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

Void in Law: Criminal Regulation Vacuum on the Detrimental Impact of AI Artificial Intelligence

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

Advances in artificial intelligence (AI) technology have brought new challenges in the realm of criminal law, especially related to accountability for autonomous actions that cause legal losses. Indonesia's criminal law system, which is still based on an anthropo-centric paradigm with the conditions of actus reus and mens rea, has not been able to accommodate non-human digital entities such as AI. The absence of explicit criminal norms against AI's detrimental behavior leads to a legal void, where real harm cannot be effectively acted upon. Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) has not specifically regulated the attribution of errors to AI, developers, and system operators. This study uses normative juridical methods with conceptual and comparative legal approaches to analyze the need for the formation of a new criminal framework for AI. The results of the study show the urgency of reformulating criminal regulations that are risk-based and adaptive to technological developments, as reflected in the EU Artificial Intelligence Act model. It is also necessary to strengthen the concept of indirect criminal liability and the possibility of recognition of electronic legal entities. Without regulatory innovation, Indonesia's criminal justice system risks failing to protect the digital society fairly and effectively. This study recommends the establishment of specific norms that are responsive to the risks of AI technology.

Keywords: Artificial Intelligence; Criminal Liability; Legal Void.

INTRODUCTION

Advances in artificial intelligence (AI) technology in the past decade have brought significant disruption in various sectors of life, from healthcare, financial systems, logistics and transportation, to legal and administrative decision-making processes. AI is no longer just a technical tool, but has become a digital entity capable of executing analytical and predictive functions autonomously, even in situations that require complex reasoning and adaptive responses. While these developments bring benefits to efficiency and innovation, there are also serious concerns about potential negative impacts that are systemic and individual. AI can produce and disseminate misleading information (disinformation), reinforce algorithmic biases that lead to discrimination against certain groups, and systematically violate the privacy rights of individuals through the practice of data collection and processing without explicit consent.[1]

This phenomenon shows the dimension of real losses caused by the use of AI, both in the form of material losses, rights violations, and threats to social integrity and democracy.[2] Unfortunately, this reality has not been fully accommodated in the current criminal law system, which is still based on classical principles regarding legal subjects, faults, and criminal liability. Criminal law designed in an anthropo-centric paradigm has difficulty reaching digital entities that are non-human and have no will or moral awareness. Therefore, there is a normative void that hinders the effectiveness of the criminal justice system in responding appropriately and fairly to the risk dynamics of AI technology. The absence of a legal framework specific to AI poses a serious challenge to the principles of legal certainty and the protection of people's rights in the digital age.

The void of criminal regulation in the context of artificial intelligence in Indonesia reflects the absence of legal norms that explicitly regulate the forms of adverse behavior generated by AI systems. In practice, many losses arising from the autonomous actions of AI cannot be prosecuted or criminally accounted for due to the absence of legal provisions that establish AI as a legal subject, nor a mechanism for attributing faults to the creators, programmers, or users of the system.[3] As a concrete example, in 2023 there was an incident in the digital financial sector when an AI-based investment platform recommended high-risk transactions to thousands of retail users, resulting in a collective loss of more than IDR 25 billion. However, there is no criminal law basis that allows law enforcement officials to ensnare entities or individuals responsible for losses arising from such algorithmic errors. Similar cases also occur in AI-based recruitment systems used by several large companies, where discrimination is found against female job applicants and people with disabilities, but no criminal instrument can be used to crack down on such discriminatory practices because the perpetrators are not humans, but algorithmic systems.[4]

The absence of specific criminal regulations on AI in Indonesia is not solely due to legislative negligence, but also due to epistemological and juridical complexity in setting the limits of accountability for non-human actions.[5] The Indonesian government has so far only responded to the development of digital technology through sectoral regulations such as the ITE Law, the Personal Data Protection PP, and the Artificial Intelligence Bill which are still in the conceptual stage. However, none of these instruments specifically govern the criminal framework against adverse behavior generated by AI autonomously. One of the main obstacles is the ambiguity of who should be held accountable for the losses arising from AI decisions: whether the algorithm's developers, the users of the

---

[1] Astiti, N. M. Y. A. (2023). Strict Liability of Artificial Intelligence: Pertanggungjawaban kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban. *Jurnal Magister Hukum Udayana*, *12*(4), 962-980.

[2] Amelia, Y. F., Kaimuddin, A., & Ashsyarofi, H. L. (2024). Pertanggungjawaban pidana pelaku terhadap korban penyalahgunaan artificial intelligence deepfake menurut hukum positif Indonesia. *Dinamika*, *30*(1), 9675-9691.

[3] Syahirah, S. N., & Prasetyo, B. (2025). Tinjauan Yuridis Terhadap Penggunaan Teknologi Deepfake Untuk Pornografi Melalui Artificial Intelligence (AI) Di Indonesia. *Jurnal Inovasi Hukum Dan Kebijakan*, *6*(1).

[4] Nabhila, C. (2024). Analisis Tentang Respon Hukum Terkait Penggunaan Artificial Intelligence Di Indonesia. *Pancasila Law Review*, *1*(2), 69-87.

[5] Al Adwan, M. A. S. (2025). Legislative Confrontation to Protect Public Rights and Freedoms from The Impact of Artificial Intelligence. *Pakistan Journal of Criminology*, *17*(1).

system, the corporations that operate it, or the AI itself.[6] On the other hand, the slow formation of regulations is also caused by the lack of a global consensus on the ethical and legal approach to this technology, so Indonesia tends to have a wait-and-see attitude towards regulations that are still developing in international jurisdictions. In fact, the longer this vacancy is left untouched, the greater the risk of losses that cannot be reached by the existing legal mechanism.

The traditional concept in criminal law is based on the principle of individual responsibility, namely that the subject of criminal law is a human being as a rational being who has awareness, free will, and the ability to understand the consequences of his actions. In this construction, the existence of mens rea (inner error) and actus reus (unlawful acts) are cumulative conditions for punishment.[7] However, the emergence of artificial intelligence (AI) as a digital entity capable of performing autonomous actions without direct human intervention has blurred the line between actors and tools. AI, as a system that can "learn" through machine learning algorithms, has the potential to carry out actions that have unexpected legal consequences by its creators, so that it does not meet the criteria of conventional legal subjects in Indonesia's positive criminal law. This is a critical point in efforts to attribute criminal liability for adverse actions committed by AI systems.[8]

In Indonesia's positive legal perspective, the void of criminal regulation against AI can be studied through the theory of interpretation and the principle of legality (nullum crimen sine lege), which affirms that no act can be punished without the provisions of the law that governs it first.[9] Therefore, when AI systems autonomously cause losses such as algorithm-based discrimination or wrong decisions in the AI-based medical sector, there are no explicit criminal norms to take action or attribute legal responsibility.[10] In the context of AI, Indonesia's criminal law does not have adequate instruments to adapt itself to disruptive technological developments that create a *legal vacuum* in the protection of victims. This condition opens up a space of impunity, where actors who are indirectly responsible for the damage caused by AI can escape legal proceedings due to the weak norms governing *vicarious liability*.

The urgency of criminal law reformulation in the face of AI challenges can also be analyzed through a progressive approach to criminal law, as developed by contemporary legal experts such as Mireille Hildebrandt and Gabriel Hallevy. This approach provides a normative solution so that criminal law remains functional in responding to technology-based crime, without having to wait for the legal status of AI as a formal legal subject. In the Indonesian context, this urgency is even more relevant given the massive use of AI in the public and private sectors without an adequate legal framework to accommodate the conflicts and losses arising from it.

---

[6] Gaviria, C. I. G. (2022). The role of artificial intelligence in pushing the boundaries of US regulation: A systematic review. *Santa Clara High Tech. LJ*, *38*, 123.

[7] Feri Antoni, S. (2025). *REKONSTRUKSI PENGATURAN SANKSI PIDANA BAGI KORPORASI TERHADAP PELANGGARAN ADMINISTRATIVE PENAL LAW DALAM RANGKA PEMBAHARUAN HUKUM PIDANA* (Doctoral dissertation, Program Studi Doktor Hukum).

[8] Abbott, R., & Sarch, A. (2022, April). Punishing artificial intelligence: legal fiction or science fiction. In *International Conference on Autonomous Systems and the Law* (pp. 83-115). Cham: Springer International Publishing.

[9] Senjaya, M. (2023). APPLICATION OF CRIMINAL LAW TO UTILIZATION ARTIFICIAL INTELLIGENCEIN INDONESIA. *International Journal of Social Science*, *3*(4), 415-422.

[10] Belouadah, T. (2025). The Criminal Law Challenges in Confronting AI Crimes, *10*(1), 1157-1172.

The Indonesian government has so far not adopted concrete steps in formulating a specific criminal legal framework for AI, although the development of this technology has had a variety of real negative impacts on the ground. The Personal Data Protection Bill (PDP Law) and the discourse on the Artificial Intelligence Bill are still normative in general nature and have not regulated the aspects of criminal responsibility in detail. This is in contrast to other jurisdictions such as the European Union which have introduced the concept *of the AI Act* and discussed *risk-based criminal liability*. This regulatory lag must be immediately responded to by lawmakers through a multidisciplinary approach that combines legal science, technological ethics, and system engineering, in order to avoid legal vacuums that can erode public trust in the criminal justice system and social justice in the digital era.

METHOD

This research uses a normative juridical method, which is a legal research method that relies on the study of applicable positive legal norms. The purpose of this method is to examine the emptiness, ambiguity, and inconsistency of legal norms, as well as to formulate legal arguments for the need to form new regulations in accordance with technological developments. 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.[11]

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.[12] 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.[13] 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.[14]

In the study, the normative juridical method was used to identify and analyze the absence of a criminal regulation that specifically regulates legal liability for losses caused by autonomous artificial intelligence (AI) systems in Indonesia.

The normative approach is carried out by examining a number of relevant laws and regulations, such as the Criminal Code (KUHP) and Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) along with its amendments and implementing regulations, especially in terms of regulating responsibility for the use of electronic systems and digital algorithms. In addition, the Draft Law on Personal Data Protection (PDP Bill) as well as academic manuscripts and the initial concept of artificial intelligence regulations that are being developed were also studied. The *conceptual approach* is used to elaborate modern criminal law theories related to non-human liability, while the *comparative approach* is used to analyze the practices of other

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

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

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

[14] 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.

countries such as the *AI Act* of the European Union and the concept *of criminal liability of AI* in the common law system.

The data sources in this study are secondary data, consisting of primary legal materials (laws and regulations), secondary legal materials (legal literature, results of previous research, scientific journals), and tertiary legal materials (legal dictionaries, legal encyclopedias, and regulatory databases). The data collection technique is carried out through a systematic literature study, and analyzed in a normative qualitative manner, by interpreting the applicable legal principles to develop an argumentative framework for the need for new criminal regulations that are adaptive to the development of AI.

With this approach, the research is expected to make a theoretical and practical contribution in forming a criminal law framework that is able to answer legal challenges in the digital era, as well as fill the regulatory gap that has the potential to harm society due to the absence of legal norms that regulate losses by AI systems directly.

DISCUSSION

1. Incompatibility of the Traditional Criminal Liability Concept for Artificial Intelligence Entities

In classical criminal law doctrine, criminal liability can only be imposed on legal subjects who have legal awareness, namely human beings as natural legal subjects, and legal entities as fictitious legal subjects subject to corporate accountability mechanisms. However, artificial intelligence (AI) capable of performing cognitive functions such as learning, making decisions, and acting autonomously raises new questions about who should be criminally liable if the actions of AI cause harm or violate the law.[15] The main principles of criminal law such as actus reus (unlawful acts) and mens rea (malicious intent or inner error) become difficult to apply to entities that have no human consciousness or will.

In the Indonesian criminal law system, which is based on the principle of culpa and the principle of nullum crimen sine culpa, fault (mens rea) is an essential element to determine criminal liability. Therefore, AI that has no intention or will cannot be easily subject to criminal sanctions. This becomes a serious obstacle, especially when AI generates decisions independently of human intervention and such actions result in significant legal repercussions, for example in autonomous vehicle accidents, biased algorithmic recommendation systems, or the use of deepfakes for criminal purposes.[16]

A number of approaches have been proposed by contemporary criminal law scholars to respond to this challenge. One approach is the use of the principle of vicarious liability, which is criminal liability imposed on other parties who have a relationship with the perpetrator, in this case the developer, owner, or operator of AI. This approach has been used in the context of corporate accountability, but it is not yet fully compatible with situations where AI acts beyond the expectations of its owners. Another approach is strict liability, which is accountability without fault, where parties related to AI can still be held criminally liable even if there is no element of subjective fault.[17] However, the application

---

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

[16] Kadir, Z. K. (2025). Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse. *Jurnal Litigasi Amsir*, *12*(2), 124-137.

[17] 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.

of strict liability in Indonesian criminal law is still limited and generally applied to administrative crimes or those that have a broad impact on society, such as the environment and food.

Furthermore, some experts propose the establishment of a new legal framework that recognizes an "electronic legal entity" or "electronic legal personality" for AI, thus allowing AI to become a separate legal subject with a distinctive accountability mechanism, for example through special compensation funds or the imposition of administrative sanctions. In this case, criminal law no longer relies entirely on the human personification of the perpetrator, but begins to adjust to the complexity of the human-technology relationship.[18] The development of the international criminal law literature, as proposed by Gabriel Hallevy with the theories of Perpetration-via-Another, Natural-Probable-Consequence, and the Direct Liability Model, provides a direction to reconstruct the doctrine of criminal liability in the face of entities operating outside the framework of ordinary human will. However, the application of these theories in Indonesia still requires normative legitimacy and legislative reformulation that is not yet available in the current positive legal system.

2. Void and Limitations of Criminal Regulation in Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law)

Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), which is the main legal basis in regulating digital activities in Indonesia, faces serious challenges when faced with the development of artificial intelligence (AI) technology. The ITE Law is designed to regulate crimes committed by humans through electronic systems, such as defamation, hacking, and data manipulation. However, AI technology has now evolved into an autonomous system, capable of making decisions independently without direct instructions from humans. The ITE Law is limited because it does not accommodate the possibility of non-human entities that can produce harmful acts independently, thus creating a legal vacuum in criminal enforcement of AI.

One of the main problems in this context is the absence of explicit regulation of how AI is qualified in criminal law: whether AI is only seen as an instrument or needs to be positioned as a new legal subject. The classical approach of criminal law requires the existence of two main elements, namely acts (actus reus) and malicious intent (mens rea), which can only be fulfilled by humans. AI, which operates on machine learning algorithms and big data, has no legal will or awareness, making it impossible to meet the conventional mens rea element.[19] This inaccuracy in classification leads to confusion in the law enforcement process, especially in proving a causal relationship between the actions of AI and the harm suffered by the victim, in the absence of a human actor directly involved.

Furthermore, the ITE Law does regulate the prohibition of misuse of electronic systems, including illegal access, interference with data integrity, and information manipulation. However, these provisions are highly dependent on the identification of the

---

[18] Hammouri, J. A., Almahasneh, A. A. A., Khwaileh, K. M., & Al-Raggad, M. M. (2024). The Criminal Liability of Artificial Intelligence Entities. *Pakistan Journal of Life and Social Sciences*, *22*(2), 8785-8790.

[19] Jahriyah, V. F., Kusuma, M. T., Qonitazzakiyah, K., & Fathomi, M. A. (2021). Kebebasan Berekspresi di Media Elektronik Dalam Perspektif Pasal 27 Ayat (3) Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Pelayanan Transaksi Elektronik (UU ITE). *Sosio Yustisia: Jurnal Hukum Dan Perubahan Sosial*, *1*(2), 65-87.

perpetrator and the accompanying intentions. In certain cases, such as when AI causes the spread of false information or privacy violations without direct orders from humans, no single article can effectively be used to ensnare criminal liability. In fact, in scenarios where losses occur due to algorithmic errors or systemic bias, the determination of responsibility between developers, platform operators, or end users becomes blurred. As a result, the legal process is often hampered by the lack of a clear legal mechanism to determine who must be held criminally accountable.

Thus, the emptiness and limitations in the ITE Law mark the urgency of reformulating criminal regulations that are able to answer the complexity of human interaction and AI. Current regulations are reactive and inadequate to anticipate the negative impacts of the use of autonomous technology.[20] A progressive criminal law approach is needed, such as the expansion of the principle of corporate criminal liability that can include the acts of AI as part of a system controlled by a specific legal entity. In addition, the formulation of special norms through the establishment of lex specialis also needs to be considered, so that criminal liability for losses caused by AI can be determined proportionately and fairly. Without legal updates that are adaptive to digital reality, the ITE Law will continue to lag behind in the face of technological evolution that continues to move rapidly.

3. The Urgency of Establishing a Specific and Responsive Criminal Law Framework to AI Technology Risks

In the face of the widespread penetration of artificial intelligence (AI) technology into various aspects of life, the need for the formation of a specific and responsive criminal law framework has become a legal necessity. The autonomous, adaptive, and in some cases self-learning characteristics of AI pose serious challenges to the national criminal justice system, particularly in terms of fault attribution, mens rea construction, and identification of perpetrators. AI technology can produce real harm to individual and public rights, but it often cannot be directly attributed to humans as subjects of conventional law. Indonesia's criminal law system, which still relies heavily on the principle of strict legality and individual accountability structures, faces a real lacuna legis.[21] Therefore, the urgency of reformulating criminal legislation policies that are anticipatory and futuristic needs to be seriously encouraged in order to fill the existing void in law.

By comparison, international approaches to regulating artificial intelligence have begun to take shape systematically. One of them is the EU Artificial Intelligence Act which divides AI risks into several categories: minimal risk, high risk, and unacceptable risk. This approach is the basis for the establishment of a risk-based criminal regulation system where legislation is not only reactive to consequences, but also preventive to potential harm.[22] In addition, in the common law system, especially in the United

---

[20] Nur, M. I., & Jaya, F. (2022). Efektivitas Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Sebagai Upaya Penanggulangan Tindak Asusila Berbasis Teknologi (Cybersex). *Ensiklopedia ofJournal*, *4*(3), 166-174.

[21] 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.

[22] Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal of Law*, *1*(1), 1-23

Kingdom and the United States, the concepts of vicarious liability and strict liability to corporate entities or owners of AI systems have developed first, inspiring Indonesia to adopt a more flexible and forward-looking model of criminal liability. This is important because the perpetrators who are "responsible" for losses due to AI can be non-human entities or corporations, not just individuals.

No less important is how criminal law must maintain fundamental principles, especially the principles of legal certainty, equality before the law, and protection of victims' rights. In a complex digital context, strengthening the aspect of legal protection for victims is the main pressure point. For example, victims of deepfake pornography, algorithmic manipulation to the detriment of consumers, or automated discrimination by AI systems in public services need to have clear and effective legal channels. Without a specific criminal law instrument, victims risk facing technological impunity, which is a situation in which real losses cannot be legally recovered because the perpetrator is not recognized or cannot be held normatively accountable.

Thus, the urgency of establishing a criminal law framework specific to AI is not only oriented towards criminalization as a form of retribution, but also as a tool of governance in forming an ethical and fair technological ecosystem. Indonesia needs to design a criminal law system that is adaptive, anticipatory, and risk-based, by prioritizing the principle of substantive justice in the digital society. This requires not only the renewal of the Law, but also the establishment of new legal norms that can accommodate the complexity of human-machine relationships, as well as strengthening the capacity of law enforcement in understanding digital technology. This step will position the criminal law not just as a repressive instrument, but as a proactive mechanism in ensuring public protection in the era of artificial intelligence.

CONCLUSION

The overall discussion shows that Indonesia's classical criminal law system faces significant challenges in dealing with autonomous and adaptive artificial intelligence (AI) entities. The inconsistency between the principles of actus reus and mens rea with the character of AI creates a real legal vacuum. The ITE Law as the basis of cybercriminal law in Indonesia does not anticipate the role of AI as a non-human actor. As a result, AI that causes losses often escapes the reach of criminal sanctions because the elements of error are not met conventionally. Criminal efforts through the principles of vicarious liability and strict liability have not gained adequate normative legitimacy. Therefore, there is a need for a reformulation of the criminal accountability system that is able to accommodate non-human entities in a positive legal structure. The establishment of a specific criminal law framework for AI is urgent, not only for the sake of law enforcement effectiveness, but also for the sake of justice for victims. The risk-based legal model, as applied in the EU Artificial Intelligence Act, can be a relevant reference for Indonesia. The expansion of legal subjects through the concept of electronic legal personality is also an option worth studying. In this context, criminal law must be proactive and anticipatory, as well as ensure substantive legal protection in the digital environment. Without responsive regulatory updates, the risk of technological impunity will continue to increase. Thus, the establishment of new criminal norms against AI is inevitable in the era of digital transformation.

REFERENCES

Abbott, R., & Sarch, A. (2022, April). Punishing artificial intelligence: legal fiction or science fiction. In International Conference on Autonomous Systems and the Law (pp. 83-115). Cham: Springer International Publishing.

Al Adwan, M. A. S. (2025). Legislative Confrontation to Protect Public Rights and Freedoms from The Impact of Artificial Intelligence. Pakistan Journal of Criminology, 17(1).

Amelia, Y. F., Kaimuddin, A., & Ashsyarofi, H. L. (2024). Pertanggungjawaban pidana pelaku terhadap korban penyalahgunaan artificial intelligence deepfake menurut hukum positif Indonesia. Dinamika, 30(1), 9675-9691.

Astiti, N. M. Y. A. (2023). Strict Liability of Artificial Intelligence: Pertanggungjawaban kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban. Jurnal Magister Hukum Udayana, 12(4), 962-980.

Belouadah, T. (2025). The Criminal Law Challenges in Confronting AI Crimes. المجلة الجزائرية للحقوق والعلوم السياسية, 1(10, 1172-1157).

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. Dame Journal of Law, 1(1), 1-23

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.

Feri Antoni, S. (2025). Rekonstruksi Pengaturan Sanksi Pidana Bagi Korporasi Terhadap Pelanggaran Administrative Penal Law Dalam Rangka Pembaharuan Hukum Pidana (Doctoral dissertation, Program Studi Doktor Hukum).

Gaviria, C. I. G. (2022). The role of artificial intelligence in pushing the boundaries of US regulation: A systematic review. Santa Clara High Tech. LJ, 38, 123.

Hammouri, J. A., Almahasneh, A. A. A., Khwaileh, K. M., & Al-Raggad, M. M. (2024). The Criminal Liability of Artificial Intelligence Entities. Pakistan Journal of Life and Social Sciences, 22(2), 8785-8790.

Jahriyah, V. F., Kusuma, M. T., Qonitazzakiyah, K., & Fathomi, M. A. (2021). Kebebasan Berekspresi di Media Elektronik Dalam Perspektif Pasal 27 Ayat (3) Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Pelayanan Transaksi Elektronik (UU ITE). Sosio Yustisia: Jurnal Hukum Dan Perubahan Sosial, 1(2), 65-87.

Kadir, Z. K. (2025). Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse. Jurnal Litigasi Amsir, 12(2), 124-137.

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).

Nabhila, C. (2024). Analisis Tentang Respon Hukum Terkait Penggunaan Artificial Intelligence Di Indonesia. Pancasila Law Review, 1(2), 69-87.

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

Nur, M. I., & Jaya, F. (2022). Efektivitas Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Sebagai Upaya Penanggulangan Tindak Asusila Berbasis Teknologi (Cybersex). Ensiklopedia ofJournal, 4(3), 166-174.

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

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.

Senjaya, M. (2023). Application Of Criminal Law To Utilization Artificial Intelligencein Indonesia. International Journal of Social Science, 3(4), 415-422.

Syahirah, S. N., & Prasetyo, B. (2025). Tinjauan Yuridis Terhadap Penggunaan Teknologi Deepfake Untuk Pornografi Melalui Artificial Intelligence (AI) Di Indonesia. Jurnal Inovasi Hukum Dan Kebijakan, 6(1).

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