Journal of Strafvordering:
https://nawalaeducation.com/index.php/JOSI/index
Jurnal Hukum Pidana Vol.2 No.3, July 2025
E-ISSN : 3046-8620
DOI : https://doi.org/10.62872/y6p4jb16

Preventive Criminal Regulation on the Risk of Crime by Artificial Intelligence in Indonesia

Hendri Khuan
Universitas Borobudur Indonesia
e-mail: wulandjari86@gmai.com*

Entered	:June 12, 2025	Revised	: July 05, 2025
Accepted	: July 16, 2025	Published	: July 22, 2025

ABSTRACT

The rapid development of Artificial Intelligence (AI) technology has presented new legal challenges, especially in the realm of criminal law in Indonesia. AI systems that are capable of acting autonomously create the potential for digital crime that cannot be reached by conventional criminal law structures that are oriented towards human offenders. The Criminal Code and Law No. 19 of 2016 concerning Information and Electronic Transactions are still human-centric and have not anticipated crimes mediated by non-human entities. This study uses normative juridical methods to evaluate the normative gaps in criminal regulation against AI-based crimes and offers a risk-based preventive criminal regulation model. This approach emphasizes the importance of a legal system that is adaptive to the design and implementation of AI from the early stages, by adopting the principles of risk-based regulation and precautionary principles. The regulations formulated must not only ensure legal accountability for potential violations, but also uphold ethical and human rights values. The recommendations include the need to redefine legal subjects, strengthen institutional capacity, and establish new laws on AI. Thus, risk-based criminal law reform is a juridical urgency in building a national legal system that is responsive to the threat of autonomous technology in the digital era.

Keywords: Artificial Intelligence; Cybercrime; Preventive Criminal Regulation.

INTRODUCTION

The rapid development of Artificial Intelligence (AI) technology has had a major impact on various dimensions of social, economic, and legal life. AI is now not just a supporting device, but has become an autonomous system that is able to perform actions based on machine *learning* algorithms. According to the *Global AI Index 2023*, global investment in AI has exceeded USD 100 billion, showing that this technology is becoming the backbone of the digital industrial revolution. Behind this acceleration, there are criminal threats that originate from or mediated by AI, such as deepfake fraud, botnet attacks, and the crime of information manipulation through digital media. This phenomenon poses a serious challenge to Indonesia's criminal law system, which does not yet have normative instruments that are adaptive to these new risks.

The national criminal law system is still based on classical principles that have not anticipated the evolution of intelligent digital technology. The Criminal Code as a basis for criminalization does not recognize non-human entities such as AI as perpetrators who

can be held legally accountable. The same thing can also be seen in Law Number 19 of 2016 concerning Information and Electronic Transactions, which does not adequately regulate crimes mediated by autonomous devices. This normative lag creates a legal *vacuum* that provides opportunities for criminals to hide behind layers of intelligent technology that are untouched by conventional criminal accountability systems.[1]

The problem becomes more complicated when AI is used as a tool or even an actor who makes decisions independently in a criminal act. The theory of liability in criminal law requires the existence of intentionality (mens rea) and real action (actus reus) by conscious and responsible humans. AI, which can make decisions based on algorithmic processes without direct human involvement, makes it difficult to apply these principles.[2] Three conceptual approaches regarding the possibility of criminal liability by AI, namely perpetration-via-another, natural-probable-consequence liability, and direct liability model. These approaches open up an important discourse on the need to redefine the criminal liability structure in Indonesian law.

The criminal regulation model that has been applied so far emphasizes more on a repressive approach, namely the provision of sanctions after a crime occurs. However, the speed of AI development and the magnitude of the threat posed suggest that this kind of approach is no longer adequate. Therefore, a preventive criminal law system is needed with a focus on controlling potential dangers from the design, testing, to AI implementation stages. Preventive in this case does not only mean technical prevention, but early law enforcement based on a risk assessment of AI's destructive ability to undermine law and order and public protection.[3]

The preventive criminal law model should adopt the principle of risk-based regulation, where the main focus is to identify and classify the level of risk of each AI system.[4] The European Union, through its 2021 Artificial Intelligence Act proposal, has developed a risk categorization system into four levels: unacceptable risk, high risk, limited risk, and minimal risk. For example, the use of AI in biometric surveillance systems or judicial systems is considered to be high-risk and required to be subject to strict and transparent regulations. Indonesia needs to adopt a similar approach, in order to develop a criminal law basis that is able to anticipate crimes from digital entities with adaptive normative coverage.

In addition to the risk aspect, the formulation of preventive criminal laws against AI must take into account ethical values and human rights protection. AI has great potential in reproducing structural bias and systematic discrimination, especially if used by government institutions or law enforcement agencies without public oversight.[5] The UNESCO Recommendation on the Ethics of Artificial Intelligence affirms the

---

[1] Nuhi, M. H., Al Ghozi, L., Nazla, S., & Syakirah, D. (2024). Pembaharuan Hukum Penanganan Tindak Pidana Pemalsuan Identitas Akibat Penyalahgunaan Artificial Intelligence Di Indonesia. *Jurnal Batavia*, *1*(2), 80-88.

[2] Ruhtiani, M. (2025). HUKUM PIDANA DAN HAK CIPTA DI ERA KECERDASAN ARTIFISIAL: ANALISIS PERTANGGUNGJAWABAN DALAM HUKUM POSITIF DAN HUKUM ISLAM. *Jurnal Al-Wasith: Jurnal Studi Hukum Islam*, *10*(1), 62-79.

[3] Nasution, R. (2025). Optimizing The Role Of Artificial Intelligence Technology In The Prevention And Enforcement Of Criminal Law: An Indonesian Legal Perspective. *Jurnal Multidisiplin Sahombu*, *5*(02), 363-369.

[4] Ras, H., Pranadita, N., & Wiradirja, I. R. (2023). Potential technological interventions in transnational crime from the perspective of criminal law in Indonesia. *Russian Law Journal*, *11*(3), 11-16.

[5] Dharmayanti, Y. P., & Soponyono, E. Criminal Law Policy in Efforts to Combat Artificial Intelligence (AI) in Cyber Crime. *Jurnal Hukum Khaira Ummah*, *20*(2), 2255-2274.

importance of the principles of transparency, algorithmic fairness, and accountability in the entire life cycle of AI. Therefore, any preventive regulation must be able to guarantee that AI is not misused as an instrument of violation of citizens' rights.

The implementation of preventive criminal regulations also requires strengthening institutional capacity, both normatively and technically. Law enforcement officials, including investigators and prosecutors, need to be given a deep understanding of how AI systems work, such as the use of machine learning, natural language processing, and data-driven decision-making systems. Institutions such as BSSN, the Ministry of Communication and Information, and the police must be synergized in an integrated surveillance framework in order to be able to carry out early identification of dangerous AI systems. Without institutional capacity building, the regulations that are drafted will risk becoming purely normative without effectiveness in practical implementation.

In closing, the development of a preventive criminal regulation model against crime risk by AI must be a national priority within the framework of digital legal reform. The government and legislators need to design legal instruments that not only respond to crimes that have occurred, but also anticipate potential violations that can arise due to technological sophistication. The drafting of the Artificial Intelligence Bill which contains risk-based preventive criminal provisions, clarity on the limits of legal responsibility, and the protection of the integrity and privacy of citizens is a strategic step towards a modern, fair, and responsive legal system to the challenges of the times..

METHOD

This research uses a normative juridical method, which is legal research that focuses on the study of norms in laws and regulations and legal doctrines. This approach is used to analyze the adequacy of national criminal law, especially Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE), in anticipating the risk of crimes committed through or by Artificial Intelligence (AI) systems.

Normative research aims to examine and understand how the law should apply (das sollen), not how the law is practiced in empirical reality (das sein), so that the entire analysis process relies on primary and secondary legal materials that are textual and conceptual.[6]

As explained by Peter Mahmud Marzuki, normative legal research is a method that focuses on the study of legal materials as the main object of study, by interpreting and constructing applicable laws to answer certain legal issues.[7] According to Marzuki, this approach is prescriptive because it aims not only to describe the law, but also to provide normative arguments for the validity of a legal action or act in the legal system adopted.[8] Meanwhile, Soerjono Soekanto and Sri Mamudji stated that normative legal research includes research on legal principles, legal systematics, legal synchronization, legal history, and comparative law.[9] This research uses primary legal materials in the form of Law No. 19 of 2016, the Criminal Code, and other related regulations, as well as secondary legal materials in the form of scientific literature, journals, and international

[6] Novea Elysa Wardhani, Sepriano, and Reni Sinta Yani, *Metodologi Penelitian Bidang Hukum* (Jambi: PT. Sonpedia Publishing Indonesia., 2025).

[7] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Group, 2011).

[8] Mahlil Adriaman et al., *Pengantar Metode Penelitian Ilmu Hukum* (Padang: Yayasan Tri Edukasi Ilmiah, 2024).

[9] Rangga Suganda, "Metode Pendekatan Yuridis Dalam Memahami Sistem Penyelesaian Sengketa Ekonomi Syariah," *Jurnal Ilmiah Ekonomi Islam* 8, no. 3 (2022): 2859, https://doi.org/10.29040/jiei.v8i3.6485.

policy reports related to AI and criminal law. The analysis technique used is qualitative descriptive with an approach to interpretation and legal construction, to formulate a criminal regulation model that is preventive against AI-based crimes.

Through this method, the research aims to formulate normative bases and juridical solutions to overcome the legal vacuum in criminal regulation against autonomous technology entities in Indonesia.

DISCUSSION

1. Normative Gap in Indonesian Criminal Law on the Risk of Crime by Artificial Intelligence

The development of artificial intelligence (AI) technology has created new dynamics in the modern crime landscape. In Indonesia, the national criminal law system, especially as contained in the Criminal Code (KUHP) and Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE), does not yet have explicit and adequate arrangements in responding to crimes committed by intervention or through AI systems. This normative gap poses serious implications for the reach of criminal law in formulating accountability for unlawful acts committed substantially by non-human autonomous systems.[10]

Conceptually, the Indonesian Criminal Code is still rooted in the principles of actus reus and mens rea as subjective and objective prerequisites in punishment. In fact, AI-based crimes are often carried out by non-human entities that have no legal awareness, but are capable of executing actions automatically, predictively, and adaptively. In the current positive legal structure, there is no norm that recognizes AI as a legal entity that can be held criminally responsible, either directly or as an instrument of human actors[11]. This results in a legal vacuum when AI commits an act that can factually be categorized as a criminal act, but cannot be subject to normative criminal sanctions.

Furthermore, Law No. 19 of 2016 concerning ITE, although it has expanded the scope of criminal offenses in the digital realm, still assumes the perpetrator of the crime as a natural person or legal person (corporation). The norms in Articles 30 to 36 of the ITE Law, for example, only regulate illegal access, system disruption, and information manipulation, but do not specifically target criminal acts committed by AI systems capable of acting independently or semi-independently without direct human control.[12] The absence of this norm shows that criminal regulations in Indonesia are human-centric and incompatible with the development of machine agencies.

On the other hand, in the principles of modern criminal law, there is a shift towards a constructive approach to criminal accountability within the framework of strict liability, vicarious liability, and even the concept of algorithmic accountability. However, Indonesian criminal law has not adopted this approach, so it fails to reach the possibility of non-human actors playing a determinant role in the occurrence of criminal events. This raises a theoretical debate about whether it is necessary to create legal fiction to construct

[10] Hernawan, C. N. P., Antow, D. T., & Sendow, A. (2025). TINJAUAN HUKUM MENGENAI PENYALAHGUNAAN ARTIFICIAL INTELLIGENCE DALAM TINDAK PIDANA KEKERASAN SEKSUAL. *LEX PRIVATUM*, *15*(5).

[11] Febriyani, E., Syarief, E., & Seroja, T. D. (2024). Pemanfaatan Artificial Intelligence dalam Deteksi dan Pencegahan Tindak Pidana Pencucian Uang: Potensi dan Tantangan Hukum. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *13*(4), 877-898.

[12] Nirmala, A. Z., & Rahmania, N. (2025). Transformasi Bentuk Pelecehan Seksual Dalam Era Kecerdasan Buatan: Tinjauan Hukum Indonesia. *Unizar Law Review*, *8*(1), 77-90.

AI as a subject of criminal law or simply return responsibility to the developer, operator, or owner of the AI system.

From an interpretive point of view, the provisions of Articles 55 and 56 of the Criminal Code which regulate participation and assistance in criminal acts have not been effectively applied to technological entities. Since no legal subject can be held directly accountable for the actions of AI that is autonomous, the legal system will experience a normative collapse in response to crimes that originate from machine initiatives. This is where there is an urgency to construct new norms or reinterpret laws that are adaptive to digital reality.[13]

These regulatory limitations also reveal weaknesses in the techno-legal foresight aspect of lawmakers, who have not anticipated emerging threats in the digital space, including the use of AI for deepfakes, algorithm manipulation, automated cyberattacks, and large-scale data engineering.[14] These crimes have a high potential for disruption, and without a strong normative foundation, the criminal justice system will not be able to respond effectively and justly.[15]

Constructively, the formation of new criminal norms that are preventive and adaptive to AI is inevitable. This can be realized through soft law approaches, such as AI ethics guidelines and digital prudence principles, as well as through legislative revisions to the Criminal Code and the ITE Law to accommodate the reality that criminals are no longer limited to humans, but also algorithm-based intelligent systems. In the future, the recognition of AI as a quasi-subject of law in criminal law must begin to be considered, at least in the framework of indirect criminal liability.

Thus, the normative gap that occurs reflects the stagnation of national criminal law in reaching digital transformation. Without progressive legal reforms, the impunity space for crimes committed by or through AI will widen, threatening the principles of legality and justice in the Indonesian criminal justice system.

2. The Urgency of Formulating a Preventive Criminal Regulation Model on the Potential for AI Criminality

Digital transformation based on artificial intelligence (AI) has expanded the potential for non-traditional crime that no longer depends on the presence of humans as direct perpetrators. In the framework of classical criminal law, the dominant approach is repressive, namely responding to criminal events after they occur. However, for autonomous technologies such as AI, this approach is no longer adequate, due to the characteristics of AI that can act independently, evolve adaptively, and operate in cyberspace that is difficult for conventional law enforcement to reach.[16] Therefore, the need to formulate a preventive criminal regulation model is urgent as a legal response to the potential risk of crime by AI.

---

[13] Zuwanda, Z. S., Lubis, A. F., Solapari, N., Sakmaf, M. S., & Triyantoro, A. (2024). Ethical and Legal Analysis of Artificial Intelligence Systems in Law Enforcement with a Study of Potential Human Rights Violations in Indonesia. *The Easta Journal Law and Human Rights*, *2*(03), 176-185.

[14] Iwannudin, I., & Heriani, I. (2025). Legal Challenges in Regulating Artificial Intelligence Use in Criminal Justice Systems. *The Journal of Academic Science*, *2*(6), 1603-1611.

[15] Putri Mecca, A. S., Hidaya, W. A., & Tuasikal, H. (2025). PEMANFAATAN TEKNOLOGI KECERDASAN BUATAN (ARTIFICIAL INTELLIGENCE) DALAM SISTEM PERADILAN PIDANA DI INDONESIA. *Journal of Social & Technology/Jurnal Sosial dan Teknologi (SOSTECH)*, *5*(6).

[16] Caianiello, M. (2021). Dangerous liaisons. Potentialities and risks deriving from the interaction between artificial intelligence and preventive justice. *European Journal of Crime, Criminal Law and Criminal Justice*, *29*(1), 1-23.

The preventive regulatory model emphasizes a risk-based approach, which is a risk-based approach that is carried out before a violation of the law occurs. This principle demands the presence of a law that not only regulates the consequences, but also intervenes at the stages of design, development, and deployment of technology. This approach is in line with the precautionary principle, which is a key principle in high-tech regulation in many global legal regimes, including the EU Artificial Intelligence Act. This principle states that if a technological activity has the potential to have a serious impact on the public or human rights, then scientific ignorance should not be used as a basis for delaying preventive measures from the state.

The urgency of preventive regulation can also be seen from the aspect of human rights protection. AI has the potential to violate various rights, such as algorithmic discrimination, privacy violations, and non-transparent data-based profiling. Within the framework of a state of law that upholds human rights, preventive measures in the form of supervision and control of AI developers and users are the normative obligations of the state. This is because if AI systems are used for criminal purposes such as information manipulation, automated fraud, or even autonomous cyberattacks, not only do the criminal law fail to respond, but also the protection of basic rights is threatened.

Comparisons with international legal frameworks show that some jurisdictions have been more progressive in adopting preventive principles. The European Union, through the Artificial Intelligence Act, divides AI risks into unacceptable risk, high risk, limited risk, and minimal risk, each of which has different legal consequences. The high-risk category, for example, includes AI systems used in the health sector, penegakan hukum, dan pengelolaan infrastruktur kritis. In this category, ex-ante compliance and impact assessment are required before the system can be operated. This approach illustrates that preventive criminal law is no longer limited to the imposition of sanctions, but also involves regulation and monitoring before violations occur.[17]

Meanwhile, the UNESCO Recommendation on the Ethics of Artificial Intelligence also emphasizes the urgency of an ethical and preventive regulatory framework. UNESCO emphasizes the need for ethical impact assessments and transparency mechanisms to avoid the misuse of AI. In the recommendation, countries are asked to establish a supervisory system for AI technology that is not only based on conventional law enforcement, but also strengthens regulatory capacity across sectors and multidisciplinary. This indicates that future criminal law is required to be more proactive, evidence-based, risk-based, and based on human rights principles.

In the Indonesian context, there is no regulation that specifically regulates criminal liability for AI entities or products. Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE) and Law No. 19 of 2016 as its revision are still normative in general nature and have not reached the complexity of AI structures. This is where the urgency of formulating a preventive criminal model becomes important: the law is not enough to wait for a criminal event, but must be present in the form of a compliance framework, mandatory disclosure, and a risk-based AI audit system. This model can also be a licensing mechanism that requires ethical audits and digital security testing on a regular basis.

Theoretically, the strengthening of preventive criminal law can adopt the concept of compliance-based criminal law, where business actors and AI developers are obliged to establish an internal legal compliance system before marketing their products. If the

[17] Haley, P., & Burrell, D. N. (2025). Using Artificial Intelligence in Law Enforcement and Policing to Improve Public Health and Safety. *Law, Economics and Society*, *1*(1), p46-p46.

perpetrator does not comply with the preventive mechanism, then new criminal sanctions can be imposed. This approach expands on the concepts of strict liability and corporate criminal responsibility that were previously known in environmental criminal law. Thus, the formation of preventive criminal norms against AI is not only a change in the area of formulation, but also in the realm of criminal law epistemology itself.

This urgency leads to a demand to redesign the national criminal law structure that is able to reach technological innovation in an adaptive, anticipatory, and collaborative manner. Regulations should not be reactive to AI disruption, but should be designed with a techno-regulatory foresight approach, namely the ability to formulate criminal law norms that take into account the long-term impacts and future technological dynamics. Therefore, the formulation of a preventive criminal regulation model against potential criminality by AI in Indonesia is

a juridical, ethical, and functional necessity that must be immediately responded to by lawmakers.

3. Recommendations for Risk-Based Criminal Regulation Models for Strengthening the National Legal System

In the face of the escalation of the use of Artificial Intelligence (AI) technology that is increasingly widespread, Indonesia needs a criminal regulation model that is not only reactive to the legal consequences that have occurred, but is preventive and based on risk assessment. This model is designed based on the awareness that the potential dangers posed by AI are not only technological, but also have complex legal dimensions, so they require a risk governance approach to anticipate threats that may arise to human rights, national security, and legitimate public interests.

To build a legal system that is responsive to the development of AI, it is necessary to apply a risk classification of AI technologies used in various sectors. The classification includes the categories of low risk, high risk, and unacceptable risk, as developed by the European Union through the EU Artificial Intelligence Act. AI used in the public interest with minimal potential impact, such as spam filters, can be exempted from strict scrutiny. Meanwhile, the use of AI in law enforcement, public oversight, or administrative decision-making that affects the basic rights of citizens must be closely monitored through regulation. In fact, AI technologies that have the potential to be systemic discriminatory or threaten civil liberties should be legally banned.

Legal supervision of AI must be integrated into the Indonesian legal system through a combination of administrative and criminal approaches. Institutions such as Kominfo, BSSN, and personal data protection authorities must be mandated to conduct audits, certifications, and controls of AI systems before and during their use. In the event of negligence or intentionality that causes losses or violations of the law through AI, a criminal approach must be applied to provide a deterrent effect and affirm the legal accountability of perpetrators, both individuals and corporations, as a form of application of the law as a means of protecting the community.

Law No. 19 of 2016 concerning Information and Electronic Transactions needs to be revised to accommodate the expansion of regulations regarding criminal liability for actions carried out through AI systems. In the revision, it is important to include new norms that govern that parties that control, develop, or benefit from AI can be held liable for any losses or violations of the law that arise. The principles of strict liability and vicarious liability can be used to ensure accountability for violations of the law committed

by entities that do not have the capacity of will such as AI, but have a real impact on social life.[18]

This model also recommends the birth of new laws that specifically regulate risk-based criminal regulation of the use of AI. The law should include legal definitions of AI, risk classification, system and algorithm audit obligations, restrictions on the use of AI in sensitive public sectors, as well as procedural law provisions for the prosecution of crimes involving autonomous systems. The clarity of this norm is important so that industry players, state apparatus, and the general public have legal certainty in developing and using AI technology.

The reformulation of this model also demands a redefinition of legal subjects in the criminal system. When AI has achieved autonomy in decision-making, then it is not enough to simply impose legal responsibility on the end operator.[19] It is necessary to design a multi-layered accountability model that includes manufacturers, technology owners, and business entities that use AI as part of their operational systems. This is in line with the development of corporate criminal law that has been regulated in Perma No. 13 of 2016, which places legal entities as the subject of criminal acts.

In anticipating the impact of the use of AI, strengthening the criminal justice system is absolutely necessary. The capacity of law enforcement officials, both in terms of technology understanding, forensic digital skills, and the ability to analyze causal relationships in the actions of AI systems against their legal consequences, must be improved systemically. This aims to ensure that the national legal system is able to respond to the development of AI in a predictive and adaptive manner, not just waiting for violations to occur.[20]

Finally, the success of risk-based criminal regulation models relies heavily on the involvement of multisectors, including governments, academia, the tech industry, and civil society. This collaborative approach is important to ensure that the formulation of legal norms does not curb innovation, but still provides maximum protection for the public interest. Criminal law, in this case, must be a social engineering tool that is flexible to the changing times without losing its functional legitimacy as a guardian of justice and order.

CONCLUSION

The normative gap in Indonesian criminal law on the risk of crimes committed by Artificial Intelligence (AI) systems reflects the weak reach of the legal system to the dynamics of cybercrime based on autonomous technology. The Criminal Code and the ITE Law, which are still oriented towards human actors, have not been able to accommodate the complexity of unlawful acts committed by non-human entities such as AI. The absence of recognition of AI as a legal subject or instrument of criminal acts has created a legal vacuum that has the potential to give birth to a new space of impunity. When AI is able to act automatically, predictively, and adaptively without human intervention, then the principles of actus reus and mens rea that are the basis of

[18] Puannandini, D. A., Fabian, R., Firdaus, R. A. P., Mustopa, M. Z., & Herdiyana, I. (2025). Liabilitas Produk Ai Dalam Sistem Hukum Indonesia: Implikasi Bagi Pengembang, Pengguna, Dan Penyedia Layanan. *Iuris Studia: Jurnal Kajian Hukum*, *6*(1), 24-33.

[19] Zulfa, A. A. Pemanfaatan Data Pengguna Layanan Melalui Cookie Oleh Artificial Intelligence Ditinjau Dari Perspektif Hak Asasi Manusia. *Artificial Dalam Bidang Hukum Di Era Teknologi Informasi: Tantangan Dan Peluang*, 95.

[20] Kadir, Z. K. (2025). Meruntuhkan Pilar Keadilan: Apakah Sistem Peradilan Dapat Berfungsi Tanpa Standar Pembuktian?. *Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora*, *3*(2), 40-61.

classical punishment become irrelevant. Even though the ITE Law has reached the digital world, it is still human-centric and does not anticipate the potential of machine agencies. As a result, the legal system has stagnated in responding to technological transformations that have shifted the locus and modus delicti. The failure of the criminal system in establishing legal responsibility for crimes by AI shows the need for a more adaptive and risk-based regulatory paradigm shift. The provisions of the article on inclusion in the Criminal Code are also not sufficient to ensnare technology actors who do not have the legal will. As a result, if new norms are not established immediately, criminal law will experience dysfunction in dealing with AI crimes that continue to grow. The neglect of the development of AI in the formulation of criminal norms shows the weak foresight of lawmakers in anticipating future legal threats. Therefore, strengthening the criminal law system through new formulations that reach intelligent entities is an urgent need to ensure that the law continues to function as a protector of society in the digital era.

REFERENCES

Caianiello, M. (2021). Dangerous liaisons. Potentialities and risks deriving from the interaction between artificial intelligence and preventive justice. European Journal of Crime, Criminal Law and Criminal Justice, 29(1), 1-23.

Dharmayanti, Y. P., & Soponyono, E. Criminal Law Policy in Efforts to Combat Artificial Intelligence (AI) in Cyber Crime. Jurnal Hukum Khaira Ummah, 20(2), 2255-2274.

Febriyani, E., Syarief, E., & Seroja, T. D. (2024). Pemanfaatan Artificial Intelligence dalam Deteksi dan Pencegahan Tindak Pidana Pencucian Uang: Potensi dan Tantangan Hukum. Jurnal Magister Hukum Udayana (Udayana Master Law Journal), 13(4), 877-898.

Haley, P., & Burrell, D. N. (2025). Using Artificial Intelligence in Law Enforcement and Policing to Improve Public Health and Safety. Law, Economics and Society, 1(1), p46-p46.

Hernawan, C. N. P., Antow, D. T., & Sendow, A. (2025). TINJAUAN HUKUM MENGENAI PENYALAHGUNAAN ARTIFICIAL INTELLIGENCE DALAM TINDAK PIDANA KEKERASAN SEKSUAL. LEX PRIVATUM, 15(5).

Iwannudin, I., & Heriani, I. (2025). Legal Challenges in Regulating Artificial Intelligence Use in Criminal Justice Systems. The Journal of Academic Science, 2(6), 1603-1611.

Kadir, Z. K. (2025). Meruntuhkan Pilar Keadilan: Apakah Sistem Peradilan Dapat Berfungsi Tanpa Standar Pembuktian?. Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora, 3(2), 40-61..

Mahlil Adriaman et al., Pengantar Metode Penelitian Ilmu Hukum (Padang: Yayasan Tri Edukasi Ilmiah, 2024).

Nasution, R. (2025). Optimizing The Role Of Artificial Intelligence Technology In The Prevention And Enforcement Of Criminal Law: An Indonesian Legal Perspective. Jurnal Multidisiplin Sahombu, 5(02), 363-369.

Nirmala, A. Z., & Rahmania, N. (2025). Transformasi Bentuk Pelecehan Seksual Dalam Era Kecerdasan Buatan: Tinjauan Hukum Indonesia. Unizar Law Review, 8(1), 77-90.

Novea Elysa Wardhani, Sepriano, and Reni Sinta Yani, Metodologi Penelitian Bidang Hukum (Jambi: PT. Sonpedia Publishing Indonesia., 2025).

Nuhi, M. H., Al Ghozi, L., Nazla, S., & Syakirah, D. (2024). Pembaharuan Hukum Penanganan Tindak Pidana Pemalsuan Identitas Akibat Penyalahgunaan Artificial Intelligence Di Indonesia. Jurnal Batavia, 1(2), 80-88.

Peter Mahmud Marzuki, Penelitian Hukum (Jakarta: Kencana Prenada Media Group, 2011).

Puannandini, D. A., Fabian, R., Firdaus, R. A. P., Mustopa, M. Z., & Herdiyana, I. (2025). Liabilitas Produk Ai Dalam Sistem Hukum Indonesia: Implikasi Bagi Pengembang, Pengguna, Dan Penyedia Layanan. Iuris Studia: Jurnal Kajian Hukum, 6(1), 24-33.

Putri Mecca, A. S., Hidaya, W. A., & Tuasikal, H. (2025). PEMANFAATAN TEKNOLOGI KECERDASAN BUATAN (ARTIFICIAL INTELLIGENCE) DALAM SISTEM PERADILAN PIDANA DI INDONESIA. Journal of Social & Technology/Jurnal Sosial dan Teknologi (SOSTECH), 5(6).

Rangga Suganda, "Metode Pendekatan Yuridis Dalam Memahami Sistem Penyelesaian Sengketa Ekonomi Syariah," Jurnal Ilmiah Ekonomi Islam 8, no. 3 (2022): 2859, https://doi.org/10.29040/jiei.v8i3.6485.

Ras, H., Pranadita, N., & Wiradirja, I. R. (2023). Potential technological interventions in transnational crime from the perspective of criminal law in Indonesia. Russian Law Journal, 11(3), 11-16.

Ruhtiani, M. (2025). HUKUM PIDANA DAN HAK CIPTA DI ERA KECERDASAN ARTIFISIAL: ANALISIS PERTANGGUNGJAWABAN DALAM HUKUM POSITIF DAN HUKUM ISLAM. Jurnal Al-Wasith: Jurnal Studi Hukum Islam, 10(1), 62-79.

Zulfa, A. A. PEMANFAATAN DATA PENGGUNA LAYANAN MELALUI COOKIE OLEH ARTIFICIAL INTELLIGENCE DITINJAU DARI PERSPEKTIF HAK ASASI MANUSIA. Artificial Dalam Bidang Hukum Di Era Teknologi Informasi: Tantangan Dan Peluang, 95.

Zuwanda, Z. S., Lubis, A. F., Solapari, N., Sakmaf, M. S., & Triyantoro, A. (2024). Ethical and Legal Analysis of Artificial Intelligence Systems in Law Enforcement with a Study of Potential Human Rights Violations in Indonesia. The Easta Journal Law and Human Rights, 2(03), 176-185.