JGSP
Jurnal Greenation Sosial dan Politik
+62 81210467572 https://greenationpublisher.org/JGSP greenation.info@gmail.com
GREENATION PUBLISHER

DOI: https://doi.org/10.38035/jgsp.v3i3

Artificial Intelligence in Predictive Policing: A Systematic Literature Review and Its Implications for Indonesia

Radyan Kunto Wibisono[1], Joko Setiono[2], Ilham Prisgunanto[3]
[1]Sekolah Tinggi Ilmu Kepolisian, Indonesia, raccoonz.1946@gmail.com
[2]Sekolah Tinggi Ilmu Kepolisian, Indonesia, joko_setiono@ymail.com
[3]Sekolah Tinggi Ilmu Kepolisian, Indonesia, prisgunanto@gmail.com

Corresponding Author: raccoonz.1946@gmail.com[1]

Abstract: The use of Artificial Intelligence (AI) in predictive policing is rapidly developing globally as a response to demands for effectiveness and efficiency in law enforcement. Although this technology promises predictive capabilities that can assist the police in identifying potential crimes in the future, its implementation raises complex legal and ethical issues, especially in the context of a rule-of-law country like Indonesia. This article presents a systematic review of academic literature related to AI in predictive policing over recent years sourced from Scopus, Web of Science, and Google Scholar. The study results indicate that although predictive policing has the potential to reduce crime rates, this technology is fraught with risks of algorithmic discrimination, data bias, privacy violations, and unclear legal accountability. A juridical analysis of existing regulations in Indonesia, such as Law No. 27 of 2022 on Personal Data Protection and the Electronic Information and Transactions Law (UU ITE), shows the absence of legal norms that specifically regulate the application of AI in the context of criminal law. Furthermore, the use of algorithmic prediction results as a basis for legal action potentially contradicts fundamental principles in criminal procedural law, such as the presumption of innocence and the right to personal data protection. This study recommends the urgency of establishing a national legal framework capable of ensuring the ethical, fair, and accountable application of AI technology in law enforcement sectors. Adaptive and human rights-based regulations are necessary so that AI can be used responsibly without sacrificing the values of justice and democracy.

Keywords: *Artificial Intelligence*, Predictive Policing, Criminal Law, Personal Data Protection, Algorithmic Discrimination.

Abstrak: Penggunaan Kecerdasan Buatan (AI) dalam penegakan hukum prediktif berkembang pesat secara global sebagai respons terhadap tuntutan efektivitas dan efisiensi dalam penegakan hukum. Meskipun teknologi ini menjanjikan kemampuan prediktif yang dapat membantu polisi mengidentifikasi kejahatan potensial di masa depan, implementasinya menimbulkan isu hukum dan etika yang kompleks, terutama dalam konteks negara berlandaskan hukum seperti Indonesia. Artikel ini menyajikan tinjauan sistematis terhadap literatur akademik terkait AI dalam kepolisian prediktif selama beberapa tahun terakhir yang bersumber dari Scopus, Web

of Science, dan Google Scholar. Hasil studi menunjukkan bahwa meskipun kepolisian prediktif berpotensi mengurangi tingkat kejahatan, teknologi ini dipenuhi dengan risiko diskriminasi algoritmik, bias data, pelanggaran privasi, dan ketidakjelasan pertanggungjawaban hukum. Analisis yuridis terhadap peraturan yang ada di Indonesia, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE), menunjukkan ketidakhadiran norma hukum yang secara khusus mengatur penerapan AI dalam konteks hukum pidana. Selain itu, penggunaan hasil prediksi algoritmik sebagai dasar tindakan hukum berpotensi bertentangan dengan prinsip-prinsip dasar dalam hukum acara pidana, seperti asas praduga tak bersalah dan hak atas perlindungan data pribadi. Studi ini merekomendasikan urgensi pembentukan kerangka hukum nasional yang mampu memastikan penerapan teknologi AI secara etis, adil, dan akuntabel di sektor penegakan hukum. Regulasi yang adaptif dan berbasis hak asasi manusia diperlukan agar AI dapat digunakan secara bertanggung jawab tanpa mengorbankan nilai-nilai keadilan dan demokrasi.

Kata Kunci: Kecerdasan Buatan, prediksi kepolisian, hukum pidana, perlindungan data pribadi, diskriminasi algoritmik.

INTRODUCTION

The phenomenon of using Artificial Intelligence (AI) in predictive policing has become a global spotlight over the past decade (Windani, 2023). In various countries, police forces have begun to rely on algorithmic systems to predict the location and timing of potential crimes based on historical data (Alikhademi, 2022). This step aims to increase the efficiency of law enforcement while minimizing crimes before they actually occur. However, the integration of AI in police practices has raised concerns regarding algorithmic bias, privacy violations, and limitations in technological transparency (Setiawan, 2024). This situation raises major questions about how the law can respond appropriately and proportionately to such innovation.

Indonesia, as a state based on the rule of law, certainly cannot turn a blind eye to developments in global law enforcement technology (Sulistyawan, 2019). The increasingly complex and technology-based nature of crime challenges law enforcement to seek more adaptive and precise methods (Wahyudi, 2025). AI in predictive policing offers potential to map crime-prone areas or identify hidden crime patterns within big data (Muhammad Wali, 2023). However, this advanced technology cannot be applied just like that without being adjusted to the principles and norms of national law. The need for effectiveness in law enforcement must remain in line with respect for human rights and the principles of justice (Husna, 2023).

The main challenge lies in how the law can accommodate the use of AI without sacrificing fundamental values in the criminal justice system (Septiawan, 2024). Predictive policing is not just about technology, but about how data is used to shape decisions that have a direct impact on citizens' freedom (Berk, 2021). If algorithms are used without adequate oversight, there is a risk that individuals may be suspected or profiled purely based on statistical tendencies, not concrete evidence. This opens up the potential for violations of the presumption of innocence and the principle of non-discrimination. Therefore, attention to the ethical and legal aspects of predictive policing is crucial in the context of Indonesia.

In a legal context, Artificial Intelligence can be understood as a technological system capable of making decisions or taking actions that resemble human intelligence, based on complex data processing (Kushariyadi, 2024). Global regulations such as the OECD Principles on AI and the European Union Artificial Intelligence Act have provided more standardized definitions of AI, including criteria for transparency, accountability, and safety (Laksito, 2024).

In Indonesia, although there is not yet a specific regulation regarding AI, the 2020–2045 National Artificial Intelligence Strategy document has provided an initial framework for the responsible development and use of AI (Komarudin, 2024). This shows an awareness at the policy level that AI requires a serious and structured legal approach, including when AI is used in a law enforcement context such as predictive policing.

The types of AI used in predictive policing generally include machine learning and natural language processing. These technologies allow systems to learn patterns in crime data, identify relationships between variables, and generate predictions about potential criminal incidents (Sudirwo, 2025). In practice, such systems can be tailored to recognize geographic crime patterns (crime mapping), criminal behavior analysis, and even social interactions on digital media. However, the use of AI in law enforcement requires strict validation to ensure predictive results do not lead to discriminatory decisions. This is a major concern because AI systems learn from historical data and can replicate structural biases in society (Andriyani, 2025).

Predictive policing is conceptually rooted in the theory of data-driven policing, which emphasizes the use of data as the basis for law enforcement policy. This approach developed through the application of crime mapping technology that enables visualization of crime-prone areas based on past incidents. Subsequently, predictive algorithms are used to estimate crimes that may occur within a certain time frame and location (Lee, 2024). The PredPol system developed in the United States became one of the earliest popular examples, although it later drew criticism for reinforcing racial and social bias (Slobogin, 2023). Besides PredPol, there are also HunchLab and ShotSpotter which combine spatial, temporal, and audio analysis in identifying potential criminality (Zakaria, 2023).

Predictive policing models do offer efficiency, but they must be understood within the socio-legal context of each country. In countries with legal systems that still face issues of transparency, accountability, and human rights protection like Indonesia, the adoption of such technology needs to be strictly monitored. Without clear regulation, predictive policing can become a tool of power that endangers civilians, particularly vulnerable groups. This context emphasizes that the formation of a legal framework cannot merely follow technological logic, but must be adjusted to social realities and values of justice. The success of predictive policing is not only about the accuracy of prediction but also how fair and lawful its use is (Sandhu, 2021).

The progressive legal theory developed by Satjipto Rahardjo is highly relevant in addressing the legal challenges of AI use. This theory emphasizes that the law must not be rigid and left behind by the times, but must be able to provide real protection for society in ever-changing social conditions. In the context of predictive policing, the law must be able to limit the abuse of technology without hindering legitimate innovation (Hartanto, 2024). This perspective encourages that the regulatory approach to AI should be dynamic, participatory, and humane, not merely procedural and formalistic.

The theory of human rights protection in the criminal justice system also provides an important framework for assessing the acceptability of predictive policing. The right to privacy, individual freedom, and fair treatment must be guaranteed, even under the most advanced technology use. It is not enough for the technology to merely meet technical or functional requirements it must also be normatively tested against human rights standards. Predictive policing must be assessed not only for its effectiveness but also for whether it respects human dignity and ensures procedural justice. This approach forces policymakers and legal practitioners to be more critical of the narrative of technological efficiency (Strikwerda, 2021).

The theory of legality and due process of law is another fundamental basis for assessing the legality of predictive policing. All actions by law enforcement officers must have a clear legal basis and be carried out according to lawful procedures. If AI is used to justify arrests,

surveillance, or interventions against individuals without an explicit legal framework, then such actions risk violating the principle of legality. Likewise, algorithmic systems that cannot be explained (non-explainable AI) are in conflict with due process principles because individuals have no access to the reasons behind the legal actions taken against them. This situation shows that the law must regulate not only what technology may do, but also how the technology is operated and monitored.

The connection between legal theory and the development of AI in predictive policing reflects the importance of a legal approach that is not separated from social and technological contexts. Regulations to be implemented in the future must consider the dynamics of the relationship between security needs and the protection of citizens' rights. AI as a tool in the criminal justice system is not a neutral entity, as it carries values, assumptions, and inherent risks. Therefore, knowledge of legal theory must serve as the foundation for understanding and regulating technology, not merely following technological progress blindly. The placement of AI within the Indonesian legal framework must begin with deep reflection on the constitutional values that form the foundation of our legal system.

METHOD

This research uses a normative juridical method with a systematic approach to relevant scientific literature in order to examine the legal aspects of using Artificial Intelligence (AI) in predictive policing practices. The normative juridical approach was chosen because the primary focus of the study lies in analyzing the applicable positive legal norms as well as the evolving legal principles, both nationally and internationally, in relation to AI technology in the law enforcement sector. The primary data in this research consists of Indonesian legislation such as Law Number 27 of 2022 on Personal Data Protection, Law Number 11 of 2008 on Electronic Information and Transactions and its amendments, as well as the Criminal Procedure Code (KUHAP). Meanwhile, secondary data were collected through a systematic review of scientific literature from databases such as Scopus, Web of Science, and Google Scholar, with a publication time range of the past few years. The literature analyzed includes academic journals discussing predictive policing from legal, human rights, and technological perspectives. The search was conducted using keywords such as "AI in predictive policing," "algorithmic discrimination," "legal implications of artificial intelligence," and "human rights and AI in law enforcement." Inclusion criteria were strictly set to only include peer-reviewed literature that substantially discusses the impact or practice of AI use in the context of law enforcement. The analysis was conducted by examining the relationship between the legal theories used and the existing practices and regulations, to assess the compatibility and legal gaps that need to be addressed through national legal policy reform.

RESULT AND DISCUSSION

Systematic Literature Review on AI in Predictive Policing

The systematic literature review in this study was conducted to gain a comprehensive understanding of how AI is applied in predictive policing practices across various jurisdictions. The literature used is sourced from reputable academic databases such as Scopus, Web of Science, and Google Scholar, with a publication time range of the past few years. The main focus is on articles discussing the legal, ethical, and technical aspects of AI-based predictive policing. This review only includes literature that discusses the actual use or evaluation of predictive systems in the context of law enforcement, and which contains normative discussions or analyses of their impact on society. Descriptive literature without critical analysis or that is not directly related to the criminal justice system was excluded from this review.

Literature selection was carried out through a search process using keywords such as "predictive policing," "AI in law enforcement," "algorithmic bias," and "legal implications of AI." This was followed by filtering based on abstracts and relevance to legal and human rights focus. Other inclusion criteria were peer-reviewed publications, in English or Indonesian, and containing significant discussion on the social or legal impact of the technology. Meanwhile, publications in the form of personal opinions without clear supporting data, popular news articles, or blog posts were not used as main references. This step was taken to ensure that this review is based on sources with high academic validity and can be scientifically accounted for. The following is a list of the main literature used in the systematic review on the use of Artificial Intelligence (AI) in predictive policing, especially in the context of law and ethics:

1) "Artificial Intelligence & Crime Prediction: A Systematic Literature Review"
   Author: Fatima Dakalbab, Manar Abu Talib, Omnia Abu Waraga, Ali Bou Nassif, Sohail Abbas, Qassim Nasir, Jurnal: *Social Sciences & Humanities Open*, Volume 6, Issue 1, 2022, Artikel No. 100342. DOI: 10.1016/j.ssaho.2022.100342
   This article is a systematic review of 120 publications between 2008 and 2021, focusing on AI approaches in crime prediction. The analysis covers 34 types of crime studied, as well as the technical and ethical approaches used in these studies.
2) "Recommendation Paper: Artificial Intelligence and Predictive Policing: Risks and Challenges"
   Publisher: *European Crime Prevention Network (EUCPN)*, 2022
   Link:https://eucpn.org/document/recommendation-paper-artificial-intelligence-and-predictive-policing-risks-and-challenges
   This paper explains the technology behind predictive policing computer programs and provides an overview of the opportunities and risks of applying AI in this context.
3) "Artificial Intelligence in Criminal Justice Management: A Systematic Literature Review"
   Authors: Khairul Alam Talukder, Touhida Ferdousi Shompa, Jurnal: *Journal of Machine Learning, Data Engineering and Data Science*, Volume 1, Issue 1, 2023, DOI: 10.70008/jmldeds.v1i01.42
   This study explores the role of AI in criminal justice management, with a focus on applications in predictive policing, judicial risk assessment, and surveillance, as well as associated ethical and regulatory challenges.
4) "Runaway Feedback Loops in Predictive Policing"
   Authors: Danielle Ensign, Sorelle A. Friedler, Scott Neville, Carlos Scheidegger, Suresh Venkatasubramanian
   Platform: *arXiv*, 2017
   Link: https://arxiv.org/abs/1706.09847
   This paper develops a mathematical model to explain why predictive policing systems are prone to excessive feedback loops, where police are repeatedly deployed to the same neighborhoods regardless of the actual crime rate.

The main findings from the literature show that predictive policing has the potential to reduce crime rates in several major cities around the world. Systems like PredPol and HunchLab can help officers allocate resources more efficiently, focusing on areas or times predicted to have high crime rates. In some studies, a statistically recorded decline in crime was observed, although the results often depend on the type of crime being monitored. This effectiveness becomes the main argument for technology advocates to promote its broader adoption. Nevertheless, this effectiveness is not unconditional and needs to be critically examined from a legal and justice perspective.

The risk of algorithmic discrimination and data bias emerges as a key issue repeatedly highlighted across nearly all literature. AI systems process historical data, and if that data contains racial, social, or economic biases, the algorithm will reinforce those biases in the

resulting predictions. For instance, if a particular community has historically been disproportionately surveilled or targeted by law enforcement, AI systems will identify that area as a crime-prone zone, even if this is not supported by current realities. This leads to minority or low-income communities being vulnerable to excessive surveillance. Such discrimination not only violates the principle of equality but also undermines public trust in legal institutions.

Transparency and accountability are two essential principles in the design and implementation of AI systems for predictive policing. Many scholarly sources emphasize that algorithms used must be auditable and explainable to the public and oversight authorities. Lack of clarity about how the algorithms function prevents the public from raising objections or defending themselves if harmed by AI-based decisions. The presence of a "black box" in AI systems can obscure accountability, as law enforcement officers or technology developers may shift blame when errors occur. The principle of transparency in legal systems demands openness in processes, including the technologies used to support law enforcement.

Individual privacy becomes one of the main issues in criticisms of predictive policing. AI relies on large volumes of data, including personal information collected from various sources such as CCTV footage, social media, criminal records, and even individual mobility patterns. Without clear legal boundaries, the use of such data may violate citizens' privacy rights. Some studies even show a trend of increasing surveillance on certain communities without valid legal grounds. This issue becomes more serious when individuals are neither notified nor give consent that their data is being processed for predictive purposes that may result in law enforcement intervention.

The issue of over-policing is also highlighted in the literature reviewed. Predictive policing often results in concentrated surveillance in areas marked by algorithms as "high crime zones" without considering complex social contexts. As a result, communities living in these areas become subjects of intensive inspection and enforcement, even though not all members are involved in criminal activity. This approach can create an unjust cycle of surveillance and instill fear within communities. The long-term effects can include social alienation and damaged relationships between citizens and law enforcement.

Many studies criticize predictive policing for often being incompatible with the principle of non-discrimination as guaranteed by international law and the constitutions of many countries, including Indonesia. When algorithms identify individuals or groups based on patterns formed from discriminatory historical data, the resulting predictions also carry structural prejudice. The law must ensure that the treatment of citizens is equal and based on evidence, not statistical predictions. The presence of AI in this domain complicates efforts to achieve substantive justice, as technology is often perceived as neutral when it is not. This poses a challenge for regulators to ensure that the use of AI does not lead to human rights violations.

The principles of fairness and explainability are vital foundations required in every use of AI in legal contexts. Fairness demands that the system does not create hidden injustices behind the algorithms, while explainability requires that the system can be described in a way understandable to humans. Without these principles, system users and affected individuals cannot evaluate whether decisions are fair and lawful. Some studies propose that explainability should be the minimum requirement for AI systems used in legal processes. This approach allows for democratic control over technology and strengthens public trust.

This literature review shows that while AI in predictive policing promises technical effectiveness, the accompanying legal and ethical challenges are far more complex and profound. Legal literacy and awareness of the social impact of technology are key to building systems that are not only smart but also fair. The global academic discourse is moving toward the understanding that the success of predictive policing must be evaluated not only based on predictive accuracy but also on the system's alignment with values of justice, human rights,

and the rule of law. The integration of AI in law enforcement in Indonesia needs to be based on a deep understanding of international experiences and constitutional principles. Scientific literature serves as an important initial foundation in drafting regulations that both protect the public and adapt to technological advances.

Legal Analysis of the Implications of AI Use in Predictive Policing in Indonesia

Regulations governing artificial intelligence and digital technologies in Indonesia have not fully responded to the dynamics of AI use in the context of law enforcement. Law No. 27 of 2022 on Personal Data Protection is a major legal milestone that establishes the rights of data subjects and the obligations of data controllers, but it does not specifically regulate the use of data in predictive policing. Article 20 of the PDP Law regulates the principles of transparency and accountability in personal data processing, while Article 35 prohibits data processing that results in discriminatory impacts on individuals. This becomes a challenge because predictive algorithms work by analyzing historical data, which is not always free from bias. The implementation of technology that does not consider the principle of non-discrimination as stipulated in Article 3 of the PDP Law may result in violations of citizens' rights.

Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016, provides a legal basis regarding electronic information and systems used in public services and law enforcement. Article 40A paragraph (2) affirms the state's obligation to protect digital spaces from misuse that disrupts public order, including the potential misuse of AI for profiling citizens. However, the ITE Law does not explicitly regulate the boundaries of AI use in criminal legal processes, especially during investigation and suspect determination phases. This ambiguity opens wide interpretative space and may lead to the use of technology in ways that contradict the principle of due process of law. The absence of firm norms also makes it difficult for both authorities and the public to evaluate the legitimacy of predictive system use.

Ministerial Regulation of the Ministry of Administrative and Bureaucratic Reform (Permen PANRB) No. 3 of 2023, which amends Ministerial Regulation No. 25 of 2020 on the Bureaucratic Reform Roadmap 2020–2024, encourages digital transformation in government, including the use of smart technologies. However, in the context of predictive policing, this roadmap does not specifically address the need for the integration of ethics and human rights standards into digital law enforcement systems. This regulation focuses more on bureaucratic efficiency and inter-agency data integration, without regulating mechanisms for controlling data misuse. When technology is used in law enforcement without adequate normative oversight, the potential for abuse of power increases significantly. This administrative regulation cannot serve as a sufficient legal basis to guarantee the protection of citizens' constitutional rights.

Indonesia's National Artificial Intelligence Strategy 2020–2045, issued by BPPT, outlines AI development plans including in the public security sector. This document mentions the need for the development of security systems based on data and AI, but lacks binding legal safeguards. There is no elaboration on accountability of AI-using institutions, public involvement in oversight, or complaint mechanisms when AI systems cause harm. In the context of predictive policing, this is problematic because technology may be used to make decisions affecting a person's civil liberties. Without a strong legal foundation, the implementation of technology in law enforcement risks violating the principle of legality and proportionality in criminal law.

The Indonesian Criminal Procedure Code (KUHAP) does not explicitly regulate the use of digital technology during investigation stages. Although Article 184 of KUHAP mentions valid evidence such as witness testimony, expert statements, documents, indications,

and defendant statements, AI-based predictive systems do not yet fall within these categories. The lack of classification creates legal uncertainty when AI analysis results are used as the basis for police actions such as intensive patrols, inspections, or even arrests. Indonesian criminal procedure still relies on the principle of legal proof, while AI systems operate based on probabilities and statistical correlations. This opens up debate regarding the validity of legal actions taken solely on algorithmic predictions.

The use of data in crime prediction systems raises issues regarding the source, legality, and context of data collection. In many cases, the data used by algorithms comes from historical police records, including crime location, type, and demographic characteristics of offenders. If such data is not obtained through lawful procedures, its use violates the principle of chain of custody as applied in criminal law practice. Moreover, using data that reflects past racial or social bias can result in systemic discrimination. From a legal perspective, data-driven actions that are unverifiable and cannot be judicially tested pose a high risk of violating the right to a fair trial.

The absence of specific regulations regarding predictive policing results in the technology being used without clear accountability mechanisms. In a legal system that emphasizes legal certainty, every exercise of state power must be grounded in written norms. Predictive policing still operates in a legal gray area, making it prone to misuse for purposes other than legitimate law enforcement. The lack of laws or government regulations that set boundaries, evaluation methods, and oversight institutions allows this practice to exceed the authority granted by law-to-law enforcement officials. A state governed by law cannot allow technological tools to reduce fundamental rights without adequate legal safeguards.

The presumption of innocence, as guaranteed in Article 8 paragraph (1) of Law No. 39 of 1999 on Human Rights, requires that everyone be presumed innocent until a final and binding court verdict declares otherwise. Predictive policing potentially violates this principle by imposing special treatment on individuals or communities simply because they live in areas deemed crime-prone by algorithms. Although preventive action is part of policing strategies, excessive restriction of freedom or surveillance of individuals who have not committed any crime results in violations of fundamental criminal law principles. A clear distinction must be made between preventive measures based on legitimate intelligence and actions based purely on statistical assumptions. This risk of generalization also creates unfair social stigma for affected communities.

The validity of evidence generated by AI algorithms raises serious questions in criminal judicial processes. The justice system demands proof based on facts, not unverifiable statistical assumptions. When decisions by law enforcement rely on algorithmic analyses that cannot be explained in detail (black box systems), the defendant's right to a fair defense is threatened. The principle of *audi alteram partem* in criminal procedure law requires that each party have the opportunity to understand and respond to the evidence used against them. The lack of clarity in how AI systems operate makes it difficult for courts to determine the reliability of such evidence and may violate the right to a fair trial.

Privacy as a constitutional right is guaranteed in Article 28G paragraph (1) of the 1945 Constitution and Article 14 of the Human Rights Law. When predictive policing uses personal data without the subject’s consent, it constitutes a violation of the right to control personal information. This right becomes even more crucial when the data comes from sources unknown to the public, such as CCTV recordings, phone location tracking, or metadata from social media. The PDP Law stipulates that personal data processing must be based on explicit and revocable consent, yet no mechanisms currently exist that regulate exceptions in the law enforcement context in detail. Without clear norms, law enforcement can invoke public security as a reason to disregard citizens' fundamental rights.

Legal accountability in the use of predictive policing technology has not been clearly distributed among system providers, algorithm developers, and on-the-ground technology users. In practice, system errors or faulty predictions often are not followed by adequate accountability mechanisms. In the context of administrative and state administrative law, there should be a grievance and compensation system for citizens harmed by law enforcement actions based on AI systems. However, the absence of substantive regulations and dedicated oversight institutions renders such administrative justice mechanisms ineffective. Justice cannot rely on unmonitored and opaque technology, for what is at stake is the dignity of the law and the public's trust in the state.

CONCLUSION

The use of artificial intelligence in predictive policing presents serious challenges to the legal system in Indonesia, particularly in the context of protecting human rights and ensuring legal certainty. Although there are some regulations concerning personal data and electronic systems, there is currently no legal norm that specifically governs the use of AI in the process of criminal law enforcement. This legal ambiguity creates opportunities for potential violations of the presumption of innocence principle, the inadmissibility of evidence, and infringements on citizens' privacy. Algorithm-based predictive systems, which are not always explainable or transparently testable, are at risk of being arbitrarily used by law enforcement officers without adequate accountability mechanisms. In a state governed by the rule of law that upholds the principle of due process, the implementation of advanced technologies should always be accompanied by binding regulations, independent oversight, and guarantees of the right to remedy in case of errors.

A comprehensive legal reform is needed to ensure that the utilization of AI technology in policing does not create an imbalance between the efficiency of law enforcement and the protection of citizens' rights. The establishment of a clear legal framework—including regulations on ethical standards, system evaluation methods, and legal responsibilities for both users and developers of the technology is an urgent necessity. The government must also encourage the involvement of civil society and academia in the policy-making process so that the use of AI is not solely focused on efficiency, but also ensures justice and transparency. Without a strong legal foundation and active public participation, technologies like predictive policing risk deepening social inequality and eroding the democratic values upheld by the constitution.

REFERENCES

Alikhademi, K. D. (2022). A review of predictive policing from the perspective of fairness. *Artificial Intelligence and Law*, 1-17.

Andriyani, W. W. (2025). *When Data Is Everywhere.* Banjarnegara: PT. Penerbit Qriset Indonesia.

Berk, R. A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology, 4(1)*, 209-237.

Hartanto, D. R. (2024). Legalitas dan Etika Penggunaan Artificial Intelligence Perspektif Hukum Progresif dan Tinjauan Hukum Internasional. *Prosiding Seminar Nasional Wijayakusuma National Conference, 5(1)*, 127-137.

Husna, S. K. (2023). Pancasila dan Hubungannya dengan Hak Asasi Manusia di Indonesia. *Civic Education: Media Kajian Pancasila dan Kewarganegaraan, 7(2)*, 104-112.

Komarudin, D. C. (2024). Dinamika Kebijakan Publik dan Inovasi Kecerdasan Buatan di Indonesia Tahun 2020-2024. *Arus Jurnal Sosial dan Humaniora, 4(3)*, 1793-1803.

Kushariyadi, K. A. (2024). *Artificial Intelligence: Dinamika Perkembangan AI Beserta Penerapannya.* Jambi: PT. Sonpedia Publishing Indonesia.

Laksito, J. P. (2024). Harmonizing Data Privacy Frameworks in Artificial Intelligence: Comparative Insights from Asia and Europe. *Perkara: Jurnal Ilmu Hukum dan Politik, 2(4)*, 579-588.

Lee, Y. B. (2024). The effectiveness of big data-driven predictive policing: systematic review. *Justice Evaluation Journal, 7(2)*, 127-160.

Muhammad Wali, S. T. (2023). *Penerapan & Implementasi Big Data di Berbagai Sektor (Pembangunan Berkelanjutan Era Industri 4.0 dan Society 5.0).* Jambi: PT. Sonpedia Publishing Indonesia.

Sandhu, A. &. (2021). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. *Policing and society, 31(1)*, 66-81.

Septiawan, R. A. (2024). Pemanfaatan Artificial Intelligence dalam Hukum Acara Pidana: Tinjauan Yuridis dan Dampak Sosial. *Perkara: Jurnal Ilmu Hukum dan Politik, 2(4)*, 640-654.

Setiawan, G. N. (2024). KAJIAN HUKUM TERHADAP PENGGUNAAN TEKNOLOGI ANALISIS SENTIMEN OLEH PIHAK KEPOLISIAN. *LEX PRIVATUM, 14(3)*.

Slobogin, C. (2023). Predictive Policing in the United States. *Vanderbilt Law Research Paper*(23-01).

Strikwerda, L. (2021). Predictive policing: The risks associated with risk assessment. *The Police Journal, 94(3)*, 422-436.

Sudirwo, S. H. (2025). *Artificial Intelligence: Teori, Konsep, dan Implementasi di Berbagai Bidang.* Jambi: PT. Sonpedia Publishing Indonesia.

Sulistyawan, A. Y. (2019). Urgensi harmonisasi hukum nasional terhadap perkembangan hukum global akibat globalisasi. *Jurnal Hukum Progresif, 7(2)*, 171-181.

Wahyudi, B. R. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *Innovative: Journal Of Social Science Research, 5(1)*, 3436-3450.

Windani, C. A. (2023). Strategi dan Tantangan Predictive Policing di Era Big Data bagi Masyarakat Modern. *Deviance Jurnal Kriminologi, 7(2)*, 101-120.

Zakaria, M. G. (2023). AI applications in the criminal justice system: the next logical step or violation of human rights. *Journal of Law and Emerging Technologies, 3(2)*, 233-257.