

CRIMINAL LIABILITY FOR ARTIFICIAL INTELLIGENCE-BASED CRIMES UNDER CRIMINAL LAW IN INDONESIA

Hendri Saputra Manalu, Rahmadany, Anto Mutriady
Universitas Amir Hamzah Medan

Email: hendri89.hm@gmail.com, danyrahma993@gmail.com, Antomutri8@gmail.com

Received: 12/05/2026 | Revised: 13/05/2026 | Accepted: 17/07/2026 | Published: 24/07/2026

Abstract

The development of Artificial Intelligence (AI) technology brings complex legal implications, particularly in the field of criminal law. Crimes committed using AI systems such as deepfakes, automated cyberattacks, algorithm-based fraud, and data manipulation raise 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 current Indonesian criminal law framework and identify existing legal gaps (*leemten in het recht*). The research method used is normative juridical with a statutory 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 bridged by autonomous AI systems. Comprehensive regulatory reform is urgently needed, including the establishment of new legal subjects, the implementation of adapted doctrines of strict liability and vicarious liability, 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

AI is no longer just 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 the existing criminal justice system. Indonesia, as a country with the fourth largest internet user population in the world, faces high exposure to AI-based crimes. The phenomenon of **deepfakes**—video and audio manipulation using AI machine learning technology—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 now 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 emerge.

Amidst these developments, a fundamental question has emerged that has not been satisfactorily answered by Indonesian criminal law: Who should be held criminally responsible when an AI system autonomously performs an action that objectively constitutes a crime? Should the developer, owner, operator, user of the AI system, or even the AI system itself be held responsible? The current Indonesian criminal law framework, based on the Dutch colonial Criminal Code and Law No. 19 of 2016 concerning Electronic Information and Transactions (UU ITE), is built on the premise that perpetrators of criminal acts are human beings with free will (**mens rea**) and the physical capacity to act (**actus reus**). The fundamental principle of criminal liability, that there is no crime without fault (**geen straf zonder schuld**), faces existential challenges when faced with AI systems that lack consciousness, intent, or moral capacity.

The urgency of this research becomes increasingly relevant considering that Law No. 1 of 2023 concerning the National Criminal Code has come into effect, which specifically addresses the dimensions of criminal liability in the context of AI-based crimes. Meanwhile, several jurisdictions, such as the European Union, have gone further

by passing the *EU Artificial Intelligence Act* in 2024, which is the first comprehensive AI regulation in the world. Based on the above background, this research 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 reform.

Page 786

LITERATURE REVIEW

1. The Concept of Criminal Responsibility in Indonesian Criminal Law

Criminal responsibility (*toerekeningsvatbaarheid*) is the core of the entire criminal law system. Moeljatno (2008) defines criminal responsibility as a person's ability to bear the legal consequences of a crime. This responsibility 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 that eliminates the fault (*schulduitsluitingsgrond*).

Roeslan Saleh (1983) emphasized that the principle of fault is the main basis 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 mind is also guilty. Schaffmeister, Keijzer, and Sutorius (2011) classify the forms of fault in Indonesian criminal law into two main categories: intention (*opzet*), which includes intention as intent/purpose, intention as certainty, and intention as possibility; and negligence (*culpa*), which includes conscious negligence and unconscious negligence.

The Indonesian Criminal Code has historically recognized only 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 crimes, or crimes that use or target AI systems, has grown rapidly in the last 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 simply carries out instructions from its programmer. 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* pornography that 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.** Manipulation of financial market algorithms 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

Some relevant criminal liability doctrines in the context of AI crimes include: First, strict liability, which does not require proof of fault but rather proof of the criminal act itself (*actus reus*). Second, vicarious liability, which imposes responsibility on the party who has control over the direct perpetrator. Third, the product liability doctrine, which places responsibility on the manufacturer or developer of AI for the harm caused by their product. Fourth, the natural-probable consequence doctrine, which emphasizes the predictability of harmful actions of 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 aligns with the 2017 European Parliament resolution. This concept, while controversial, offers an alternative solution to address the legal vacuum in AI criminal liability.

Page 787

4. Comparative Legal Studies

Comparative approaches to AI regulation across jurisdictions provide valuable insights. The European Union, through the *EU Artificial Intelligence Act* (2024), adopted a risk-based approach that classifies AI systems into

four risk tiers with varying legal consequences. The United States developed a sectoral approach through various regulations such as the *FTC Act*, *CFPB* Guidance, and several state-level 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 study uses a normative legal research approach, namely legal research conducted by examining library materials or secondary data as a basis for research by searching regulations and literature related to the problem under study (Soekanto and Mamudji, 2001). This approach was chosen because this study aims to examine rules or norms in positive law. This study combines three main approaches. First, a statute approach is used to examine all laws and regulations related to criminal liability and cybercrime in Indonesia, including the Criminal Code (KUHP), the Electronic Information and Transactions Law (ITE), the 2023 National Criminal Code, 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, Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE), Law Number 1 of 2023 concerning the 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 carried out through a literature study, 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 repository of Indonesian laws and regulations (JDIH). The legal material analysis was conducted prescriptively and analytically, using grammatical, systematic, historical, and teleological interpretation techniques to produce a coherent legal proposition.

RESULTS AND DISCUSSION

1. Analysis of the Indonesian Criminal Law Framework for AI-Based Crimes

Research findings indicate that the Indonesian criminal law framework faces at least five fundamental challenges in addressing AI-based crimes. The first challenge is the failure to meet the *mens rea* requirement. The Criminal Code and the Electronic Information and Transactions 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 the *mens rea* to be held accountable.

The second challenge is the problem of identifying the perpetrator (attribution of *actus reus*). In the complex architecture of modern AI systems involving multiple layers of developers, platform providers, operators, and end users, determining who legally committed *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 only recognizes humans and corporations as subjects of criminal law, but does not specifically accommodate AI as an entity that can be prosecuted or used as a basis for liability for others.

The fourth challenge is the issue of jurisdiction. 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) is inadequate to address the transnational nature of AI-based crimes and the technical evidentiary issues. The decision-making process in AI systems is opaque (the *black box* problem), making it difficult to legally prove how and why the AI system made certain decisions that led to harm. This creates epistemological difficulties in criminal evidence, which requires a standard of proof beyond a reasonable doubt.

2. Mapping of Existing Regulations and Legal Gaps

An analysis of the 2016 ITE Law shows that while it specifically addresses cybercrime, its provisions are designed with the assumption that the perpetrators are human beings using computer systems as tools. Article 30,

CRIMINAL LIABILITY FOR ARTIFICIAL INTELLIGENCE-BASED CRIMES UNDER CRIMINAL LAW IN INDONESIA

Hendri Saputra Manalu et al

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 Criminal Code (National Criminal Code), which will come into full force 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 generally prohibited based on the principles of legality (*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 that data.

3. Applicable Criminal Liability Models

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

The second is Operator Liability. Those operating AI systems—whether individuals or 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.

Third 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* rests with the user. However, challenges arise when the AI system performs actions outside of the user's instructions, resulting in harm to a third party. The fourth model is Layered Liability. Given the complexity of the AI ecosystem, the most comprehensive model is the Layered Liability model, which allocates responsibility to different parties in the AI chain according to their level of control, profit, 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 addressing AI-based crimes. First, the drafting of a comprehensive Artificial Intelligence Law (AI Law) is urgently needed. Ideally, such 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. The criminal provisions in the AI Law should explicitly regulate:

* **a.** Definition of AI systems and related entities;

* **b.** Criminal liability allocation mechanisms in the AI ecosystem;

Page 789

* **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 governing the following should be added: liability of AI service providers for content or actions generated by their systems; 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 dedicated 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. Significant legal gaps remain, 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 regulation 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 an AI criminal liability doctrine, but require significant adaptation and normative innovation to be implemented effectively and fairly.

Suggestion

1. Indonesia 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 should issue a Supreme Court Regulation (PERMA) to guide judges in deciding cases involving AI systems while awaiting the development of comprehensive regulations.

2. Law enforcement officials need to improve their technical and legal capacity to handle AI-based crimes, including the establishment of a special AI crimes unit;

3. An Indonesian National Standard for the security and transparency of AI systems needs to be developed to serve as a reference for law enforcement. Interdisciplinary research involving experts in law, information technology, and ethics is crucial for developing legal solutions that are both technologically robust and humane.

REFERENCES

- * 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>
- * 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.
- * 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.
- * 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.

CRIMINAL LIABILITY FOR ARTIFICIAL INTELLIGENCE-BASED CRIMES UNDER CRIMINAL LAW IN INDONESIA

Hendri Saputra Manalu **et al**

* 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.

* 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.