DOI: 10.46924/jihk.v7i2.330

Artificial Intelligence and Criminal Liability: A Preliminary Study within the Indonesian Legal System

Novelina Mutiara Sariati Hutapea[1]*, Desy Kartika Caronina Sitepu[2], Jenriswandi Damanik[3], & Srikandi Karmeli Lusia Sianipar[4]

[1,2,3,4]Universitas Simalungun, Indonesia

Correspondence

Novelina Mutiara Sariati Hutapea, Universitas Simalungun, Indonesia, Jl. Sisingamangaraja Barat, Bah Kapul, Kec. Siantar Sitalasari, Kota Pematang Siantar, Sumatera Utara 21142, e-mail: novelina.hutapea@yahoo.com

How to cite

Hutapea, Novelina Mutiara Sariati., Sitepu, Desy Kartika Caronina., Damanik, Jenriswandi., & Sianipar, Srikandi Karmeli Lusia. 2026. Artificial Intelligence and Criminal Liability: A Preliminary Study within the Indonesian Legal System. *Jurnal Ilmu Hukum Kyadiren* 7(1), 688-704. https://doi.org/10.46924/jihk.v7i2.330

Original Article

Abstract

The rapid development of Artificial Intelligence (AI) presents significant challenges for Indonesian criminal law, particularly in determining accountability for actions involving AI, whether as an auxiliary tool or as an indirect perpetrator. This study seeks to examine the current criminal law framework, identify deficiencies in the Criminal Code (KUHP), the Electronic Information and Transactions Law (ITE Law), and related regulations, and assess the applicability of alternative liability models, including vicarious liability and strict liability. Employing a normative juridical approach—through the analysis of statutory provisions, legal doctrine, and international case studies—this research finds that national regulations remain predominantly reactive, fail to adequately anticipate the emergence of autonomous AI, and encounter technical evidentiary challenges arising from the 'black box' phenomenon. The findings suggest that alternative liability models are better suited to the distinctive characteristics of AI. The study concludes that a responsive reformulation of criminal law norms is essential to ensure legal certainty, protect victims, and facilitate effective law enforcement in the context of AI.

Keywords: *Artificial Intelligence, Criminal Law, Criminal Liability*

Abstrak

Perkembangan Artificial Intelligence (AI) menimbulkan tantangan baru bagi hukum pidana Indonesia, khususnya dalam menentukan pertanggungjawaban atas tindakan yang melibatkan AI baik sebagai alat bantu maupun pelaku tidak langsung. Penelitian ini bertujuan menganalisis kerangka hukum pidana yang berlaku, mengidentifikasi kelemahan dalam KUHP, UU ITE, dan regulasi terkait, serta mengkaji relevansi model pertanggungjawaban alternatif seperti vicarious liability dan strict liability. Menggunakan metode yuridis normatif dengan analisis peraturan perundang-undangan, doktrin hukum, dan studi kasus internasional, penelitian menemukan bahwa regulasi nasional masih bersifat reaktif, belum mengantisipasi AI otonom, dan menghadapi kendala teknis pembuktian akibat fenomena *black box*. Model pertanggungjawaban alternatif dinilai lebih adaptif terhadap karakteristik AI. Kesimpulannya, diperlukan reformulasi norma hukum pidana yang responsif untuk memastikan kepastian hukum, perlindungan korban, dan efektivitas penegakan hukum untuk AI.

Kata kunci: *Kecerdasan Buatan, Hukum Pidana, Pertanggungjawaban Pidana*

1. INTRODUCTION

Over the past two decades, advancements in information and communication technology have profoundly transformed the paradigms of human interaction, economic activity, and legal systems. Among the most transformative innovations is Artificial Intelligence (AI), which has evolved far beyond simple automation to become autonomous systems capable of complex decision-making. While this development offers substantial opportunities across various sectors, including law enforcement, it also poses fundamental challenges to criminal justice systems that were historically designed to regulate human behavior.

In Indonesia, AI has permeated numerous sectors—from manufacturing and banking to autonomous transportation, public services, and even the judiciary. However, alongside these benefits emerge significant risks, including deepfakes, data manipulation, adaptive cyberattacks, and accidents involving autonomous vehicles. These risks raise a critical legal question: when AI engages in unlawful conduct or causes harm, who should bear criminal responsibility? This question is further complicated by the fact that AI systems, driven by self-learning algorithms (machine learning), may exhibit behaviors unpredictable even to their creators.

The Indonesian criminal law system, as codified in the Criminal Code and various sector-specific laws such as the Electronic Information and Transactions Law, adheres to the principle of *geen straf zonder schuld* ("no crime without fault"), which requires both *mens rea* (criminal intent) and actus reus (criminal act) on the part of a legally responsible subject. However, AI lacks consciousness, volition, and moral capacity, and therefore does not meet the criteria for a criminal law subject. This creates a legal vacuum in which the existing framework does not recognize the possibility of AI functioning as a direct perpetrator of criminal acts.

Several jurisdictions have attempted to address this issue. The European Union, for instance, through its European Parliament Resolution on Civil Law Rules on Robotics, has introduced the concept of "electronic personhood" for certain highly autonomous AI systems.[1] Other jurisdictions, such as the United States and Japan, favor vicarious or strict liability models, holding operators, controllers, or manufacturers responsible. Nonetheless, there is no global consensus on the most appropriate framework, and academic debate remains ongoing.

In Indonesia, scholarly discussions on AI criminal liability remain relatively nascent, often focusing on conceptual and ethical considerations rather than on operational frameworks aligned with national criminal law principles. Previous research has primarily addressed the urgency of AI regulation, its potential recognition as a legal

[1] The European Parliament, "European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics" (Strasbourg: The European Parliament, 2017), https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html.

subject, and ethical risk assessments, without offering concrete models for legal implementation. Moreover, the rapid adoption of AI in both commercial and public domains underscores the risks of delayed legal adaptation, which could lead to legal uncertainty, enforcement challenges, and societal harm.

Sulistio and Salsabilla emphasize the necessity of regulating AI as a legal entity within Indonesian criminal law, noting the increasing human-like capacities of AI to perform acts that may infringe legal interests. Employing a normative approach, their research advocates for the eventual recognition of AI as a legal subject to enable direct criminal prosecution.[2] Continuing this discourse, Setyawan highlights the absence of AI-related provisions in the new Criminal Code (Law No. 1 of 2023). Through a normative and comparative legal analysis, he demonstrates that several jurisdictions have adopted AI as a legal subject—either directly or via vicarious liability—while Indonesia continues to hold accountable those who control or utilize AI.[3]

Ikawati et al. examine the application of AI from a judicial perspective, particularly as a tool to assist judges and court officials in managing cases. While emphasizing efficiency and effectiveness, they underscore the risks of algorithmic bias, privacy violations, and data security breaches. Their work focuses more on ethical considerations and technology governance than on issues of direct criminal liability.[4] Similarly, Nasman et al. adopt an ethical and regulatory approach, emphasizing four fundamental pillars of responsible AI use: transparency, accountability, fairness, and data security and privacy. Employing a normative-comparative methodology, they recommend strengthening regulatory frameworks to minimize the potential misuse of AI. Although their study does not center on criminal sanctions, it stresses the importance of developing an adaptive legal framework.[5]

Hibatulloh directs his research toward law enforcement measures against AI-related offenses, using conceptual, legislative, and comparative approaches. He concludes that AI is not yet recognized as a legal subject under Indonesian law; thus, criminal liability can only be attributed to individuals or legal entities formally acknowledged by law. Beryl, in a similar vein, advocates for regulations that explicitly

[2] Faizin Sulistio and Aizahra Daffa Salsabilla, "Pertanggungjawaban Pada Tindak Pidana Yang Dilakukan Agen Otonom Artificial Intelegence," *Unes Law Review* 6, no. 2 (2023): 5479–90, https://doi.org/10.31933/unesrev.v6i2.1209.

[3] Vincentius Patria Setyawan, "Prospek Pengaturan Kecerdasan Buatan Sebagai Subjek Hukum Pidana Dan Model Pertanggungjawabannya," *Sultan Adam: Jurnal Hukum Dan Sosial* 3, no. 1 (2025): 115–122, https://doi.org/10.71456/sultan.v3i1.1214.

[4] Linda Ikawati, Sulaiman Sulaiman, and Muhammad Fahri Huseini, "Masa Depan Penegakan Hukum Indonesia: Sistem Peradilan Pidana Berbasis Kecerdasan Buatan (AI)," in *Prosiding Seminar Nasional Ilmu Hukum* (Pemalang: Asosiasi Peneliti dan Pengajar Ilmu Hukum Indonesia, 2024), 1–18, https://doi.org/10.62383/prosemnashuk.v1i1.19.

[5] Nasman Nasman, Pudji Astuti, and Dita Perwitasari, "Etika Dan Pertanggungjawaban Penggunaan Artificial Intelengence Di Indonesia," *Jurnal Hukum Lex Generalis* 5, no. 10 (2024): 1–15, https://ojs.rewangrencang.com/index.php/JHLG/article/view/622.

address AI as a potential criminal actor.[6] Sofian also addresses this issue, emphasizing the need for future criminal law reform (ius constituendum) to incorporate AI as a legal subject. He argues that several jurisdictions have already adopted such recognition and that Indonesia should consider following suit to address potential legal violations committed by autonomous AI systems.[7]

In the context of judicial duties, Rondonuwu et al. analyze the use of AI based on existing legal instruments, such as Law No. 19 of 2016 and the Circular Letter of the Minister of Communication and Information Technology No. 9/2023. They conclude that, under current Indonesian law, AI is regarded as an electronic agent rather than a criminal law subject. Their study focuses on integrating AI into judicial work and the administrative arrangements necessary to facilitate this integration.[8]

Wahyudi BR provides a broader examination of AI-related crimes, including adaptive cyberattacks, data manipulation, and the misuse of deepfakes. He observes that both the Electronic Information and Transactions Law and international frameworks such as the Budapest Convention do not explicitly address AI-based offenses. His recommendations include regulatory reform, capacity building for enforcement authorities, and global legal harmonization.[9] Astiti contends that AI cannot be recognized as a legal subject because it lacks the capacity for will or control over its actions. Consequently, she argues that criminal liability should be borne by AI developers and users, in line with the doctrines of strict liability and vicarious liability, without extending legal subject status to AI.[10]

Maharani et al. (2025) broaden the discussion to societal protection against AI-related harms, including copyright infringement, plagiarism, and the malicious use of deepfakes. Using a normative legal approach, they call for comprehensive regulations that prioritize the protection of human values.[11] Putri et al. stress the urgency of AI implementation in law enforcement while acknowledging barriers such as legal gaps and low public awareness. They view AI as a complementary tool that enhances efficiency but cannot fully replace human decision-making.[12] Setiawan and Wijayanto provide a

[6] Beryl Helga Fredella Hibatulloh, "Upaya Penegakan Hukum Terhadap AI (Artificial Intelligence) Sebagai Subjek Hukum Pidana Dalam Perspektif Kriminologi," *Taruna Law: Journal of Law and Syariah* 3, no. 1 (2025): 87–98, https://doi.org/10.54298/tarunalaw.v3i01.300.

[7] Ahmad Sofian, "Konsepsi Subjek Hukum Dan Pertanggungjawaban Pidana Artificial Intellegence," *Halu Oleo Law Review* 9, no. 1 (2025): 13–26, https://doi.org/10.33561/holrev.v9i1.129.

[8] Natalie Tresye Rondonuwu, Donna Okthalia Setiabudhi, and Carlo A Gerungan, "Pengaturan Penggunaan Kecerdasan Buatan Dalam Tugas Profesional Hakim Di Indonesia," *Lex Privatum* 15, no. 2 (2025): 1–12, https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/60761.

[9] Wahyudi BR, "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI," *Innovative: Journal Of Social Science Research* 5, no. 1 (2025): 3436–3450, https://doi.org/10.31004/innovative.v5i1.17519.

[10] Ni Made Yordha Ayu Astiti, "Strict Liability of Artificial Intelligence: Pertanggungjawaban Kepada Pengatur AI Ataukah AI Yang Diberikan Beban Pertanggungjawaban?," *Jurnal Magister Hukum Udayana* 12, no. 4 (2023): 962–80, https://doi.org/10.24843/JMHU.2023.v12.i04.p14.

[11] Bondan Ayu Maharani et al., "Perlindungan Hukum Masyarakat Dari Dampak Negatif Penggunaan AI," *Media Hukum Indonesia* 3, no. 2 (2025): 666–73, https://ojs.daarulhuda.or.id/index.php/MHI/article/view/1939.

[12] Feby Milenia Yahya Krisna Putri et al., "Thinking the Future Potential of Artificial Intelligence in Law Enforcement," *Perspektif Hukum* 24, no. 2 (2024): 269–294, https://doi.org/10.30649/ph.v24i2.319.

sector-specific analysis of AI in the automotive industry, particularly in autonomous vehicles. They recommend applying strict liability principles to drivers and product liability principles to manufacturers, while advocating regulatory reforms to address AI as a legal subject.[13]

Previous scholarship has explored AI regulation, the possibility of recognizing AI as a legal subject, and the challenges of law enforcement. However, no prior research has comprehensively integrated an analysis of alternative criminal liability models—such as vicarious liability and strict liability—within the Indonesian criminal law framework for AI-related cases. Most studies remain focused on ethical, administrative, or conceptual dimensions without offering operational formulations applicable in practice. This study fills that gap by proposing a realistic model of criminal liability that aligns with national criminal law principles while accommodating the increasingly autonomous capabilities of AI. Based on these considerations, this study aims to:

1) Analyze the Indonesian criminal law framework concerning liability for actions involving Artificial Intelligence, whether as an auxiliary tool or as an indirect perpetrator;
2) Identify weaknesses and gaps in existing provisions within the Criminal Code, the Electronic Information and Transactions Law, and related regulations in addressing AI developments; and
3) Examine the relevance and potential applicability of alternative liability models—such as vicarious liability and strict liability—in the context of AI.

2. RESEARCH METHODOLOGY

This study employs a normative legal research approach, focusing on the analysis of positive legal norms, criminal law principles, and legal doctrines relevant to the issue of criminal liability for Artificial Intelligence (AI) in Indonesia. This approach was selected because the topic is closely linked to the existing legal vacuum and the need to formulate a criminal liability model consistent with national criminal law principles. The research adopts a descriptive-analytical doctrinal method, incorporating three main approaches: (1) a statutory approach, examining the Criminal Code, the Electronic Information and Transactions Law, and AI-related regulations; (2) a conceptual approach, analyzing the doctrines of *mens rea*, *actus reus*, vicarious liability, and strict liability; and (3) a comparative approach, exploring models of AI criminal liability in jurisdictions such as the European Union, the United States, Japan, and Singapore.

The study relies exclusively on secondary data, comprising: primary legal materials (national laws and regulations, international treaties, supranational regulations, and

[13] Ardi Dwi Setiawan and Indung Wijayanto, "Tinjauan Yuridis Pertanggungjawaban Pidana Dalam Tindak Pidana Yang Melibatkan Artificial Intelligence," *Yustisi: Jurnal Hukum Dan Hukum Islam* 12, no. 2 (2025): 174–187, https://doi.org/10.32832/yustisi.v12i2.19535.

court decisions pertaining to AI); secondary legal materials (academic literature, peer-reviewed journal articles, reports from international institutions, and conference proceedings); and tertiary legal materials (legal dictionaries, encyclopedias, and legal indexes). Data collection was conducted through an extensive literature review of international and national academic databases, alongside the examination of legal documents, including statutory instruments, minutes of parliamentary proceedings, and government reports on AI developments.

Data were analyzed using a normative qualitative method through several stages: inventory and classification of legal materials; legal interpretation employing grammatical, systematic, and teleological approaches; comparative analysis across jurisdictions; and normative synthesis to formulate an AI criminal liability model applicable in Indonesia. The validity of the findings was ensured through source triangulation, peer review of literature, and legal justification, thereby guaranteeing that the analysis aligns with established legal principles.

3. RESEARCH RESULT AND DISCUSSION

3.1. Indonesian Criminal Law Framework on Liability for Acts Involving Artificial Intelligence

This study examines the Indonesian criminal law framework governing liability for acts involving Artificial Intelligence (AI), both when AI functions as an assistive tool and when it operates as an indirect actor. Based on an analysis of primary, secondary, and tertiary legal materials, it is evident that Indonesian criminal law does not specifically recognize AI as an entity capable of bearing criminal liability. The Criminal Code (Law No. 1 of 2023) and the Electronic Information and Transactions Law (UU ITE) contain general provisions applicable to unlawful acts involving technology; however, they lack explicit mechanisms for assigning liability when the immediate perpetrator is an autonomous system.

Findings from this study indicate that the principle of *geen straf zonder schuld* ("no punishment without fault") remains a fundamental obstacle to positioning AI as a subject of criminal law. This is due to AI's inability to possess *mens rea*, or the conscious intent required under conventional criminal law. The concept of fault—central to this principle—cannot be attributed to non-human entities that lack free will or the moral capacity to discern right from wrong. Strict adherence to this principle therefore renders it difficult to prosecute AI as a direct perpetrator of criminal acts.

The research further reveals that, in AI-related crimes, criminal liability is generally directed toward the human or legal entity that controls, develops, or benefits from the AI's actions. This approach aligns with the doctrines of vicarious liability and corporate criminal liability, whereby the party exercising control or deriving benefit is held responsible. While this model is considered more realistic and consistent with

Indonesia's prevailing legal framework, it nonetheless requires normative and procedural reinforcement.

In cases where AI serves solely as an instrumental tool, the existing legal framework is relatively adequate to prosecute human perpetrators who employ AI to commit offenses. However, when AI operates as an indirect perpetrator or functions autonomously beyond human control, the applicable legal norms remain vague and lack a definitive basis. This normative gap creates potential legal loopholes that could be exploited to evade criminal responsibility.

The study also finds that Indonesia's positive law does not yet provide mechanisms for algorithm auditability or explainable AI. The absence of such legal instruments poses significant challenges in establishing causality in AI-related offenses. Without the means to audit or transparently explain AI decision-making processes, law enforcement agencies face substantial difficulties in proving culpability and demonstrating the causal link between AI actions and their legal consequences. This underscores the urgency of comprehensive legal reforms to address the evolving nature of AI technology. A comparative review of regulatory developments in the European Union, Japan, and Singapore shows that these jurisdictions have begun formulating specific legal frameworks for high-risk AI, including requirements for algorithm transparency and the application of strict liability in certain sectors, such as autonomous transportation.

This study finds that Indonesia's criminal law framework remains largely reactive to advancements in Artificial Intelligence (AI) technology. This reactive stance contributes to legal uncertainty, particularly in cases involving autonomous AI systems capable of producing criminal outcomes. Current regulations fail to address AI's distinctive characteristics—such as its capacity for independent learning and decision-making without direct human intervention—thereby creating a potential legal vacuum that undermines victim protection and the pursuit of justice.

The second finding underscores the centrality of the culpability principle in applying criminal law to AI. The absence of *mens rea*, or moral consciousness, in AI systems renders traditional fault-based doctrines inapplicable. This gap necessitates the adaptation of existing legal concepts or the development of new principles capable of encompassing non-human entities implicated in criminal acts.

Third, the research highlights that alternative liability models—such as vicarious liability, strict liability, and corporate criminal liability—are more practical than recognizing AI as a subject of criminal law. These models shift responsibility to individuals or legal entities that control, develop, or benefit from AI. This approach is deemed more realistic, as it places accountability on actors with the legal and moral capacity to be held liable.

The fourth finding addresses the evidentiary challenges posed by the "black box" phenomenon in AI. The opacity of algorithms and AI decision-making processes impedes the establishment of causality in criminal proceedings. In the absence of mechanisms for algorithm auditability or explainable AI, law enforcement faces substantial difficulties in tracing the causal link between AI behavior and criminal acts, thereby undermining the effectiveness of enforcement measures.

Finally, the study identifies the lack of cross-jurisdictional cooperation in prosecuting AI-related crimes as a significant weakness. Given AI's capacity to operate across national borders, the absence of effective international collaboration limits legal protection for victims. This highlights the need for a transnational legal framework to anticipate and address AI-related criminality comprehensively.

These findings are consistent with the positions of Hibatulloh, Pagallo, Sofian, and Wahyudi BR, who argue that AI can act as a perpetrator, victim, or instrument of crime, and that accountability should rest with the party exercising control over the AI.[14] They also align with Muladi and Arief, who emphasize fault as a prerequisite for criminal prosecution, thereby excluding the possibility of holding AI directly liable.[15]

In contrast to studies such as Walton et al., which focus primarily on the technical challenges of proof, this research identifies the absence of clear legal norms as an equally pressing obstacle.[16] Moreover, while international scholarship has explored the concept of granting AI the status of an "electronic person," this study concludes that, in the Indonesian context, such recognition is premature given the current limitations in regulatory readiness and legal infrastructure.

The findings suggest that applying Indonesian criminal law to AI-related cases requires adapting legal doctrines while preserving foundational principles such as legality and fault. The vicarious liability model may serve as an interim solution, ensuring that those operating or benefiting from AI bear criminal responsibility.

Furthermore, the application of strict liability in high-risk sectors—such as autonomous transportation and AI-driven healthcare—can enhance public protection by eliminating the need to prove fault. However, such implementation must be accompanied by robust technological oversight mechanisms, including mandatory algorithm audits. From a law enforcement standpoint, technical barriers such as AI's "black box" phenomenon must be addressed through regulations requiring algorithmic transparency and explainability. This approach aligns with emerging international

[14] Hibatulloh, "Upaya Penegakan Hukum Terhadap AI (Artificial Intelligence) Sebagai Subjek Hukum Pidana Dalam Perspektif Kriminologi"; Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts*, Law, Governance and Technology Series (Dordrecht: Springer, 2013), https://doi.org/10.1007/978-94-007-6564-1; Sofian, "Konsepsi Subjek Hukum Dan Pertanggungjawaban Pidana Artificial Intellegence"; Wahyudi BR, "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI."

[15] Muladi Muladi and Barda Nawawi Arief, *Teori-Teori Dan Kebijakan Pidana* (Bandung: Alumni, 2010).

[16] Douglas Walton, Giovanni Sartor, and Fabrizio Macagno, "An Argumentation Framework for Contested Cases of Statutory Interpretation," *Artificial Intelligence and Law* 24, no. 1 (2016): 51–91, https://doi.org/10.1007/s10506-016-9179-0.

standards, in which algorithmic accountability constitutes a core element of high-risk AI regulation. Accordingly, this study concludes that:

1) AI-related provisions in Indonesian criminal law remain general in scope and are inadequate for addressing specific issues when AI operates as an indirect actor.
2) Adaptation of criminal law doctrines is essential, particularly through the broader application of vicarious liability and strict liability, to close existing accountability gaps.
3) Strengthening technical capacities and fostering international cooperation are critical to effective enforcement, given the transnational reach and algorithmic complexity of AI systems.
4) The development of sector-specific AI regulations is an urgent priority, especially in domains that present elevated risks to public safety and data security.

3.2. Weaknesses and Gaps in the Criminal Code, the Electronic Information and Transactions Law, and Related Regulations Concerning the Development of Artificial Intelligence

This study seeks to identify weaknesses and gaps in the Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and other related regulations with respect to the development of Artificial Intelligence (AI) in Indonesia. It further examines enforcement challenges—including technical barriers, jurisdictional constraints, and institutional capacity—to formulate recommendations for strengthening the regulatory framework in anticipation of future legal needs.

An analysis of the Criminal Code, the ITE Law, and several sectoral regulations reveals that Indonesia's current legal framework remains firmly rooted in a human-centric offender paradigm. The Criminal Code adheres to the principle of *geen straf zonder schuld* ("no crime without fault"), which requires the perpetrator to possess moral awareness (mens rea). In the case of AI, the absence of such awareness precludes the direct attribution of criminal liability. Although the ITE Law addresses unlawful acts in the electronic domain, it does not explicitly account for the autonomous or adaptive characteristics of AI. Similarly, sector-specific regulations—such as those governing traffic, healthcare, and personal data protection—provide only limited provisions for AI-specific legal responsibilities.

The research identifies three prevailing patterns of liability: (1) user or operator liability, where individuals who operate AI systems negligently or unlawfully are held responsible; (2) manufacturer or developer liability, for design defects or negligent system maintenance; and (3) corporate liability, where ownership or beneficial use of AI invokes the doctrine of corporate criminal liability. However, these approaches face substantial evidentiary challenges due to the "black box" nature of AI algorithms, which obstruct traceability and transparency in decision-making processes.

Five principal findings emerge from this study. First, the Indonesian criminal law framework remains reactive to AI developments, failing to provide legal certainty in cases involving autonomous AI with criminal consequences. Second, the principle of fault (culpability) presents a fundamental barrier in addressing non-human entities, necessitating doctrinal adaptation. Third, alternative liability models—such as vicarious liability, strict liability, and corporate criminal liability—are more pragmatic than treating AI as a direct perpetrator. Fourth, technical limitations in evidentiary processes, particularly the opacity of AI algorithms, significantly impede the establishment of causality in criminal proceedings. Fifth, the absence of a cross-jurisdictional law enforcement framework for AI-related crimes undermines victim protection.

These results are consistent with the findings of Astiti, Kan, and Setyawan, who argue that classical criminal law doctrines are inadequate for directly prosecuting AI entities given the absence of *mens rea*.[17] They also align with Balasubramaniam et al., who stress the necessity of incorporating explainable AI principles and algorithm auditability into law enforcement mechanisms.[18] However, unlike prior research that primarily addresses AI from data protection and ethical perspectives, this study emphasizes the criminal law dimension, highlighting normative gaps within the Criminal Code and the ITE Law and their intersection with international jurisdictional issues.

Moreover, this research advances the existing discourse by integrating a multi-layered liability framework—assigning responsibility concurrently to users, producers, and corporations—which remains underexplored in the Indonesian legal context. Such an approach is particularly relevant given the complex, multi-actor structure of the AI ecosystem and the numerous stakeholders involved in the technology's lifecycle.

Table 1.
Challenges and Strategic Solutions for Addressing Criminal Liability of Artificial Intelligence (AI) in Indonesia

Aspect	Challenge Description	Strategic Solution
Technical – Algorithmic Transparency (Black Box)	AI systems operate using complex algorithms that are often opaque and difficult to audit, creating significant challenges in proving causality and establishing fault.	Mandate algorithm audits (algorithm auditability) and incorporate the principle of *explainable AI* into binding regulations.

[17] Astiti, "Strict Liability of Artificial Intelligence: Pertanggungjawaban Kepada Pengatur AI Ataukah AI Yang Diberikan Beban Pertanggungjawaban?"; Celal Hakan Kan, "Criminal Liability of Artificial Intelligence from the Perspective of Criminal Law: An Evaluation in the Context of the General Theory of Crime and Fundamental Principles," *International Journal Of Eurasia Social Sciences* 15, no. 55 (2024): 276–313, https://doi.org/10.35826/ijoess.4434; Setyawan, "Prospek Pengaturan Kecerdasan Buatan Sebagai Subjek Hukum Pidana Dan Model Pertanggungjawabannya."

[18] Nagadivya Balasubramaniam et al., "Transparency and Explainability of AI Systems: From Ethical Guidelines to Requirements," *Information and Software Technology* 159 (2023): 1–15, https://doi.org/10.1016/j.infsof.2023.107197.

Aspect	Challenge Description	Strategic Solution
Legal – Absence of *Mens Rea*	AI lacks consciousness and intent, making it incompatible with the traditional principle of *nulla poena sine culpa* ("no crime without fault").	Develop alternative liability frameworks, such as vicarious liability, strict liability, or corporate criminal liability.
Cross-Border Jurisdiction	AI can be controlled remotely from foreign jurisdictions, with data and servers distributed across multiple countries, complicating enforcement.	Enhance international cooperation, establish extradition treaties, and implement mutual legal assistance agreements specifically addressing AI-related crimes.
Law Enforcement Capacity	Limited technical expertise among law enforcement personnel in understanding and analyzing AI-generated digital evidence.	Provide intensive digital forensics training, foster collaboration with technology experts, and create a dedicated investigative unit for AI-related crimes.
Data Leakage & Privacy	AI's ability to process vast amounts of personal data increases the risk of privacy violations.	Enforce the Personal Data Protection Law rigorously and require AI developers to obtain data security certifications.
Potential Abuse of AI	AI can be exploited for malicious purposes such as deepfakes, automated phishing, and other cybercrimes.	Establish a legally binding list of prohibited AI applications and implement strict oversight mechanisms for high-risk AI systems.

The findings indicate that the primary weakness of Indonesia's regulatory framework lies not only in the absence of explicit provisions on Artificial Intelligence (AI) but also in the incompatibility between prevailing criminal law doctrines and the autonomous, adaptive nature of AI. The principle of *geen straf zonder schuld* ("no punishment without fault"), a cornerstone of criminal law, presupposes free will and moral awareness—attributes that AI inherently lacks. Consequently, liability should be assigned to those who control and derive benefit from AI, consistent with the principle of risk allocation in modern law.

The "black box" phenomenon in AI compounds these challenges by obscuring critical information about decision-making processes. In the absence of legally mandated algorithmic audit mechanisms and the adoption of explainable AI principles, law enforcement agencies will face substantial obstacles in establishing causality and culpability. This is not solely a technical limitation; it also implicates fundamental legal rights, including a defendant's right to be informed of the charges and evidence against them, as well as a victim's right to justice.

The lack of cross-jurisdictional cooperation presents further practical difficulties. Given AI's capacity to operate globally, its servers and supporting infrastructure are often located outside the jurisdiction where criminal conduct occurs. Without a dedicated mutual legal assistance framework for AI-related offenses, enforcement efforts—particularly in cases of AI-enabled cybercrimes such as deepfake fraud, automated phishing, and digital market manipulation—will be significantly hindered.

This study confirms that the Criminal Code (KUHP), the Electronic Information and Transactions Law (ITE Law), and related regulations are insufficient to address the normative and technical challenges posed by AI. The current legal framework is reactive rather than anticipatory and fails to provide legal certainty in cases involving autonomous AI. Traditional doctrines requiring *mens rea* must be adapted through the incorporation of alternative, layered liability models, including vicarious liability, strict liability, and corporate criminal liability.

Comprehensive regulatory reforms are urgently required, encompassing mandatory algorithm audits, the integration of explainable AI principles, provisions for cross-jurisdictional liability, and enhanced capacity-building in digital forensics for law enforcement personnel. Without these measures, regulatory gaps will persist, enabling offenders to evade accountability. Accordingly, the development of a robust, adaptive, and forward-looking regulatory framework for AI is imperative to ensure that Indonesia's legal system remains responsive in the era of autonomous technology.

3.3. Relevance and Potential Application of Alternative Liability Models, Such as Vicarious Liability and Strict Liability, in the Context of AI

This study examines the relevance and potential application of alternative liability models—particularly vicarious liability and strict liability—in the context of the use and operation of Artificial Intelligence (AI) in Indonesia. The inquiry is prompted by the absence of explicit statutory provisions on AI, with current legal practice relying on the interpretation of general criminal norms contained in the Criminal Code (KUHP), the Electronic Information and Transactions Law (ITE Law), the Personal Data Protection Law, and the Road Traffic and Transportation Law. The objective is to provide a comprehensive analysis of how these alternative liability models can be integrated into the national legal framework to ensure legal certainty, safeguard public interests, and promote accountability among AI-related businesses and developers.

The findings indicate that Indonesia's legal system currently lacks a dedicated instrument establishing criminal liability for damages or offenses caused by AI. Analysis of domestic legal documents and international case studies reveals the following:

1) Vicarious Liability has potential applicability where AI functions within a legal relationship in which a developer, operator, or corporation acts as the "principal" and the AI system functions as the "agent." Under this model, criminal or civil liability is imposed on the party exercising control and authority over the AI, even when the unlawful act is performed autonomously by the AI system.

2) Strict Liability is particularly relevant in contexts where AI is categorized as high-risk technology, such as autonomous vehicles, AI-based medical diagnostic systems, or biometric data processing algorithms. This model imposes liability without requiring proof of fault, thereby expediting dispute resolution and providing victims with greater legal certainty.
3) Existing legislation—the Criminal Code, the ITE Law, the Personal Data Protection Law, and the Road Traffic and Transportation Law—remains fragmented and requires adaptation to address AI-specific characteristics. For instance, while the ITE Law may be applied to prosecute AI-driven data breaches, it does not address the criminal liability of parties operating autonomous AI.
4) Comparative practices, such as the European Union's AI Act and Product Liability Directive, illustrate that combining strict liability for high-risk activities with vicarious liability for employment or contractual relationships can provide a balanced model that fosters both innovation and legal protection.

The principal conclusion of this study is that the application of vicarious liability and strict liability offers a realistic and effective means of addressing the legal vacuum surrounding AI-related harm or criminal conduct in Indonesia. Vicarious liability serves to protect victims in situations where AI operates within an employment or contractual framework under clear instructions, while strict liability ensures maximum protection in high-risk AI applications that operate autonomously.

These findings are consistent with prior scholarship, including Astiti, Pagallo, and Putri et al., which advocate the use of vicarious liability to secure the accountability of AI controllers and strict liability for technologies with significant potential for harm.[19] However, this study contributes a uniquely Indonesian perspective, emphasizing the reliance on general statutory instruments—such as the KUHP and the ITE Law—and the absence of dedicated AI legislation. Unlike European jurisdictions, which are moving toward harmonized AI regulations, Indonesia remains in the preliminary stages of policy development; thus, the recommendations in this study prioritize the adaptation of existing laws as an interim measure prior to the enactment of specialized AI legislation.

From a legal standpoint, the findings indicate that the adoption of vicarious liability and strict liability is not only normatively viable but also urgently needed to address the legal challenges posed by the distinctive characteristics of AI—namely, decision-making autonomy, behavioral unpredictability, and the inherent difficulty of establishing "intent" or *mens rea*. In the absence of these alternative liability models, victims of AI-

[19] Astiti, "Strict Liability of Artificial Intelligence: Pertanggungjawaban Kepada Pengatur AI Ataukah AI Yang Diberikan Beban Pertanggungjawaban?"; Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts*; Putri et al., "Thinking the Future Potential of Artificial Intelligence in Law Enforcement."

related harm are likely to face substantial evidentiary obstacles, particularly in proving fault on the part of a human perpetrator.

The application of strict liability to high-risk AI technologies would compel businesses and AI developers to comply with rigorous security standards and conduct regular audit procedures, as highlighted in this study's findings. Conversely, implementing vicarious liability would incentivize companies to closely monitor and control the use of AI by employees or third parties operating under contractual arrangements.

The results underscore the need for two strategic measures in Indonesia. First, existing laws—including the Electronic Information and Transactions Law (ITE Law), the Personal Data Protection Law (PDP Law), and the Road Traffic and Transportation Law (LLAJ Law)—should be amended to incorporate explicit provisions on AI-related liability under both vicarious and strict liability frameworks. Second, a dedicated AI statute should be enacted, establishing clear security requirements, mandatory audit mechanisms, and accountability procedures, particularly for high-risk AI systems. Adopting this alternative liability framework would help Indonesia avoid a legal vacuum that undermines victim protection, while ensuring that AI innovation continues within a well-defined and equitable legal structure. In the broader context of technological globalization, this step would also align Indonesia with jurisdictions that have already enacted comprehensive AI legislation.

4. CONCLUSION

This study seeks to analyze Indonesia's criminal law framework governing liability for actions involving Artificial Intelligence (AI), both when AI functions as an assistive tool and when it operates as an indirect perpetrator. It further aims to identify weaknesses and regulatory gaps in the Criminal Code, the Electronic Information and Transactions Law (ITE Law), and related legislation, as well as to assess the relevance of adopting alternative liability models—particularly vicarious liability and strict liability—in the context of AI. The findings indicate that the current Indonesian criminal law framework remains centered on the concept of a human actor (natural person), rendering it ill-suited to address the autonomous and self-learning characteristics of AI. Neither the Criminal Code nor the ITE Law explicitly provides mechanisms for attributing fault in cases where AI acts without direct human instruction. This gap risks creating legal uncertainty in establishing key elements such as *mens rea* and causation.

Further analysis confirms that alternative liability models offer potential solutions. Vicarious liability can be applied to assign criminal responsibility to parties exercising control over or deriving benefit from AI, while strict liability is particularly relevant for high-risk AI applications, ensuring that victims are not burdened with the challenge of proving fault. These findings offer practical guidance for policymakers and law enforcement authorities in formulating legal norms that are responsive to technological change. The principal limitation of this research lies in its normative–conceptual scope, as it does not incorporate empirical testing through concrete case studies within Indonesia. Consequently, future studies should integrate empirical methodologies, including case simulations and comparative analyses with jurisdictions that have already implemented AI-specific regulations. As a policy recommendation, revisions to the Criminal Code and the ITE Law—or the development of dedicated AI legislation incorporating a hybrid accountability framework, ensuring robust victim protection, and fostering responsible innovation—are urgently needed.

REFERENCES

Journals

Astiti, Ni Made Yordha Ayu. "Strict Liability of Artificial Intelligence: Pertanggungjawaban Kepada Pengatur AI Ataukah AI Yang Diberikan Beban Pertanggungjawaban?" *Jurnal Magister Hukum Udayana* 12, no. 4 (2023): 962–80. https://doi.org/10.24843/JMHU.2023.v12.i04.p14.

Balasubramaniam, Nagadivya, Marjo Kauppinen, Antti Rannisto, Kari Hiekkanen, and Sari Kujala. "Transparency and Explainability of AI Systems: From Ethical Guidelines to Requirements." *Information and Software Technology* 159 (2023): 1–15. https://doi.org/10.1016/j.infsof.2023.107197.

Hibatulloh, Beryl Helga Fredella. "Upaya Penegakan Hukum Terhadap AI (Artificial Intelligence) Sebagai Subjek Hukum Pidana Dalam Perspektif Kriminologi." *Taruna Law: Journal of Law and Syariah* 3, no. 1 (2025): 87–98. https://doi.org/10.54298/tarunalaw.v3i01.300.

Kan, Celal Hakan. "Criminal Liability of Artificial Intelligence from the Perspective of Criminal Law: An Evaluation in the Context of the General Theory of Crime and Fundamental Principles." *International Journal Of Eurasia Social Sciences* 15, no. 55 (2024): 276–313. https://doi.org/10.35826/ijoess.4434.

Maharani, Bondan Ayu, Hasnaa Amelia Rahajeng, Triana Triana, and Zahra Dwi Arianti. "Perlindungan Hukum Masyarakat Dari Dampak Negatif Penggunaan AI." *Media Hukum Indonesia* 3, no. 2 (2025): 666–73. https://ojs.daarulhuda.or.id/index.php/MHI/article/view/1939.

Nasman, Nasman, Pudji Astuti, and Dita Perwitasari. "Etika Dan Pertanggungjawaban Penggunaan Artificial Intelengence Di Indonesia." *Jurnal Hukum Lex Generalis* 5, no. 10 (2024): 1–15. https://ojs.rewangrencang.com/index.php/JHLG/article/view/622.

Putri, Feby Milenia Yahya Krisna, Hary Abdul Hakim, Chrisna Bagus Edhita Praja, and Gerald Espares. "Thinking the Future Potential of Artificial Intelligence in Law Enforcement." *Perspektif Hukum* 24, no. 2 (2024): 269–294.

https://doi.org/10.30649/ph.v24i2.319.

Rondonuwu, Natalie Tresye, Donna Okthalia Setiabudhi, and Carlo A Gerungan. "Pengaturan Penggunaan Kecerdasan Buatan Dalam Tugas Profesional Hakim Di Indonesia." *Lex Privatum* 15, no. 2 (2025): 1–12. https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/60761.

Setiawan, Ardi Dwi, and Indung Wijayanto. "Tinjauan Yuridis Pertanggungjawaban Pidana Dalam Tindak Pidana Yang Melibatkan Artificial Intelligence." *Yustisi: Jurnal Hukum Dan Hukum Islam* 12, no. 2 (2025): 174–187. https://doi.org/10.32832/yustisi.v12i2.19535.

Setyawan, Vincentius Patria. "Prospek Pengaturan Kecerdasan Buatan Sebagai Subjek Hukum Pidana Dan Model Pertanggungjawabannya." *Sultan Adam: Jurnal Hukum Dan Sosial* 3, no. 1 (2025): 115–122. https://doi.org/10.71456/sultan.v3i1.1214.

Sofian, Ahmad. "Konsepsi Subjek Hukum Dan Pertanggungjawaban Pidana Artificial Intellegence." *Halu Oleo Law Review* 9, no. 1 (2025): 13–26. https://doi.org/10.33561/holrev.v9i1.129.

Sulistio, Faizin, and Aizahra Daffa Salsabilla. "Pertanggungjawaban Pada Tindak Pidana Yang Dilakukan Agen Otonom Artificial Intelegence." *Unes Law Review* 6, no. 2 (2023): 5479–90. https://doi.org/10.31933/unesrev.v6i2.1209.

Walton, Douglas, Giovanni Sartor, and Fabrizio Macagno. "An Argumentation Framework for Contested Cases of Statutory Interpretation." *Artificial Intelligence and Law* 24, no. 1 (2016): 51–91. https://doi.org/10.1007/s10506-016-9179-0.

Wahyudi BR. "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI." *Innovative: Journal Of Social Science Research* 5, no. 1 (2025): 3436–3450. https://doi.org/10.31004/innovative.v5i1.17519.

Proceedings

Ikawati, Linda, Sulaiman Sulaiman, and Muhammad Fahri Huseini. "Masa Depan Penegakan Hukum Indonesia: Sistem Peradilan Pidana Berbasis Kecerdasan Buatan (AI)." In *Prosiding Seminar Nasional Ilmu Hukum*, 1–18. Pemalang: Asosiasi Peneliti dan Pengajar Ilmu Hukum Indonesia, 2024. https://doi.org/10.62383/prosemnashuk.v1i1.19.

Books

Muladi, Muladi, and Barda Nawawi Arief. *Teori-Teori Dan Kebijakan Pidana*. Bandung: Alumni, 2010.

Pagallo, Ugo. *The Laws of Robots: Crimes, Contracts, and Torts*. Law, Governance and Technology Series. Dordrecht: Springer, 2013. https://doi.org/10.1007/978-94-007-6564-1.

Working Papers

The European Parliament. "European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics." Strasbourg: The European Parliament, 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html.