Journal of International Islamic Law, Human Rights and Public Policy
(JISHUP Journal) | ISSN(e): 3031-2280
Website https://jishup.org/index.php/ojs/index | Volumes 4 No. 2 (2026)

CRIMINAL RESPONSIBILITY FOR CRIMES BASED ONARTIFICIAL INTELLIGENCE FROM THE PERSPECTIVE OF INDONESIAN CRIMINAL LAW

Hendri Saputra Manalu[1], Rahmayanti[2], Tita Rosmawati[3]
Universitas Pembangunan Panca Budi, Medan
Email correspondence: **rahmayanti@dosen.pancabudi.ac.id**

Received: 02/04/2026 | **Revised:** 11/04/2026 | **Accepted:** 01/05/2026 | **Published:**02/06/2026

Abstract

The rapid development of Artificial Intelligence (AI) technology has complex legal implications, particularly in the field of criminal law. Crimes committed using AI systems such as deepfakes, automated cyber attacks, algorithm-based fraud, and data manipulation raises fundamental questions about who should be held criminally responsible. This study aims to analyze the concept of criminal liability for AI-based crimes within the existing Indonesian criminal law framework and identify existing legal gaps (leemten in het recht). The research method used is normative juridical with a statute approach, a conceptual approach, and a comparative approach. The results show that the Criminal Code (KUHP) and Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE) have not been able to optimally address criminal liability for crimes mediated by autonomous AI systems. Comprehensive regulatory reform is needed, including the determination of new legal subjects, the implementation of adapted strict liability and vicarious liability doctrines, and the establishment of a specific legal framework related to AI. This study recommends the drafting of an Artificial Intelligence Bill that explicitly regulates aspects of criminal liability in the AI ecosystem.

Keywords:Artificial Intelligence; Indonesian Criminal Law; Cybercrime; Criminal Liability; AI Regulation

INTRODUCTION

The fourth industrial revolution, marked by the proliferation of Artificial Intelligence (AI) technology, has fundamentally changed the way humans interact, work, and even commit crimes. AI is no longer a simple tool; it has evolved into an autonomous system capable of learning, making decisions, and acting independently without direct human intervention. This development creates a new dimension in the dynamics of modern crime that has not yet been fully anticipated by existing criminal justice systems. Indonesia, as the country with the fourth largest internet user population in the world, faces high exposure to AI-based crimes. The deepfake phenomenon video and audio manipulation using machine learning technology AI has been used to create non-consensual pornography, identity fraud, and political disinformation. Cyberattacks using automated AI, such as personalized phishing, adaptive malware, and natural language processing-based social engineering, are becoming increasingly prevalent and difficult to detect. Furthermore, cases of financial fraud using AI algorithms to manipulate capital markets and banking systems are beginning to surface.

Amid these developments, a fundamental question arises that remains unsatisfactorily unanswered by Indonesian criminal law: Who should be held criminally responsible when an AI system autonomously performs actions that objectively constitute a crime? Should the AI system developer, owner, operator, user, or even the AI system itself be held responsible? Indonesia's current criminal law framework, based on the Dutch colonial Criminal Code (KUHP) and Law No. 19 of 2016 concerning Electronic Information and Transactions (UU ITE), is built on the foundation that perpetrators of crimes are human beings with free will (mens rea) and physical capacity to commit acts (actus reus). The basic principle of criminal responsibility namely no crime without error (geen straf zonder schuld) face existential challenges when dealing with AI systems that lack consciousness, intention, or moral capacity.

The urgency of this research is increasingly relevant given that Law No. 1 of 2023 concerning the National Criminal Code is already in effect, specifically addressing the dimensions of criminal liability in the context of AI-

based crimes. Meanwhile, several jurisdictions, such as the European Union, have gone a step further by passing the EU Artificial Intelligence Act in 2024, the world's first comprehensive AI regulation. Based on the above background, this study aims to: (1) analyze the concept of criminal liability for AI-based crimes in Indonesian criminal law; (2) identify legal gaps in existing regulations; (3) formulate recommendations for comprehensive and implementable legal reforms.

LITERATURE REVIEW

1. The Concept of Criminal Responsibility in Indonesian Criminal Law

Criminal liability (toerekeningsvatbaarheid) is the core of the entire criminal law system. Moeljatno (2008) defines criminal liability as a person's ability to bear the legal consequences of a criminal act. This liability requires three main elements: the ability to be responsible (toerekeningsvatbaarheid), the existence of fault (schuld) in the form of intent (dolus/opzet) or negligence (culpa), and the absence of an excuse to eliminate the fault (schulduitsluitingsgrond).

Roeslan Saleh (1983) emphasized that the principle of fault is the main foundation of criminal responsibility, which is reflected in the historical adage actus non facit reum nisi mens sit rea An act does not make a person guilty unless his or her mind is also guilty. Schaffmeister, Keijzer, and Sutorius (2011) classify forms of wrongdoing in Indonesian criminal law into two main categories: intent (opzet), which includes intent as a goal, certainty, and possibility; and negligence (culpa), which includes conscious and unconscious negligence.

The subject of criminal law in the Indonesian Criminal Code has historically only recognized humans (natural persons) as perpetrators. However, with the rise of corporate crime, Article 46 of the Electronic Information and Transactions Law and various sectoral laws and regulations have recognized corporations as subjects of criminal law. The question now is, can AI systems be categorized as a new legal subject in criminal law?

2. Artificial Intelligence-Based Crime Classification

The study of AI crime, or crimes that use or target AI systems, has grown rapidly in the past decade. Caldwell et al. (2020) classify AI crimes into three categories:

a. AI as an instrument of crime (AI-assisted crimes), where humans use AI to commit crimes more effectively;
b. AI as a target of crime (crimes against AI), where the AI system itself becomes the object of attack; and
c. crimes committed autonomously by AI systems (autonomous AI crimes).

This third category is the most legally challenging. Floridi et al. (2018) proposed the concept of 'moral agency' in AI, which distinguishes between AI as a moral agent with the capacity to make ethical decisions and AI as a mere tool that merely carries out its programmer's instructions. In the context of criminal law, the question of whether AI can be treated as a responsible moral agent becomes crucial.

In Indonesia, the most relevant forms of AI-based crimes include:

a. deepfake pornographywhich violates morality and honor as regulated in Article 27 paragraph (1) of the ITE Law;
b. AI-based fraud (AI fraud) related to Article 28 paragraph (1) of the ITE Law and Article 378 of the Criminal Code;
c. automated cyber attacks relevant to Articles 30-33 of the ITE Law;
d. algorithmic manipulation of financial markets related to the Capital Markets Law; and
e. personal data breaches related to Law Number 27 of 2022 concerning Personal Data Protection.

3. Relevant Liability Doctrine

Several relevant criminal liability doctrines in the context of AI crime include: First, strict liability, which does not require proof of fault but rather requires proof of actus reus. Second, vicarious liability, which places responsibility on the party with control over the direct perpetrator. Third, the product liability doctrine, which places AI manufacturers or developers responsible for the harm caused by their products. Fourth, the natural-probable consequence doctrine, which emphasizes the foreseeability of harmful actions by AI systems. Turner (2019) in his book "Robot Rules: Regulating Artificial Intelligence" proposed the concept of "electronic personhood" for advanced AI systems, an idea that is in line with the 2017 European Parliament resolution. This concept, although controversial, offers an alternative solution to overcome the legal vacuum in AI criminal liability.

4. Comparative Law Studies

A comparative approach to AI regulation across jurisdictions provides valuable insights. The European Union, through the EU Artificial Intelligence Act (2024), adopted a risk-based approach that classifies AI systems into four risk levels with varying legal consequences. The United States developed a sectoral approach through various regulations such as the FTC Act, CFPB Guidance, and several state regulations. China, through the Regulation on Recommendation Algorithm Services (2022) and the Regulation on Generative AI Services (2023), adopted a more centralized and comprehensive regulatory approach. Singapore developed an AI Governance Framework that emphasizes the principles of accountability and transparency.

RESEARCH METHODS

This research uses a normative legal research approach, namely legal research conducted by examining library materials or secondary data as the basis for research by conducting searches of regulations and literature related to the problem being studied (Soekanto and Mamudji, 2001). This approach was chosen because this research aims to examine the rules or norms in positive law. This research combines three main approaches. First, a statutory approach is used to examine all laws and regulations related to criminal liability and cybercrime in Indonesia, including the Indonesian Criminal Code (KUHP), the Electronic Information and Transactions (ITE) Law, the 2023 National Criminal Code (KUHP), the Personal Data Protection Law, and related implementing regulations. Second, a conceptual approach is used to analyze relevant criminal law doctrines, the views of legal experts, and the development of legal thought regarding criminal liability in the context of technology. Third, a comparative approach is applied to compare legal regulations regarding AI crimes in several relevant jurisdictions, particularly the European Union, the United States, China, and Singapore.

The legal materials used consist of three categories. Primary legal materials include laws and regulations applicable in Indonesia, namely the Criminal Code (KUHP), Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE), Law Number 1 of 2023 concerning the National Criminal Code, Law Number 27 of 2022 concerning Personal Data Protection, and various related implementing regulations. Secondary legal materials include legal textbooks, national and international legal journals, research results, and opinions of legal experts. Tertiary legal materials include legal dictionaries, encyclopedias, and other supporting reference materials. The legal material collection technique was conducted through library research, which included searching for relevant laws and regulations, court decisions, legal doctrine, and scientific literature. The search was conducted through legal databases such as Westlaw, HeinOnline, Google Scholar, and the official Indonesian legal regulations repository (JDIH). The legal material analysis was conducted in a prescriptive-analytical manner, employing grammatical, systematic, historical, and teleological interpretation techniques to produce a coherent legal proposition.

RESULTS AND DISCUSSION

1. **Analysis of Indonesia's Criminal Law Framework for AI-Based Crimes**

The research findings indicate that Indonesia's criminal law framework faces at least five fundamental challenges in addressing AI-based crimes. The first challenge is the unmet mens rea requirement. The Criminal Code (KUHP) and the ITE Law require malicious intent (mens rea) from the perpetrator as an element of a crime. AI systems, as non-biological entities, lack will, intent, or consciousness. When an autonomous AI system performs an objectively harmful action, there is no legal entity directly possessing mens rea that can be held accountable.

The second challenge is the issue of perpetrator identification (actus reus attribution). In the complex architecture of modern AI systems, involving multiple layers of developers, platform providers, operators, and end users, determining who legally committed the actus reus becomes extremely complex. Conventional criminal law principles of causality struggle to identify an adequate causal link between human actions and the final outcome of an autonomous AI system's decision-making process.

The third challenge relates to legal subjects. AI systems are not considered legal subjects (rechtssubject) in the Indonesian legal system. The Indonesian Criminal Code (KUHP) recognizes humans and corporations as subjects of criminal law, but it does not specifically accommodate AI as an entity that can be prosecuted or used as a basis for liability for other parties.

The fourth challenge is jurisdictional issues. AI systems are often developed in one country, operated from another, and cause harm in a third country. The principle of territoriality in Indonesian criminal law (Articles 2-8 of the Indonesian Criminal Code) does not adequately address the transnational nature of AI-based crimes.
The fifth challenge is the technical problem of proof. The decision-making process of AI systems is opaque (the black box problem), making it difficult to legally prove how and why an AI system makes certain decisions that lead to harm. This creates epistemological difficulties in criminal evidence, which requires a standard beyond reasonable doubt.

2. **Mapping of Existing Regulations and Legal Gaps**

An analysis of the 2016 ITE Law shows that while it specifically regulates cybercrimes, its provisions are designed with the assumption that the perpetrators are humans using computer systems as tools. Article 30, which regulates illegal access, Article 32 on system disruption, and Article 33 on cyberattacks, all use the phrase "any person intentionally," which requires a human subject with conscious intent.

Law No. 1 of 2023 concerning the National Criminal Code, which will come into effect in 2026, introduces several progressive provisions, including more comprehensive provisions on corporate liability. However, the National Criminal Code does not yet explicitly address liability in the context of autonomous AI systems. Articles relating to continuing acts, participation (deelneming), and corporate crimes can serve as a basis for analogy, but analogies in criminal law are prohibited in principle (lex certa and lex stricta).

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is the most recent regulation most relevant to the AI ecosystem. The PDP Law regulates the obligations of data controllers and processors, including criminal sanctions for violations. Article 67 of the PDP Law stipulates criminal penalties of up to six years' imprisonment and fines of up to IDR 6 billion. However, the PDP Law focuses on data protection and does not comprehensively regulate criminal liability for losses caused by AI systems processing data.

3. **Applicable Criminal Liability Model**

Based on comparative and doctrinal analysis, this study identifies several models of criminal liability that can be adapted in the Indonesian legal context.The first model is Developer Liability. This model imposes criminal liability on AI system developers based on the principle of product liability adapted to the criminal realm. If an AI system is designed with a design flaw that can reasonably be predicted to result in harm, the developer can be held liable under the theory of culpa in eligendo or culpa in instruendo. The challenge with this model is proving that the developer had knowledge, or should have had knowledge, of the potential harm of the AI system they developed.

The second model is Operator Liability. The party operating the AI system both individuals and corporations can be held liable based on the principles of vicarious liability and factual control over the system. If the operator has the ability to monitor, intervene, or stop the operation of the AI system but fails to do so, negligence-based criminal liability may apply. This model is most consistent with existing criminal law principles.

The third model is User Liability. In cases where a user actively misuses an AI system for criminal purposes, criminal liability is relatively easy to identify because the mens rea lies with the user. However, challenges arise when the AI system performs actions outside the user's instructions that result in harm to a third party.

The fourth model is Layered Liability. Given the complexity of the AI ecosystem, the most comprehensive model is a layered liability model, which allocates responsibility to various parties in the AI chain according to their level of control, benefit, and ability to prevent harm. This model aligns with the approach adopted by the EU AI Act.

4. **Regulatory Update Recommendations**

Based on the above analysis, this study formulates several concrete recommendations for reforming Indonesian criminal law in dealing with AI-based crimes.First, the development of a comprehensive Artificial Intelligence Law (AI Law) is urgent. Ideally, such an AI law would adopt a risk-based approach similar to the EU AI Act, classifying AI systems based on their risk level and establishing proportionate legal obligations and responsibilities. Criminal provisions in the AI Law should explicitly address:

a. Defining AI systems and related entities;
b. Criminal liability allocation mechanisms in the AI ecosystem

c. Obligations for transparency and auditability of AI systems;
d. Minimum security standards for AI systems.

Second, amendments to the ITE Law need to be made to accommodate crimes committed through or by AI systems. Specifically, provisions should be added governing: the liability of AI service providers for content or actions generated by their systems; the criminalization of the use of AI for manipulation, fraud, or cybercrime; and mandatory moderation of AI-generated content. Third, the development of a new criminal liability doctrine specific to the AI context needs to be achieved through progressive jurisprudence and regulatory development. The "duty of care in AI deployment" doctrine, which combines elements of civil and criminal law, could serve as a foundation for developing criminal law norms for AI in Indonesia. Fourth, strengthening the capacity of law enforcement officers through specialized training in AI digital forensics and the establishment of special AI crime units within the Police and Prosecutor's Office are equally important implementation steps.

CLOSING

Conclusion

Based on the analysis that has been carried out, this study draws three main conclusions.as follows.

1. Indonesia's current criminal law framework, including the Criminal Code, the Electronic Information and Transactions Law, and the 2023 National Criminal Code, is not yet able to optimally address criminal liability for crimes committed by or through autonomous AI systems. A significant legal vacuum exists, particularly regarding the identification of legal subjects, the fulfillment of mens rea, and the mechanism for allocating responsibility within the complex AI ecosystem.
2. A comparative study of AI regulations in the European Union, the United States, China, and Singapore found that a risk-based approach combined with a layered liability model is the most comprehensive and adaptable model in the Indonesian legal context. This model allocates responsibility proportionally to developers, operators, and users of AI systems based on each party's level of control and capacity to prevent harm.
3. Existing principles of Indonesian criminal law, including vicarious liability, strict liability, and corporate liability, can be used as a basis for developing the doctrine of AI criminal liability, but require significant adaptation and normative innovation to be implemented effectively and fairly.

Suggestion

Based on the above conclusions, this study recommendsin the form of suggestions or input as follows:

1. The Indonesian government and the House of Representatives (DPR RI) need to immediately prioritize the drafting of an Artificial Intelligence Bill that comprehensively regulates criminal liability in the AI ecosystem. The Supreme Court needs to issue a Supreme Court Regulation (PERMA) as a guideline for judges in deciding cases involving AI systems while awaiting comprehensive regulations.
2. Law enforcement officials need to increase their technical and legal capacity to handle AI-based crimes, including the establishment of a dedicated AI crimes unit;
3. National standards (SNI) for the security and transparency of AI systems need to be developed to serve as a reference for law enforcement. Interdisciplinary research involving experts in law, information technology, and ethics is essential to develop legal solutions that are both technologically sound and humane.

REFERENCES

Buku:

Barda Nawawi Arief, Bunga Rampai Kebijakan Hukum Pidana, Citra Aditya Bakti.

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. Crime Science, 9(1), 1-13. https://doi.org/10.1186/s40163-020-00123-8

Floridi, L., et al. (2018). AI4People An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689-707.

Moeljatno. (2008). Asas-asas Hukum Pidana. Jakarta: Rineka Cipta.

Muladi & Barda Nawawi Arief, Teori-Teori dan Kebijakan Pidana, Alumni.

Roeslan Saleh. (1983). Perbuatan Pidana dan Pertanggungjawaban Pidana: Dua Pengertian Dasar dalam Hukum Pidana. Jakarta: Aksara Baru.

R. Soesilo, Kitab Undang-Undang Hukum Pidana (KUHP) serta Komentar-komentarnya, Politeia.

Schaffmeister, D., Keijzer, N., & Sutorius, E.P.H. (2011). Hukum Pidana (Terjemahan J.E. Sahetapy). Yogyakarta: Liberty.

Soekanto, S., & Mamudji, S. (2001). Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: Raja Grafindo Persada.

Turner, J. (2019). Robot Rules: Regulating Artificial Intelligence. Cham: Palgrave Macmillan.

Artikel/Jurnal:

Aldin, A., Jumanudin, J., & Fahlevi, A. R. (2026). Pertanggungjawaban Pidana Dalam Tindak Pidana Berbasis Artificial Intelligence. RIGGS: Journal of Artificial Intelligence and Digital Business, 5(1), 6033-6042.

Dremliuga, R., Kuznetcov, P., & Mamychev, A. (2019). Criteria for recognition of AI as a legal person. Journal of Politics and Law, 12(3), 105-113.

Hallevy, G. (2010). The criminal liability of artificial intelligence entities from science fiction to legal social control. Akron Intellectual Property Journal, 4(2), 171-201.

Hibatulloh, B. H. F. (2025). Upaya penegakan hukum terhadap AI (Artificial Intelligence) sebagai subjek hukum pidana dalam perspektif kriminologi. Tarunalaw: Journal of Law and Syariah, 3(01), 87-98.

Harahap, A., Rahmayanti, R., Tiono, R., & Pariyono, B. A. (2025). Analisis Diskresi Hakim dalam Mengintegrasikan Rekomendasi Penalaran Hukum Berbasis Kecerdasan Buatan (AI) di Pengadilan Niaga. Locus Journal of Academic Literature Review, 4(9), 734-745.

Linarelli, J., Salomon, M. E., & Sornarajah, M. (2018). The Misery of International Law: Confrontations with Injustice in the Global Economy. Oxford: Oxford University Press.

Laia, Y. R. N., Rahmayanti, R., Tampubolon, S. S., Gea, A. S., & Nasution, S. H. (2025). Implementasi Hukum terhadap Tindak Pidana Scammer. JISPENDIORA Jurnal Ilmu Sosial Pendidikan Dan Humaniora, 4(1), 603-613.

Prakasa, S. U. W., & Widiatedja, I. G. N. P. (2021). Urgensi pengaturan kecerdasan artifisial di Indonesia. Jurnal Ilmiah Kebijakan Hukum, 15(3), 499-518.

Putri, N. P. M., Hartono, M. S., & Yudiawan, I. D. G. H. (2024). Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake Dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelligence. Jurnal Pacta Sunt Servanda, 5(2), 120-129.

Syaharani, N., Rahmayanti, R., Nurdiana, C., Saputra, D. D., & Harahap, R. N. F. (2025). Perlindungan Hukum bagi Remaja Perempuan dari Kekerasan Seksual via Media Sosial. Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, 5(2), 1036-1047.

Tegnan, H. (2016). Legal pluralism and land law in Indonesia. The Journal of Legal Pluralism and Unofficial Law, 48(2), 198-216.

Wahyudi, A. (2022). Pertanggungjawaban pidana korporasi dalam tindak pidana siber: Perspektif hukum Indonesia. Jurnal Hukum Ius Quia Iustum, 29(1), 52-73.

Peraturan Perundang-undangan:

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara RI Tahun 2022 Nomor 196.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara RI Tahun 2023 Nomor 1.

European Parliament and the Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.