

Artificial Intelligence in Predictive Policing: Navigating the Tension between Law Enforcement Effectiveness and Human Rights Protection

Aghdinal Brilliant Andrew Mustafa

Centre for Psychological Research of Trisula Ungu Indonesia

Article Info

Article history:

Received February, 18, 2026

Revised March 15, 2026

Accepted April 02, 2026

Keywords:

artificial intelligence,
human rights,
predictive policing,
rule of law,
data protection

ABSTRACT

This study examines the conflict of norms arising from the use of Artificial Intelligence (AI) in predictive policing within the Indonesian legal system, where data-driven law enforcement aimed at enhancing efficiency and crime prevention simultaneously raises fundamental human rights concerns. Employing a normative legal method with statute, conceptual, and case approaches, this research analyzes key regulations on policing, electronic information, personal data protection, human rights, and criminal law. The findings identify three primary normative conflicts: first, predictive policing challenges the principle of due process of law by enabling preventive actions based on probabilistic assessments rather than actual criminal conduct; second, extensive data utilization in AI systems conflicts with the right to privacy, particularly regarding consent, purpose limitation, and accountability; and third, the assumption of algorithmic neutrality contradicts the principle of non-discrimination due to the risk of embedded bias in predictive systems. The study further reveals a regulatory gap in Indonesian law, as existing frameworks do not specifically govern AI-based law enforcement, thereby creating risks of abuse of power, systemic human rights violations, and declining public trust. Accordingly, this research argues for the establishment of a comprehensive legal framework that integrates human rights protection, algorithmic accountability, and transparency to ensure that technological innovation in law enforcement remains aligned with the rule of law and democratic principles.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Aghdinal Brilliant Andrew Mustafa

Centre for Psychological Research of Trisula Ungu Indonesia

Email: aghdinalbrilliant@gmail.com

1. INTRODUCTION

The rapid development of digital technology has significantly transformed contemporary law enforcement practices, particularly through the emergence of predictive policing based on Artificial Intelligence (AI). Predictive policing refers to the use of algorithmic systems to analyze

large-scale data in order to predict potential criminal activities, identify high-risk locations, and anticipate individuals who may be involved in future crimes. This model represents a shift from conventional reactive policing toward a proactive and data-driven approach aimed at increasing efficiency and effectiveness in crime prevention.¹

In comparative practices, predictive policing has been widely adopted in several jurisdictions, particularly in the United States through systems such as PredPol, which utilize historical crime data to forecast crime hotspots. The adoption of such technologies reflects an increasing reliance on algorithmic governance within criminal justice systems, where decision-making processes are partially delegated to automated systems.² However, while these systems promise efficiency, they also raise fundamental legal and ethical concerns, particularly regarding accountability, transparency, and the risk of algorithmic bias.³

In Indonesia, although predictive policing has not yet been explicitly regulated as a distinct legal framework, elements of data-driven policing have begun to emerge within institutional practices of the Indonesian National Police. This development operates within a fragmented regulatory environment, including Law Number 2 of 2002 on the Indonesian National Police, Law Number 11 of 2008 as amended by Law Number 19 of 2016 on Electronic Information and Transactions, Law Number 27 of 2022 on Personal Data Protection, Law Number 39 of 1999 on Human Rights, and Law Number 1 of 2023 on the new Criminal Code. These regulations, however, were not designed specifically to govern AI-based predictive policing, resulting in normative inconsistencies and regulatory gaps.⁴

The central legal issue addressed in this study is a conflict of norms between the need for effective, technology-based law enforcement and the obligation to protect fundamental human rights. This conflict manifests in several critical dimensions. First, predictive policing enables preventive actions based on probabilistic assessments rather than actual criminal conduct, thereby challenging the principle of due process of law. Second, the reliance on large-scale data processing raises concerns regarding the protection of personal data and the right to privacy. Third, algorithmic systems risk reproducing or amplifying discriminatory patterns embedded in historical data, potentially violating the principle of non-discrimination.⁵

This normative conflict reflects a broader tension between the security approach and the human rights approach in modern legal systems. On the one hand, the state is obligated to maintain public order and security through effective law enforcement mechanisms. On the other hand, it must ensure that such mechanisms do not infringe upon constitutionally protected rights. In the absence of a clear and comprehensive legal framework governing predictive policing, there is a significant risk of abuse of power, systemic rights violations, and erosion of public trust in law enforcement institutions.⁶

Previous studies have examined predictive policing from various perspectives but reveal a clear research gap. Moses and Chan (2016) in “Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability” focus on the technical and accountability challenges of algorithmic systems without adequately addressing normative conflicts in non-Western legal systems. Lynskey (2019) in “Criminal Justice Profiling and EU Data Protection Law” emphasizes data protection issues within the European Union context but does not explore broader human rights conflicts beyond privacy. Wibisono, Setiono, and Prisgunanto (2025) in “Artificial Intelligence in Predictive

¹ George-Marius Țical, “Artificial Intelligence and Big Data Analysis in Crime Prevention and Combat,” *Annals of the Academy of Romanian Scientists Series on Military Sciences* (2025).

² Sarah Brayne and Angèle Christin, “Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts,” *Social Problems* 68, no. 3 (2020): 608–624

³ Lyria Bennett Moses and Janet Chan, “Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability,” *Policing and Society* 28 (2016): 806–822

⁴ Radian Kunto Wibisono, Joko Setiono, and Ilham Prisgunanto, “Artificial Intelligence in Predictive Policing: A Systematic Literature Review and Its Implications for Indonesia,” *Jurnal Greenation Sosial dan Politik* (2025).

⁵ Ashrafur Rahman Nabil et al., “Ethical Implications of AI-Powered Predictive Policing: Balancing Public Safety with Privacy Concerns,” *Innovatech Engineering Journal* (2025).

⁶ Riska Kurnia Ningsih and Hadi Tuasikal, “Critical Review of Police Performance in Upholding Law Enforcement and Human Rights in Indonesia,” *Jurnal USM Law Review* (2025).

Policing: A Systematic Literature Review and Its Implications for Indonesia” identify the potential of AI in Indonesia but do not provide a prescriptive normative framework to resolve conflicts of norms.

Accordingly, this study aims to fill this gap by providing a normative legal analysis that not only identifies conflicts of norms but also formulates prescriptive solutions to harmonize technological innovation with human rights protection within the Indonesian legal system.

2. METHOD

This study employs a normative legal research method, which focuses on the analysis of legal norms, principles, and doctrines relevant to the regulation of predictive policing within the Indonesian legal system. Normative legal research is particularly appropriate for examining conflicts of norms, identifying legal inconsistencies, and formulating prescriptive legal solutions.⁷ The research is analytical and prescriptive in nature, aiming not only to describe existing legal conditions but also to propose normative frameworks for resolving identified legal issues.

The statute approach is utilized to examine relevant Indonesian legislation governing law enforcement, data protection, and human rights. The primary legal instruments analyzed include Law Number 2 of 2002 on the Indonesian National Police, Law Number 11 of 2008 as amended by Law Number 19 of 2016 on Electronic Information and Transactions, Law Number 27 of 2022 on Personal Data Protection, Law Number 39 of 1999 on Human Rights, and Law Number 1 of 2023 on the new Criminal Code. These statutes are analyzed to identify normative inconsistencies and limitations in addressing AI-based policing practices.⁸

The conceptual approach is employed to analyze relevant legal doctrines and theoretical frameworks, including the concept of the rule of law (*rechtstaat*), the principle of due process of law, human rights protection theories, and the emerging concept of algorithmic governance. This approach enables a deeper understanding of how predictive policing challenges traditional legal principles, particularly in relation to procedural justice, accountability, and non-discrimination.⁹

The case approach is conducted by examining comparative practices of predictive policing in other jurisdictions, particularly the United States, where systems such as PredPol have been implemented. This approach provides insights into the practical implications, risks, and regulatory responses associated with predictive policing, which are then used to assess its potential application in Indonesia.¹⁰

The legal materials used in this study consist of primary and secondary sources. Primary legal materials include statutory regulations and legal instruments, while secondary materials consist of academic journal articles, legal doctrines, and scholarly analyses on AI governance, predictive policing, and human rights law. These materials are systematically analyzed to construct a coherent normative argument regarding the regulation of predictive policing in Indonesia.

3. RESULTS AND DISCUSSION

Conflict of Norms between Predictive Policing Effectiveness and the Principle of Due Process of Law

The implementation of predictive policing based on Artificial Intelligence represents a paradigm shift in law enforcement from reactive to preemptive approaches. In this model, law enforcement authorities utilize algorithmic systems to identify potential criminal activities before

⁷ Soerjono Soekanto, *Pengantar Penelitian Hukum* (Jakarta: UI Press, 2008).

⁸ Raden Saputra, Joko Setiodjati, and Janine Barkhuizen, “Under-Legislation in Electronic Trials and Renewing Criminal Law Enforcement in Indonesia (Comparison with United States),” *Journal of Indonesian Legal Studies* (2023).

⁹ Olivia Lynskey, “Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing,” *International Journal of Law in Context* 15 (2019): 162–176

¹⁰ Patricia Haley and Darrell Norman Burrell, “Integrating Artificial Intelligence into Law Enforcement: Socioeconomic and Ethical Challenges,” *SocioEconomic Challenges* (2025).

they occur. From the perspective of effectiveness, this approach offers significant advantages, including resource optimization, targeted surveillance, and early intervention. However, from a normative legal standpoint, predictive policing raises fundamental concerns regarding its compatibility with the principle of due process of law.

The principle of due process of law requires that any legal action taken by the state must be based on clear legal grounds, including the existence of an unlawful act (*actus reus*) and culpability (*mens rea*). This principle is closely linked to the legality principle enshrined in Law Number 1 of 2023 on the Indonesian Criminal Code, which affirms that no one can be punished without a prior legal provision and without fault. Predictive policing, however, operates on probabilistic reasoning, where individuals or locations are identified as “high risk” based on data patterns rather than concrete criminal acts. This creates a normative tension between predictive intervention and legal certainty.¹¹

The conflict of norms becomes more evident when predictive policing is used as a basis for preventive measures such as surveillance, profiling, or intervention. These actions may be taken without sufficient evidence of actual wrongdoing, thereby potentially violating procedural justice and presumption of innocence. In such cases, law enforcement actions risk shifting from evidence-based enforcement to suspicion-based governance, which lacks a solid normative foundation in Indonesian criminal law.¹²

Although Law Number 2 of 2002 on the Indonesian National Police grants discretionary powers to police officers, such discretion is not absolute. It must be exercised within the limits of law, proportionality, and respect for human rights. The use of predictive policing without clear legal parameters may lead to excessive discretion, opening the possibility of abuse of power. This is particularly problematic in the absence of specific regulations governing the use of AI in law enforcement.¹³

From a conceptual perspective, predictive policing challenges the traditional framework of criminal liability, which is grounded in individual responsibility and factual conduct. By relying on predictive analytics, law enforcement may justify interventions based on statistical likelihood rather than proven acts. This creates a risk of “pre-crime” enforcement, where individuals are treated as potential offenders without committing any offense. Such a shift undermines the fundamental principles of criminal law and procedural fairness.¹⁴

The implications of this conflict are significant. First, it threatens legal certainty, as individuals may be subjected to law enforcement actions without clear legal justification. Second, it risks undermining public trust in law enforcement institutions, particularly if predictive systems are perceived as arbitrary or opaque. Third, it creates a potential for systemic abuse, especially in contexts where oversight mechanisms are weak.

Normatively, this condition indicates the need for clear legal limitations on the use of predictive policing. Such limitations should include strict criteria for intervention, transparency in algorithmic decision-making, and judicial oversight mechanisms. Without these safeguards, predictive policing remains incompatible with the principle of due process of law and the broader framework of the rule of law..

Conflict of Norms between Data Utilization in AI Systems and the Right to Privacy

Predictive policing fundamentally depends on the collection, processing, and analysis of large-scale data, commonly referred to as big data. This includes not only criminal records but also social data, behavioral patterns, geospatial information, and, in some cases, personal digital

¹¹ Lyria Bennett Moses and Janet Chan, “Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability,” *Policing and Society* 28 (2016): 806–822

¹² Arman Tjoneng, “Legal Education, Justice, and Certainty: An Analysis of Suspect Determination by the Indonesian Police,” *Journal Corner of Education, Linguistics, and Literature* (2025).

¹³ Riska Kurnia Ningsih and Hadi Tuasikal, “Critical Review of Police Performance in Upholding Law Enforcement and Human Rights in Indonesia,” *Jurnal USM Law Review* (2025)

¹⁴ Shivani Saxena, “Predictive Policing and Ethical Implications in Forensic Science,” *Journal of Advances in Science and Technology* (2025).

footprints. While such data utilization enhances the analytical capacity of law enforcement, it simultaneously raises serious concerns regarding the protection of individual privacy rights.

The conflict of norms arises between the state's obligation to ensure public security and its duty to respect and protect individual privacy. Law Number 27 of 2022 on Personal Data Protection establishes key principles, including consent, purpose limitation, data minimization, and accountability. These principles require that personal data be processed lawfully, transparently, and for specific purposes. However, in predictive policing practices, data is often aggregated from multiple sources without explicit consent, leading to potential violations of these principles.¹⁵

Moreover, predictive policing systems frequently involve the expansion of data usage beyond its original purpose, a phenomenon known as function creep. Data collected for administrative or commercial purposes may be repurposed for law enforcement without adequate legal basis. This practice directly contradicts the principle of purpose limitation and undermines the integrity of data protection frameworks.¹⁶

Law Number 39 of 1999 on Human Rights explicitly guarantees the right to privacy and protection against arbitrary interference. The use of predictive policing technologies, particularly those involving mass data collection and surveillance, risks infringing upon these rights. In extreme cases, it may lead to mass surveillance practices, where individuals are continuously monitored without reasonable suspicion. Such practices are incompatible with democratic principles and the protection of civil liberties.¹⁷

The absence of a comprehensive regulatory framework governing AI in law enforcement exacerbates these risks. While the Personal Data Protection Law provides general safeguards, it does not specifically address the complexities of algorithmic data processing in predictive policing. This creates a regulatory gap, where law enforcement agencies may operate without clear limitations or accountability mechanisms.¹⁸

To illustrate the normative conflict, the following table presents a comparison between the principles of data protection and the practices of predictive policing:

Table 1. Normative Conflict between Personal Data Protection Principles and Predictive Policing Practices

Legal Principle (PDP Law 2022)	Normative Requirement	Predictive Policing Practice	Legal Implication
Consent	Data must be processed with explicit consent	Data often collected without direct consent	Violation of data subject rights
Purpose Limitation	Data used only for specified purposes	Data repurposed for policing (function creep)	Unlawful data processing
Data Minimization	Only necessary data should be collected	Extensive data aggregation (big data)	Excessive data collection
Accountability	Clear responsibility for data processing	Lack of transparency in algorithmic systems	Weak legal accountability

The implications of this conflict are profound. First, it creates a risk of systemic human rights violations, particularly in the form of unauthorized surveillance and data misuse. Second, it undermines public trust in digital governance and law enforcement institutions. Third, it exposes individuals to potential harm, including profiling, stigmatization, and misuse of personal data.

¹⁵ Benedicta Ehimuan et al., "Global Data Privacy Laws: A Critical Review of Technology's Impact on User Rights," *World Journal of Advanced Research and Reviews* (2024)

¹⁶ Olivia Lynskey, "Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing," *International Journal of Law in Context* 15 (2019): 162–176

¹⁷ D. Almeida, Konstantin Shmarko, and Elizabeth Lomas, "The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence," *AI and Ethics* 2 (2021): 377–387

¹⁸ Gunawan Nurmansyah, Raden Natamiharja, and Iwan Setiawan, "Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach," *Pancasila and Law Review* (2025).

Normatively, addressing this conflict requires the establishment of specific legal safeguards for the use of AI in law enforcement. These include strict limitations on data collection, mandatory consent mechanisms where applicable, independent oversight, and robust accountability frameworks. Additionally, the principle of “privacy by design” should be integrated into predictive policing systems to ensure that data protection is embedded within technological architectures.

Conflict of Norms between Algorithmic Neutrality and the Principle of Non-Discrimination

The use of Artificial Intelligence in predictive policing is often justified on the basis of its perceived neutrality and objectivity. Algorithmic systems are commonly viewed as capable of producing unbiased decisions because they rely on data-driven analysis rather than subjective human judgment. However, this assumption is fundamentally problematic from a normative legal perspective. In reality, algorithmic systems are not inherently neutral; they are shaped by the data on which they are trained, the design choices of developers, and the institutional contexts in which they operate.

The conflict of norms arises between the claim of technological neutrality and the principle of non-discrimination as guaranteed under human rights law. Law Number 39 of 1999 on Human Rights explicitly prohibits all forms of discrimination, whether direct or indirect. This includes discrimination based on race, ethnicity, religion, social status, or other protected characteristics. Predictive policing systems, however, have been shown to reproduce and even amplify existing social biases embedded in historical data.¹⁹

Algorithmic bias occurs when the data used to train AI systems reflects historical inequalities or discriminatory practices. For example, if law enforcement data disproportionately targets certain communities, predictive systems will likely identify those communities as higher risk, thereby reinforcing patterns of over-policing. This creates a feedback loop in which marginalized groups are continuously subjected to increased surveillance and intervention.²⁰

From a legal standpoint, such outcomes constitute a form of indirect discrimination. Unlike direct discrimination, which involves explicit unequal treatment, indirect discrimination occurs when seemingly neutral policies or practices result in disproportionate adverse effects on certain groups. Predictive policing falls within this category because the algorithm itself does not explicitly target specific groups, yet its outputs may systematically disadvantage them.²¹

The absence of regulatory standards for algorithmic accountability in Indonesia further exacerbates this issue. There are currently no legal requirements for algorithmic auditing, transparency, or explainability in law enforcement technologies. As a result, individuals affected by predictive policing decisions have limited ability to challenge or even understand the basis of those decisions. This lack of transparency undermines procedural justice and violates the principle of equality before the law.²²

Moreover, the delegation of decision-making authority to algorithmic systems raises questions about responsibility and liability. When discriminatory outcomes occur, it becomes unclear whether responsibility lies with the developers, the data providers, or the law enforcement agencies using the system. This diffusion of responsibility creates significant challenges for legal accountability and remedies.

The implications of this conflict are substantial. First, it risks institutionalizing discrimination within the criminal justice system, thereby undermining the legitimacy of law enforcement. Second, it may lead to violations of fundamental rights, including the right to equality

¹⁹ Sarah Brayne and Angèle Christin, “Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts,” *Social Problems* 68, no. 3 (2020): 608–624

²⁰ Lyria Bennett Moses and Janet Chan, “Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability,” *Policing and Society* 28 (2016): 806–822

²¹ Ashrafur Rahman Nabil et al., “Ethical Implications of AI-Powered Predictive Policing: Balancing Public Safety with Privacy Concerns,” *Innovatech Engineering Journal* (2025).

²² Patricia Haley and Darrell Norman Burrell, “Integrating Artificial Intelligence into Law Enforcement: Socioeconomic and Ethical Challenges,” *SocioEconomic Challenges* (2025).

and fair treatment. Third, it creates barriers to legal redress, as affected individuals may lack access to the information necessary to challenge algorithmic decisions.

Normatively, resolving this conflict requires the development of a legal framework that ensures algorithmic accountability. This includes mandatory bias testing, regular algorithmic audits, transparency requirements, and the right to explanation for individuals affected by automated decisions. Additionally, the principle of non-discrimination must be explicitly integrated into the design and implementation of AI systems in law enforcement. Without such measures, predictive policing remains incompatible with the fundamental principles of human rights law.

4. CONCLUSION

The integration of Artificial Intelligence into predictive policing introduces a complex conflict of norms within the Indonesian legal system, particularly between the pursuit of effective law enforcement and the obligation to uphold fundamental human rights. This study identifies three primary dimensions of normative conflict.

First, there is a conflict between preventive law enforcement measures enabled by predictive policing and the principle of due process of law. The use of probabilistic predictions as a basis for intervention challenges the foundational requirements of *actus reus* and *mens rea*, thereby undermining legal certainty and procedural justice.

Second, there is a conflict between extensive data utilization in AI systems and the right to privacy. The reliance on large-scale data processing, often without explicit consent, contradicts the principles of personal data protection and risks enabling mass surveillance practices that infringe upon civil liberties.

Third, there is a conflict between the perceived neutrality of algorithmic systems and the principle of non-discrimination. Algorithmic bias embedded in predictive policing systems may result in indirect discrimination, reinforcing existing social inequalities and undermining the legitimacy of law enforcement institutions.

The analysis demonstrates that the current Indonesian legal framework is not adequately equipped to regulate predictive policing in a comprehensive and coherent manner. Existing laws, including those governing policing, electronic information, personal data protection, human rights, and criminal law, operate in a fragmented manner and do not specifically address the complexities of AI-based law enforcement.

In the absence of clear regulatory standards, the use of predictive policing poses significant risks, including abuse of power, systemic human rights violations, and erosion of public trust. Therefore, it is imperative to develop a normative legal framework that balances technological innovation with the protection of fundamental rights. Such a framework must ensure that the deployment of AI in law enforcement remains consistent with the principles of the rule of law, human rights, and democratic governance.

REFERENCES

Journal/Periodicals

- Almeida, D., Shmarko, K., & Lomas, E. (2021). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *Ai and Ethics*, 2, 377 - 387. <https://doi.org/10.1007/s43681-021-00077-w>.
- Brayne, S., & Christin, A. (2020). Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts.. *Social problems*, 68 3, 608-624 . <https://doi.org/10.1093/socpro/spaa004>.
- Ehimuan, B., Chimezie, O., , O., Akagha, O., Reis, O., & Oguejiofor, B. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*. <https://doi.org/10.30574/wjarr.2024.21.2.0369>.
- Haley, P., & Burrell, D. (2025). Integrating Artificial Intelligence into Law Enforcement:

- Socioeconomic and Ethical Challenges. SocioEconomic Challenges. [https://doi.org/10.61093/sec.9\(2\).60-77.2025](https://doi.org/10.61093/sec.9(2).60-77.2025).
- Lynskey, O. (2019). Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15, 162 - 176. <https://doi.org/10.1017/s1744552319000090>.
- Moses, L., & Chan, J. (2016). Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing and Society*, 28, 806 - 822. <https://doi.org/10.1080/10439463.2016.1253695>.
- Nabil, A., Tusher, M., Akther, M., & Rayhan, R. (2025). Ethical Implications Of Ai- Powered Predictive Policing: Balancing Public Safety With Privacy Concerns. *Innovatech Engineering Journal*. <https://doi.org/10.70937/itej.v2i01.54>.
- Natamiharja, R., Sabatira, F., Banjarani, D., Davey, O., & Setiawan, I. (2022). Balancing Two Conflicting Perspectives on Wiretapping Act: Rights to Privacy and Law Enforcement. *Al-Risalah: Forum Kajian Hukum dan Sosial Kemasyarakatan*. <https://doi.org/10.30631/alrisalah.v22i1.1226>.
- Ningsih, R., & Tuasikal, H. (2025). Critical Review of Police Performance in Upholding Law Enforcement and Human Rights in Indonesia. *JURNAL USM LAW REVIEW*. <https://doi.org/10.26623/julr.v8i1.11757>.
- Nurmansyah, G., Natamiharja, R., & Setiawan, I. (2025). Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach. *Pancasila and Law Review*. <https://doi.org/10.25041/plr.v6i1.4138>.
- Pambudi, P., & Fakrulloh, Z. (2025). Criminal Liability of Perpetrators in Crypto Ecosystem, the Regulatory Challenges, and Legal Voids in the Criminal Law System in Indonesia. *Majelis: Jurnal Hukum Indonesia*. <https://doi.org/10.62383/majelis.v2i3.1042>.
- Santoso, J., Setiono, J., & Gani, Y. (2025). Optimization of Smart Policing and Democratic Policing Concepts as Polri's Efforts in Building Synergy with the Community to Realize Inclusive and Just Security Governance. *Jurnal Greenation Sosial dan Politik*. <https://doi.org/10.38035/jgsp.v3i3.429>.
- Saputra, C., Setiono, J., & Indarto, I. (2025). The Urgency of Reformulating Digital Policing Regulations Within the Framework of E-Polmas and Police 5.0 to Address the Legal Vacuum Regarding the Use of Artificial Intelligence in the Field of Public Order and Security. *Greenation International Journal of Law and Social Sciences*. <https://doi.org/10.38035/gijlss.v3i2.488>.
- Saputra, R., Setiodjati, J., & Barkhuizen, J. (2023). Under-Legislation in Electronic Trials and Renewing Criminal Law Enforcement in Indonesia (Comparison with United States). *Journal of Indonesian Legal Studies*. <https://doi.org/10.15294/jils.v8i1.67632>.
- Saxena, S. (2025). Predictive Policing and Ethical Implications in Forensic Science. *Journal of Advances in Science and Technology*. <https://doi.org/10.29070/6104qh22>.
- Soekanto, Soerjono. 2008. *Pengantar Penelitian Hukum*. Jakarta: Universitas Indonesia (UI Press)
- Țical, G. (2025). ARTIFICIAL INTELLIGENCE AND BIG DATA ANALYSIS IN CRIME PREVENTION AND COMBAT. *Annals of the Academy of Romanian Scientists Series on Military Sciences*. <https://doi.org/10.56082/annalsarscimilit.2025.1.36>.
- Tjoneng, A. (2025). Legal Education, Justice, and Certainty: An Analysis of Suspect Determination by the Indonesian Police. *Journal Corner of Education, Linguistics, and Literature*. <https://doi.org/10.54012/jcell.v5i001.639>.
- Wibisono, R., Setiono, J., & Prisgunanto, I. (2025). Artificial Intelligence in Predictive Policing: A Systematic Literature Review and Its Implications for Indonesia. *Jurnal Greenation Sosial dan Politik*. <https://doi.org/10.38035/jgsp.v3i3.441>.
- Wijayanti, A., Anggraeni, D., Adriantini, D., Dewi, S., Hakim, H., Kurniaty, Y., & Setiawati, D. (2025). Bridging Technology and Justice: The Role of AI in Law Enforcement through Pancasila's Ideals. *E3S Web of Conferences*. <https://doi.org/10.1051/e3sconf/202562204003>.

Statute

Republic of Indonesia. Law Number 1 of 2023 on the Criminal Code (Kitab Undang-Undang Hukum Pidana).

Republic of Indonesia. Law Number 2 of 2002 on the Indonesian National Police.

Republic of Indonesia. Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016.

Republic of Indonesia. Law Number 27 of 2022 on Personal Data Protection.

Republic of Indonesia. Law Number 39 of 1999 on Human Rights.

Republic of Indonesia. The 1945 Constitution of the Republic of Indonesia..