial intelligence in civil proceedings: Experience of EU countries. *Scientific Journal of the National Academy of Internal Affairs*, 30(1), 45-59. doi: 10.56215/naia-herald/1.2025.45.
- [41] Pisani, A. (2021). *Artificial intelligence in China: The development of social credit system and its use in the "war of people" against Covid-19*. Venice: Ca' Foscari University.
- [42] Poirson, C. (2021). The legal regulation of facial recognition. In K. Miller & K. Wendt (Eds.), *The Fourth Industrial Revolution and its impact on ethics: Solving the challenges of the agenda 2030* (pp. 283-302). Cham: Springer. doi: 10.1007/978-3-030-57020-0_21.
- [43] Pokhariyal, P., Patel, A., & Pandey, S. (2024). *AI and emerging technologies: Automated decision-making, digital forensics, and ethical considerations*. Boca Raton: CRC Press. doi: 10.1201/9781003501152.
- [44] Regulation of the European Parliament and of the Council No. 2016/679 "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive No. 95/46/EC (General Data Protection Regulation)". (2016, April). Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.
- [45] Regulation of the European Parliament and of the Council No. 2024/1689 "Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)". (2024, June). Retrieved from <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.
- [46] Resolution of the Government of the Republic of Kazakhstan No. 592 "On Approval of the Concept of Development of Artificial Intelligence for 2024-2029". (2024, July). <https://adilet.zan.kz/rus/docs/P2400000592>.
- [47] Saparbekova, E.K., Smanova, A.B., Makhambetsaliyev, D.B., Nessipbaeva, I.S., & Nussipova, L.B. (2024). Comparative analysis of the concept of constitutional judicial law-making in the United States of America and Kazakhstan. *International Journal for the Semiotics of Law*, 38(2), 603-617. doi: 10.1007/s11196-024-10138-y.
- [48] Singh, T. (2023). AI-driven surveillance technologies and human rights: Balancing security and privacy. In A.K. Somani, A. Mundra, R.K. Gupta, S. Bhattacharya & A.P. Mazumdar (Eds.), *Proceedings of SSIC 2023: Smart systems: Innovations in computing* (pp. 703-717). Singapore: Springer. doi: 10.1007/978-981-97-3690-4_53.
- [49] Stensland, V.J. (2023). *A data-driven problem: Exploring predictive policing with random forest crime mapping in Oslo*. Oslo: University of Oslo.
- [50] Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and Society*, 40(2), 137-157. doi: 10.1080/14494035.2021.1928377.
- [51] Universal Declaration of Human Rights. (1948, December). Retrieved from <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.
- [52] Wang, M. (2019). *Facial recognition deal in Kyrgyzstan poses risks to rights: Use of same tech in Xinjiang should serve as warning*. Retrieved from <https://surl.lu/bwobuw>.
- [53] Wiek, K. (2023). *The Artificial Intelligence Act – the impact of AI on human rights standards in European law enforcement*. Enschede: University of Twente.
- [54] Xia, L., Semirumi, D.T., & Rezaei, R. (2023). A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society*, 98, article number 104771. doi: 10.1016/j.scs.2023.104771.
- [55] Yanyshivskiy, M. (2024). Regulation of artificial intelligence in Ukraine in the framework of harmonisation of legislation with EU legal norms. *Democratic Governance*, 17(1), 53-62. doi: 10.23939/dg2024.53.

- [56] Zaroff, A. (2022). *AI-based automated decision making: An investigative study on how it impacts the rule of law and the case for regulatory safeguards*. Lund: Lund University.
- [57] Zeng, D., Cao, Z., & Neill, D.B. (2021). Artificial intelligence-enabled public health surveillance – from local detection to global epidemic monitoring and control. In L. Xing, M.L. Giger & J.K. Min (Eds.), *Artificial intelligence in medicine: Technical basis and clinical applications* (pp. 437-453). London: Academic Press. doi: 10.1016/B978-0-12-821259-2.00022-3.
- [58] Zeng, J. (2022). *Artificial intelligence with Chinese characteristics: National strategy, security and authoritarian governance*. Singapore: Palgrave Macmillan. doi: 10.1007/978-981-19-0722-7.
- [59] Zhekshe kyzy, A., & Shambetov, T. (2023). “Akylduu” cameras: Has Bishkek adopted the Kremlin’s methods? Retrieved from <https://www.azattyk.org/a/akylduu-kameralar-bishkek-kremlin-ykmasyna-oettuebue-/32459225.html>.

Правові проблеми регулювання штучного інтелекту у правоохоронній діяльності з урахуванням міждисциплінарного підходу до соціально-правових трансформацій

Рауан Жалтирбаєва

Старший викладач

Актюбінський обласний університет ім. К. Жубанова

030000, просп. А. Молдагулова, 34, м. Актюбе, Республіка Казахстан

<https://orcid.org/0009-0009-1394-0863>

Арайлим Джангабулова

Кандидат юридичних наук, доцент

Казахський національний університет імені аль-Фарабі

050040, просп. аль-Фарабі, 71, м. Алмати, Республіка Казахстан

<https://orcid.org/0000-0002-4150-5393>

Сауле Сулейменова

Доктор юридичних наук, професор

Казахський національний університет імені аль-Фарабі

050040, просп. аль-Фарабі, 71, м. Алмати, Республіка Казахстан

<https://orcid.org/0000-0002-6754-9255>

Шолпан Саїмова

Кандидат юридичних наук

«Інститут парламентаризму» Департаменту матеріально-технічного забезпечення

010000, просп. Мангілік Ел, 8, м. Астана, Республіка Казахстан

<https://orcid.org/0000-0002-9000-6136>

Жанна Тлембаєва

Кандидат юридичних наук, професор

Астанський медичний університет

010000, вул. Бейбітшілік, 49А, м. Астана, Республіка Казахстан

<https://orcid.org/0000-0003-4088-1087>

Анотація. У цьому дослідженні розглядалися правові проблеми, пов'язані з регулюванням штучного інтелекту (ШІ) в правоохоронних органах, враховуючи його ширші соціально-правові трансформації. Використовуючи міждисциплінарний підхід, у дослідженні було проведено порівняльний правовий аналіз нормативно-правових актів штучного інтелекту в різних юрисдикціях, оцінка законодавчої бази, судових рішень і політичних ініціатив. Дослідження виявило ключові нормативні прогалини, зокрема відсутність чітких законодавчих визначень, проблеми підзвітності в поліцейській діяльності, керовані ШІ, і ризик упередженості алгоритмів. Завдяки порівняльному аналізу різних юрисдикцій виявлено значні відмінності в управлінні ШІ. Європейський Союз приймає запобіжний і нормативний підхід, класифікуючи правоохоронний штучний інтелект як високоризиковий і встановлюючи суворі вимоги дотримання. Сполучені Штати покладаються на децентралізоване управління, де ініціативи на державному рівні та судовий нагляд формують розгортання штучного інтелекту, що призводить до непослідовного правозастосування. Китай надає пріоритет державному контролю, швидко інтегруючи спостереження за штучним інтелектом у правоохоронні органи без незалежного

нагляду, що викликає занепокоєння щодо належного процесу та захисту прав людини. Навпаки, нові юрисдикції, такі як Казахстан і Киргизстан, знаходяться на ранніх стадіях регулювання штучного інтелекту, впроваджуючи поліцейські технології на основі ШІ, покладаючись на загальні правові положення. Дослідження показало, що інтеграція ШІ в правоохоронні органи створює як можливості, так і ризики. Хоча штучний інтелект підвищує ефективність поліцейської діяльності та розподіл ресурсів, він також посилює системні упередження, порушує конфіденційність даних і кидає виклик традиційним структурам підзвітності. Відсутність регуляторної гармонізації ще більше ускладнює транскордонне співробітництво в галузі штучного інтелекту та визначення відповідальності. Ці висновки підкреслили необхідність більш чіткої правової бази, міжнародної координації та етичного управління штучним інтелектом, щоб збалансувати імперативи безпеки та фундаментальні права. Враховуючи швидкі темпи впровадження штучного інтелекту, майбутні дослідження повинні зосередитися на емпіричних оцінках реального впливу штучного інтелекту на правові системи, громадську довіру та прозорість правоохоронних органів, гарантуючи, що регуляторні підходи залишатимуться адаптивними та справедливими.

Ключові слова: алгоритмічна підзвітність; біометричне спостереження; захист даних; автоматизоване прийняття рішень; цифрові права; громадська довіра