Jurisprudentie

Jurnal Jurisprudentie, Volume 12 Issue 2, 2025
P-ISSN: 2355-9640, E-ISSN: 2580-5738

This work is licensed under a Creative Commons Attribution 4.0 International License

Challenges of Criminal Liability Related to Artificial Intelligence (AI) in Indonesia: Lessons from European Law

Ach. Tahir[1]

[1] *Faculty of Sharia and Law, Sunan Kalijaga State Islamic University Yogyakarta, Indonesia.*
E-mail: ach.tahir@uin-suka.ac.id

Abstract: This study aims to analyze the reasons why Indonesian criminal law has not yet recognized Artificial Intelligence (AI) as a subject of criminal liability and to examine relevant models of criminal responsibility when AI is involved in criminal acts. This research employs a normative legal method with a literature-based approach, analyzing legislation, criminal law doctrines, and international literature related to the development of AI regulation. The analysis shows that the difficulty in positioning AI as a legal subject stems from juridical, philosophical, and technical limitations within Indonesian criminal law. As a solution, when AI-related crimes occur, criminal liability may be attributed to programmers, manufacturers, users, or corporations based on their degree of functional control over the AI system. This approach is compared with the regulatory framework of the European Union through its AI Act, which serves as a normative benchmark as the first comprehensive and binding AI regulation addressing accountability in autonomous systems. The relevance of this comparison lies in its emphasis on control-based and risk-oriented responsibility, which reflects legal challenges similarly faced within the Indonesian legal system and aligns with the doctrines of functional control, corporate liability, vicarious liability, and risk management. The study concludes that Indonesia's current criminal law framework does not place AI as a subject of criminal law, thereby directing liability toward humans or corporations within the technology's control chain.

Keywords: Artificial Intelligence (AI); Criminal Liability; Indonesian Law; European Law.

1. Introduction

The development of digital technology over the past two decades has given rise to a new phenomenon known as Artificial Intelligence (AI). AI is no longer used solely in entertainment and social media; it has expanded into various fields, including transportation, healthcare, finance, and even the legal system itself.[1] Autonomous vehicles, medical robots, financial recommendation systems, and AI-based chatbots demonstrate that automated algorithms are increasingly replacing human roles in decision-making processes.[2]

[1] Ajanthaa Lakkshmanan et al., "Engineering Applications of Artificial Intelligence," 2024, 166–79, https://doi.org/10.4018/979-8-3693-5261-8.ch010; Vijaykrishnan Narayanan et al., "Overview of Recent Advancements in Deep Learning and Artificial Intelligence," in *Advances in Electromagnetics Empowered by Artificial Intelligence and Deep Learning* (Wiley, 2023), 23–79, https://doi.org/10.1002/9781119853923.ch2.

[2] Sakshi Rajput, Deepak Sarangi, and Preeti Sehrawat, "Artificial Intelligence Technology in Different Fields," 2023, 161–83, https://doi.org/10.4018/978-1-6684-6418-2.ch009.

This autonomous capability opens the door to various potential risks, including the occurrence of criminal acts involving or caused by AI.[3] Such phenomena raise new issues within the field of criminal law. Such phenomena raise new issues within the field of criminal law. When AI-generated actions produce harm, error, or prohibited consequences, the question emerges: who should be held responsible? Here, the gap becomes evident between rapid technological developments and the existing legal framework, particularly in the context of Indonesian criminal law.

From a criminal law perspective, a fundamental issue arises regarding who should bear responsibility when a criminal act occurs due to an error by an AI system. To date, Indonesian criminal legislation has not explicitly regulated the position of AI within the legal framework of subjects. The Indonesian criminal law system, as governed by the old Indonesian Criminal Code, the new 2023 Criminal Code, and the Indonesian Law on Electronic Information and Transactions (UU ITE), recognizes only two subjects of criminal liability: natural persons (naturlijk persoon) and corporations (rechtspersoon). Even the UU ITE, which regulates digital technology, has not explicitly addressed criminal acts arising from failures of autonomous AI systems.

Recent studies show that discourse on AI as a subject of criminal law in Indonesia remains very limited and generally reaches the same conclusion. AI cannot yet be considered a subject of criminal liability under the current legal system. The entire normative framework — from foundational principles to positive law — continues to place humans and corporations as the only entities capable of bearing criminal liability, leaving AI as a non-legal entity incapable of being attributed with fault or intent.[4] Even studies attempting to explore whether AI could be treated similarly to humans remain theoretical and lack a sufficient juridical basis. Nevertheless, AI merits consideration as a potential legal subject due to its autonomous decision-making capacity.[5]

[3] L Escalante-Huisacayna et al., "Criminal Liability and Artificial Intelligence: A Systematic Review of the Scientific Literature," in *Lecture Notes in Networks and Systems*, vol. 1177, 2025, 473–83, https://doi.org/10.1007/978-981-97-8695-4_43.

[4] R A Rahman and R Habibulah, "THE CRIMINAL LIABILITY OF ARTIFICIAL INTELLIGENCE: IS IT PLAUSIBLE TO HITHERTO INDONESIAN CRIMINAL SYSTEM?," *Legality: Jurnal Ilmiah Hukum* 27, no. 2 (2019): 147–60, https://doi.org/10.22219/jihl.v27i2.10153; V Mahardhika, P Astuti, and A Mustafa, "Could Artificial Intelligence Be the Subject of Criminal Law?," *Yustisia* 12, no. 1 (2023), https://doi.org/10.20961/yustisia.v12i1.56065.

[5] M Ali, M.O.D.P. Mulya, and W P N Permana, "Criminal Liability of Artificial Intelligence Crime in Indonesia: Challenges and Opportunities," *Pakistan Journal of Criminology* 15, no. 3 (2023): 45–59,

The inadequacy of positive law becomes even more apparent as AI technology advances far more rapidly than the regulatory capacity to keep pace, creating a normative gap in determining who should be held accountable when crimes involving AI occur.[6] Courts have yet to establish precedents recognizing AI as a criminal perpetrator, and responsibility continues to be consistently shifted to humans: developers, controllers, or users of AI systems.[7]

Broader studies on robot lawyers, autonomous vehicles, and the use of AI in various judicial sectors uniformly agree that legal reform is necessary. It does not designate AI as a subject of criminal liability, but to clarify models of human and institutional accountability concerning risks arising from AI systems.[8] Overall, existing research suggests that Indonesia's legal system currently lacks an ontological or normative basis for AI to become a subject of criminal law. The ongoing discourse remains primarily prospective, reform-oriented, and focused on structuring human accountability within the AI ecosystem.

This condition raises further questions: why has Indonesian criminal law not yet recognized AI as a legal subject capable of bearing criminal responsibility? This question is crucial because it touches on fundamental aspects of criminal law, specifically the boundaries of who may be considered a perpetrator in the legal sense and the prerequisites that must be met for an entity to be held criminally liable. Furthermore, although AI does not yet hold the status of a legal subject, in practice, various AI-based activities have already been involved in situations with potential criminal implications. This raises the need for clarity on how criminal responsibility should be directed when AI becomes part of the chain of events leading to a criminal act. In other words, the second issue is: what models of criminal liability can be applied to address crimes involving AI?

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85173047758&partnerID=40&md5=23a3db780babfe430c722e3ea0594c05.

[6] A Wisnubroto and H Tegnan, "Preventing AI Crime Towards A New Legal Paradigm: Lessons From United States," *Journal of Human Rights, Culture and Legal System* 5, no. 2 (2025): 630–58, https://doi.org/10.53955/jhcls.v5i2.606.

[7] Mahardhika, Astuti, and Mustafa, "Could Artificial Intelligence Be the Subject of Criminal Law?"; Ali, Mulya, and Permana, "Criminal Liability of Artificial Intelligence Crime in Indonesia: Challenges and Opportunities."

[8] Z J Fernando et al., "Robot Lawyer in Indonesian Criminal Justice System: Problems and Challenges for Future Law Enforcement," *Lex Scientia Law Review* 7, no. 2 (2023): 489–528, https://doi.org/10.15294/lesrev.v7i2.69423; U Maskanah, "Artificial Intelligence in Civil Justice: Comparative Legal Analysis and Practical Frameworks for Indonesia," *Jambura Law Review* 7, no. 1 (2025): 225–42, https://doi.org/10.33756/jlr.v7i1.27786.

2. Method

This study employs a normative legal research method that focuses on examining statutory regulations, legal doctrines, and relevant legal literature.[9] This normative legal research method is combined with a comparative legal approach. The comparative analysis examines the European Union's AI regulatory framework as a normative benchmark to identify transferable principles of accountability and risk-based responsibility relevant to the Indonesian legal system. The comparison is analytical and doctrinal in nature, aimed at contextual adaptation rather than direct legal transplantation.

The research adopts two main approaches. First, the statutory approach involves reviewing various relevant regulations, such as the old Criminal Code (KUHP) and the new 2023 Criminal Code, as well as the Electronic Information and Transactions Law (UU ITE), and other sectoral regulations related to the use of electronic and digital systems. This approach is crucial for determining the extent to which Indonesian positive law has established a legal basis for the use of AI. Second, the conceptual approach involves examining various criminal law theories, including classical theories of criminal liability, strict liability, vicarious liability, corporate criminal liability, and other relevant doctrines. Through this approach, the study can assess the extent to which existing legal doctrines can be applied or need to be expanded to address issues of criminal law arising from the use of AI.

The data used in this research consist of secondary data, including primary, secondary, and tertiary legal materials. The primary legal materials include national statutory regulations, such as the Criminal Code and the Electronic Information and Transactions Law, as well as relevant international legal instruments. The secondary legal materials consist of books, scholarly journals, articles, research reports, and expert opinions in criminal law and technology related to AI. Meanwhile, tertiary legal materials include legal dictionaries, legal encyclopedias, indexes, and other general reference sources that support the analysis of primary and secondary materials. These legal materials are compiled through library research, which involves examining official documents, legal databases, academic literature, and scientific publications.

[9] Achmad Irwan Hamzani et al., "Implementation Approach in Legal Research," *International Journal of Advances in Applied Sciences* 13, no. 2 (June 1, 2024): 380, https://doi.org/10.11591/ijaas.v13.i2.pp380-388.

3. Results and Discussion

3.1 Difficulties in Positioning AI as a Subject of Criminal Law

Artificial Intelligence is understood as intelligence demonstrated by machines or computer systems to perform tasks that typically require human intelligence.[10] AI is not only capable of executing instructions, but can also learn, adapt, and even make decisions autonomously. AI systems utilize datasets to analyze information, identify patterns, and adjust their actions based on newly acquired data. This enables AI to draw logical conclusions and adapt to innovations or knowledge.[11] The application of AI across various sectors, such as autonomous vehicles in transportation, medical robots in healthcare, and credit-scoring systems in finance, illustrates that AI offers both benefits and risks. Technical errors, such as sensor malfunctions in autonomous cars or algorithmic bias in loan assessment processes, can lead to significant harm, even endangering human safety.

In the context of criminal law, a dilemma emerges regarding who should be held responsible when such errors occur. Traditional criminal law struggles to accommodate the autonomous and complex nature of AI systems. This difficulty arises because conventional law relies on concepts such as mens rea (the intention to commit a crime) and actus reus (the physical act of committing a crime).[12] Criminal liability in Indonesian law is based on the principle of "geen straf zonder schuld," meaning no punishment without fault. This doctrine requires the unity of prohibited conduct (actus reus) and a guilty mental state (mens rea). A person cannot be punished simply for committing an unlawful act if no fault accompanies it.[13] A person may only be held criminally liable when their act is committed with intent or negligence.

[10] Giovanni Cappello et al., "Artificial Intelligence in Oncologic Imaging," in *Multimodality Imaging and Intervention in Oncology* (Cham: Springer International Publishing, 2023), 585–97, https://doi.org/10.1007/978-3-031-28524-0_24.

[11] Akwi Helene Fomude et al., "AI Model to Improve HR Decision-Making with Machine Learning Predictions Algorithm," in *2023 25th International Conference on Advanced Communication Technology (ICACT)* (IEEE, 2023), 206–12, https://doi.org/10.23919/ICACT56868.2023.10079282.

[12] Nora Osmani, "The Complexity of Criminal Liability of AI Systems," *Masaryk University Journal of Law and Technology* 14, no. 1 (June 26, 2020): 53–82, https://doi.org/10.5817/MUJLT2020-1-3; Vicko Taniady, "AI-Induced Fatalities: A Criminal Law Perspective from Indonesia and International Perspective," *Yustisia Jurnal Hukum* 14, no. 2 (August 13, 2025): 126, https://doi.org/10.20961/yustisia.v14i2.101636.

[13] Muhammad Habibur Rochman, "Juridical Analysis of Unlawful Acts in a Land Grabbing Case Without Ownership Rights," *TARUNALAW : Journal of Law and Syariah* 1, no. 02 (July 17, 2023): 166–74, https://doi.org/10.54298/tarunalaw.v1i02.157.

In its development, the new Criminal Code enacted through Law No. 1 of 2023 recognizes both individuals and corporations as subjects of criminal law. This new framework opens the door to approaches such as strict liability and vicarious liability, in which a corporation may be held criminally responsible for actions committed by its personnel.[14] However, Artificial Intelligence has not been incorporated into these categories, raising the question of how AI should be situated within the framework of criminal liability.

Indonesian criminal law is conceptually built upon classical principles that are highly anthropocentric. This is evident in the formulation of offenses in both the old and the new Criminal Code, which use terms such as "barang siapa" or "every person," systematically referring to legal subjects possessing consciousness and will. Although modern legal developments have expanded the scope of criminal law to include corporations, this expansion is grounded in a legal fiction that treats human actors as representatives of the corporation's actions. Recognition of corporations as legal subjects does not imply that corporations possess intent or morality; instead, the law creates mechanisms to attribute responsibility that ultimately traces back to humans.

Another normative or juridical obstacle relates to the limited definition of "legal subject" in criminal law. A legal subject in this context is not merely an entity that can be prosecuted, but one that must possess the capacity for responsibility. Indonesian law recognizes humans and corporations as legal subjects, but has not yet recognized new categories, such as "electronic personhood," which is currently being discussed in international legal literature. Electronic personhood refers to granting AI systems a legal status similar to that of a person. This concept has been proposed to address challenges in attributing responsibility for actions performed by AI.[15]

[14] Henny Yunita Fitriani, "PERTANGGUNGJAWABAN PIDANA KORPORASI DALAM TINDAK PIDANA LINGKUNGAN HIDUP BERDASARKAN ASAS STRICT LIABILITY (STUDI KASUS PENCEMARAN LINGKUNGAN OLEH PT. RAYON UTAMA MAKMUR (RUM) KABUPATEN SUKOHARJO)," *Jurnal Hukum Dan Pembangunan Ekonomi* 8, no. 2 (July 16, 2021): 64, https://doi.org/10.20961/hpe.v8i2.49757.

[15] H Sayyed, "Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges," *Cogent Social Sciences* 10, no. 1 (2024), https://doi.org/10.1080/23311886.2024.2343195; G Lima et al., "The Conflict Between People's Urge to Punish AI and Legal Systems," *Frontiers in Robotics and AI* 8 (2021), https://doi.org/10.3389/frobt.2021.756242; L Escalante-Huisacayna et al., "Criminal Liability and Artificial Intelligence: A Systematic Review of the Scientific Literature," in *Lecture Notes in Networks and Systems*, vol. 1177, 2025, 473–83, https://doi.org/10.1007/978-981-97-8695-4_43; M Swart, "Constructing 'Electronic Liability' for International Crimes: Transcending the Individual in International Criminal Law," *German Law Journal* 24, no. 3 (2023): 589–602, https://doi.org/10.1017/glj.2023.28.

Indonesian law currently lacks a normative basis, legal theory, or precedent that would allow the creation of a new legal subject category encompassing algorithm-based entities such as AI. Consequently, even though AI may be theoretically debated as a legal subject, Indonesia lacks a normative mechanism to establish such a position. Similar issues are seen in other jurisdictions. India's criminal law system also struggles to address AI-related violations due to reliance on traditional criminal law concepts.[16] The absence of a clear framework for AI liability complicates the attribution of responsibility for actions driven by AI.[17] In Greece, criminal law practice remains inseparably tied to human agency and instead proposes a model based on objective negligence for AI-related criminal liability.[18]

Normative shortcomings also appear in the Electronic Information and Transactions Law (UU ITE). This law is primarily designed to regulate human behavior in digital spaces, rather than to subject automated systems, such as AI, to criminal law. The normative structure of UU ITE consistently centers on "every person" as the perpetrator of cybercrimes, meaning all offenses explicitly require human action, intention, or negligence. AI is often treated merely as a tool or instrument used by human actors, rather than as an autonomous entity capable of bearing responsibility. When a prohibited act is committed through automated or algorithmic mechanisms, liability under UU ITE is still attributed to the individuals who operate, command, or utilize the AI. Thus, UU ITE lacks a normative framework for assessing AI-generated actions as those of a perpetrator, and it provides no conceptual basis for treating AI as a criminal actor. Consequently, the legal framework of UU ITE does not accommodate AI as a legal subject.[19]

[16] Sayyed, "Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges."

[17] A Sachoulidou, "AI Systems and Criminal Liability," *Oslo Law Review* 11, no. 1 (2024), https://doi.org/10.18261/olr.11.1.3.

[18] M K Gbandi, A Sachoulidou, and D Lima, "GREEK REPORT ON TRADITIONAL CRIMINAL LAW CATEGORIES AND AI," *Revue Internationale de Droit Penal* 2023 (2023): 223–51, https://www.scopus.com/inward/record.uri?eid=2-s2.0-85192830987&partnerID=40&md5=72095fae2747059f06ff6e9230fe364f.

[19] R Saputra, T Tiolince, and S K Sigh, "Artificial Intelligence and Intellectual Property Protection in Indonesia and Japan," *Journal of Human Rights, Culture and Legal System* 3, no. 2 (2023): 210–35, https://doi.org/10.53955/jhcls.v3i2.69; D T Subagiyo and H Wibisono, "THE URGENCY OF ARTIFICIAL INTELLIGENCE REGULATION FROM A JOINT AUTHORSHIP PERSPECTIVE ON COPYRIGHT INFRINGEMENT," *Indonesia Private Law Review* 5, no. 2 (2024): 135–56, https://doi.org/10.25041/iplr.v5i2.3962; C B E Praja et al., "Legal Analysis of AI-Generated Creations: Copyright Law Perspectives," in *E3S Web of Conferences*, vol. 622, 2025, https://doi.org/10.1051/e3sconf/202562203005.

Another weakness lies in the offenses under UU ITE, which almost all require some form of mens rea, such as intent, specific purpose, or knowledge of wrongdoing. AI lacks the cognitive capacity or moral awareness to understand the meaning of legal prohibitions; therefore, the subjective elements of UU ITE offenses cannot be attributed to algorithmic actions. Furthermore, UU ITE regulates liability for the dissemination of illegal content, data manipulation, unauthorized access, and other actions involving electronic systems, but does not provide a mechanism for attributing fault when such actions result from autonomous processes without direct human intervention. This normative gap means that UU ITE can only prosecute humans or corporations behind AI, but cannot address situations where harmful outcomes arise purely from computational processes that neither operators nor producers could anticipate.

From a philosophical perspective, criminal law requires the principle of fault (schuld beginsel) as the basis for criminal liability. This principle demands that a perpetrator possess the capacity for responsibility (toerekeningsvatbaarheid), including the ability to understand their acts and their consequences in moral terms. Indonesian criminal law stipulates that a person is not criminally responsible if they lack mental capacity due to developmental issues or mental disorders.[20] The concept of mens rea (the mental state of the perpetrator) is crucial here, as it reflects intent and awareness. This mental element includes intent and knowledge.[21] However, in the context of AI, even though AI may perform actions outwardly resembling human behavior, it lacks intentionality, consciousness, and moral capacity to distinguish right from wrong. The non-moral and mechanistic nature of AI poses a fundamental obstacle to recognizing AI as a legal subject with criminal implications.

Another philosophical issue concerns the concept of actus reus, which refers to the physical manifestation of a criminal act. In the case of AI, such actions originate from algorithms, training data, and system design implanted by humans. Thus, it becomes difficult to determine whether an AI's action can be considered the result of autonomous will or merely the mechanical output of human programming. Since AI actions are not seen

[20] I Alfarisi and F Afriani, "Reconceptualization of The Competence to Be Held Responsible in National Criminal Code," *Law Reform: Jurnal Pembaharuan Hukum* 17, no. 1 (2021): 95–106, https://doi.org/10.14710/lr.v17i1.37555.

[21] C P Nemeth, *CRIMINAL LAW, SECOND EDITION*, *Criminal Law, Second Edition*, 2011, https://doi.org/10.1201/b11684.

as arising from free will, Indonesian law cannot assert that AI "commits" a criminal act in the legal sense. Globally, criminal liability requires the ability to distinguish right from wrong and the freedom to choose between them.[22]

Classical criminal law liability is grounded in the principle of geen straf zonder schuld, which presupposes the unity of unlawful conduct (actus reus) and a guilty mental state (mens rea). This principle is encapsulated in the maxim actus non facit reum nisi mens sit rea, an act does not make one guilty unless the mind is guilty.[23] This classical theory demonstrates the limitations of Indonesia's current criminal law, which recognizes only humans and corporations as legal subjects. AI systems lack the capacity for mens rea, making it difficult to apply traditional criminal liability principles directly to them. This necessitates a shift toward holding developers, producers, or users responsible through mechanisms such as representative liability.[24]

Another philosophical difficulty arises from an epistemological perspective concerning the relationship between humans and AI within the causal chain of criminal conduct. AI operates through machine learning processes that allow systems to generate outputs that are not always predictable by programmers or users. In some instances, AI may produce harmful or deviant decisions due to complex interactions among algorithms, training data, and adaptive processes. This complexity makes it difficult to determine the source of error in actions seemingly performed by AI; whether the fault lies in initial design, system operation, or adaptive behavior that emerges during use. This ambiguity obstructs Indonesian criminal law from positioning AI as an entity capable of criminal responsibility, as criminal law requires the identification of the perpetrator and proof of fault.

Another issue involves the technical aspects of punishment. Indonesian criminal law recognizes penalties such as imprisonment, fines, confinement, rehabilitation, community service, and other measures, all of which are designed for individuals or corporations. Such sanctions cannot be imposed on AI because AI has no physical body, personal property, or

[22] G Ferguson, "Criminal Liability and Criminal Defenses," in *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, 2015, 219–26, https://doi.org/10.1016/B978-0-08-097086-8.86147-4.

[23] Robert A. Beattey and Mark R. Fondacaro, "The Misjudgment of Criminal Responsibility," *Behavioral Sciences & the Law* 36, no. 4 (July 16, 2018): 457–69, https://doi.org/10.1002/bsl.2354; Peter Fenwick, "Epilepsy, Crime and Legal Responsibility," in *Introduction to Epilepsy* (Cambridge University Press, 2012), 585–86, https://doi.org/10.1017/CBO9781139103992.138.

[24] Taniady, "AI-Induced Fatalities: A Criminal Law Perspective from Indonesia and International Perspective."

capacity to undergo rehabilitative measures. Without applicable forms of punishment or corrective action, criminal law lacks the necessary instruments to penalize AI, thereby preventing it from being positioned as a legal subject unless major reforms to the penal system are implemented.

Additionally, fairness in criminal proceedings presents another obstacle. Criminal law requires that offenders understand the judicial process, possess the right to defend themselves, and be able to participate in legal procedures.[25] AI lacks consciousness, rights, and personal interests. Thus, AI cannot undergo legal processes in the same manner as humans or corporations do. If AI were designated as a legal subject without precise mechanisms of representation, procedural imbalances and legal uncertainty are likely to arise.

In conclusion, the difficulty of Indonesian criminal law in positioning AI as a legal subject results from a combination of normative, philosophical, and technical factors. The existing framework of criminal law is designed for entities that possess consciousness, intent, and moral capacity, whereas AI falls outside these categories. The complexity of AI operations and the conceptual limitations of criminal law doctrine mean that Indonesia's positive law currently lacks an adequate foundation for treating AI as a perpetrator of criminal offenses. AI occupies a unique space: it is neither fully an object nor entirely an agent, and is not fully comparable to a corporation. This ambiguous ontological position makes it impossible for Indonesian criminal law to incorporate AI as a legal subject without first undertaking a substantial reconstruction of the concepts of perpetrator, fault, and the penal system.

3.2 Criminal Liability in AI-Related Crimes: Lessons from Europe

Before discussing sentencing models involving AI within Indonesian criminal law, it is helpful to examine how such models have been developed within European conventions. Sentencing models involving AI under the framework of European conventions are fundamentally oriented toward attributing responsibility to humans and corporations that develop, control, or benefit from the use of AI. The Council of Europe's Convention on Cybercrime (Budapest Convention) and various European Union policy documents do not treat AI as a perpetrator of criminal acts; instead, they regard AI as an instrument used by

[25] M Alfaro Matos et al., "Budgets for the Activity of the Courts: Guarantees for Due Process of Law," *Universidad y Sociedad* 12, no. 5 (2020): 165–71, https://www.scopus.com/inward/record.uri?eid=2-s2.0-85100889104&partnerID=40&md5=7fcd55bfa810ac7509fc700dd83f20ba.

human actors. The Budapest Convention, established by the Council of Europe, is the primary international treaty addressing cybercrime. It provides a framework for national legislation and international cooperation in combating cybercrime, but does not address AI as an autonomous criminal entity.[26] The underlying principle is that digital actions generated by automated systems are attributed to the party exercising effective control over the technology. Thus, if AI is used to commit unauthorized access, data interference, or content-related offences, criminal liability is directed toward individuals or entities that create, operate, or utilize AI in a manner that results in violations of the Convention.

The European approach to sentencing also emphasizes human and corporate responsibility through the principle of corporate criminal liability. When AI is integrated into a company's operations, and its actions result in legal violations, the company may be held liable for inadequate oversight, negligence in risk management, or failure to implement adequate security systems. The European Union's Artificial Intelligence Act (EU AI Act) of 2024 imposes significant obligations on AI providers. Providers are required to ensure that their AI systems comply with the act's requirements, including the quality of training, validation, and testing datasets to prevent bias and discrimination.[27] The regulation requires system controllers and technology providers to bear a high duty of care to ensure safety, transparency, and control over AI.

Providers must also comply with a risk-based regulatory framework that prioritizes the management of risks associated with AI systems.[28] Consequently, if AI behaves in a deviant manner and its actions violate the provisions of the Convention or national laws of EU Member States, criminal liability is directed toward the entities responsible for overseeing

[26] J deArimatéiadaCruz, "The Legislative Framework of the European Union (EU) Convention on Cybercrime," in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, 223–37, https://doi.org/10.1007/978-3-319-78440-3_5; P De Hert, G G Fuster, and B.-J. Koops, "Fighting Cybercrime in the Two Europes. the Added Value of the Eu Framework Decision and the Council of Europe Convention," *Revue Internationale de Droit Penal* 77, no. 3 (2006): 503–24, https://doi.org/10.3917/ridp.773.0503; E Balajanov, "Setting the Minimum Age of Criminal Responsibility for Cybercrime," *International Review of Law, Computers and Technology* 32, no. 1 (2018): 2–20, https://doi.org/10.1080/13600869.2018.1417764.

[27] M van Bekkum, "Using Sensitive Data to De-Bias AI Systems: Article 10(5) of the EU AI Act," *Computer Law and Security Review* 56 (2025), https://doi.org/10.1016/j.clsr.2025.106115.

[28] A Erbežnik, "The Semi-Perfect AI Act – A Missed Opportunity for a Human Rights Centred Approach to AI and the Case of Facial Recognition," in *Data Protection, Privacy and Artificial Intelligence: To Govern or To Be Governed,That Is the Question*, 2025, 115–34, https://www.scopus.com/inward/record.uri?eid=2-s2.0-105014574043&partnerID=40&md5=816806e9675e97da2f383abb4606b774.

and benefitting from the technology. This approach reinforces the notion that, within European legal systems, criminal responsibility remains attached to humans and corporations. At the same time, AI is treated solely as a tool whose actions must be traced back to those with legal authority and responsibility.

Sentencing models for AI-related offences stem from the understanding that AI is positioned as an instrument whose actions result from interactions among technological design, programming, operation, and human or corporate supervision. Because AI is not yet a legal subject, all forms of criminal liability must be traced through causal relationships within the development and use cycle of the technology. Under this approach, AI's actions are not considered autonomous acts in the legal sense, but rather extensions of the activities of the humans and corporations controlling it. The following sentencing models involving AI are presented as potential adaptations for Indonesian criminal law.

The first model assigns criminal responsibility to programmers or developers when an offense arises from errors during the programming stage. This stage forms the foundation of AI's capabilities and limitations, so negligence or harmful actions embedded in the algorithmic structure may serve as a basis for criminal liability. Programmers may be held responsible when algorithmic design enables harmful actions, whether intentionally or due to failure to meet technological safety standards. Negligence in coding, decision-logic implementation, or system security qualifies as human error that may lead to criminal consequences through the intermediation of AI.

The next model involves manufacturers or companies that design and distribute AI systems. Manufacturers are responsible for ensuring the safety, reliability, and stability of their products before they are released to the market. Failure to conduct quality control or safety testing of AI products may constitute harmful conduct that generates criminal risk. Companies that disregard technological development standards or underestimate the potential hazards of their products may be held liable under the doctrine of strict liability, particularly when offenses arise from design defects in the AI systems they produce.

A third model assigns responsibility to users or operators when AI acts based on the user's instructions or due to their negligence. Users occupy operational positions that directly interact with AI systems, making their conduct a primary contributing factor to criminal outcomes. When users intentionally employ AI to commit crimes or negligently fail to supervise systems under their control, criminal liability is directed at the users as the parties who activate or trigger unlawful acts through technological means.

A fourth model directs liability toward corporations that own or control AI systems, mainly when AI is used in the context of business activities. Under this model, AI is viewed as an integral part of corporate operations, and actions that lead to criminal outcomes may be considered part of the corporation's responsibility. Companies that benefit from AI use and have the capacity to supervise the technology may be held liable through the doctrine of corporate liability, which attributes criminal responsibility to organizational fault or inadequate internal oversight.

A fifth model links criminal liability to failures in AI oversight or risk management. Many AI-related offences arise not from programmer or user error but from inadequate supervision standards. Responsibility at this stage is directed to those tasked with organizing, managing, and maintaining the system. When AI behaves in a deviant manner, such failures are viewed as structural negligence that can lead to severe consequences, including criminal penalties.

Other sentencing models emerge through the application of classical criminal law doctrines adapted to technological contexts. The doctrine of vicarious liability permits the imposition of responsibility on parties who benefit from the use of AI or who hold authoritative positions over AI, even if they are not directly involved in the actions that result in criminal outcomes. In this context, harmful AI actions may be constructed as actions of the controlling party within the organizational structure. Vicarious liability places criminal responsibility on another party with a legal relationship to the perpetrator, such as an employer for the acts of an employee. It is a doctrine under which one party is deemed responsible for the wrongful acts of another committed within the scope of their employment, irrespective of fault.[29]

An additional model arises from the application of strict liability when AI use falls within categories of high-risk activities. In such cases, actors are not required to prove malicious intent; it is sufficient to show that the criminal outcome resulted from the use of a system

[29] Mat Campbell and Bobby Lindsay, "Refining Vicarious Liability," *Edinburgh Law Review* 28, no. 2 (May 2024): 174–206, https://doi.org/10.3366/elr.2024.0892; Paula Giliker, "Comparative Law and Legal Culture: Placing Vicarious Liability in Comparative Perspective," *The Chinese Journal of Comparative Law* 6, no. 2 (December 1, 2018): 265–93, https://doi.org/10.1093/cjcl/cxy007.

under their control. This principle is suitable for situations in which AI actions are difficult to predict, but the technology is known to carry risks that may endanger public safety or legal interests. Strict liability permits the imposition of criminal responsibility without proof of fault, commonly applied to offences with significant societal impacts, such as environmental or traffic-related offences. Strict liability in criminal law refers to violations in which the prosecution does not need to prove mens rea for one or more elements of the actus reus.[30]

Collectively, these sentencing models demonstrate that criminal responsibility for AI-related offences is constructed by mapping the relationship between AI's actions and those of the humans or corporations exercising control. AI remains treated as an instrument whose actions are conceptually attributed to human or organizational error. This approach preserves the consistency of Indonesian criminal law, which continues to rely on fault and capacity for responsibility as the basis for criminal liability; hence, sentencing is directed at actors who can realistically be held accountable.

Thus, sentencing models in the context of AI involvement do not fundamentally alter the concept of the perpetrator but instead adapt it to technological realities. This approach allows criminal law to continue protecting society from technological risks without requiring AI to be recognized as a legal subject. The focus of sentencing remains on humans and corporations involved in creating, supervising, or exploiting AI, so that AI's actions can be translated back into the framework of human fault.

4. Conclusion

Indonesian criminal law has not yet recognized Artificial Intelligence (AI) as a subject of criminal liability due to conceptual, normative, and philosophical limitations within the framework of positive law. The Old Criminal Code, the New Criminal Code, and the Electronic Information and Transactions Law (UU ITE) recognize only humans and corporations as legal subjects; therefore, no juridical basis exists for attributing criminal responsibility to non-human entities such as AI. Fundamental principles such as the principle of fault, capacity for responsibility, and the interpretation of mens rea remain rooted in an anthropological understanding of perpetrators. AI's inability to meet moral

[30] Michael S. Moore, "The Strictness of Strict Liability," *Criminal Law and Philosophy* 12, no. 3 (September 29, 2018): 513–29, https://doi.org/10.1007/s11572-017-9438-5; Simester, *Appraising Strict Liability*, ed. Andrew Simester (Oxford University Press, 2005), https://doi.org/10.1093/acprof:oso/9780199278510.001.0001.

and legal consciousness requirements, along with the technical complexity of algorithmic decision-making processes, prevents Indonesian criminal law from treating AI's actions as those of a perpetrator. This situation is further reinforced by the absence of sanctions that are compatible with the nature of AI, meaning that both normatively and practically, AI cannot currently be considered a subject of criminal law within Indonesia's legal system.

Given that AI is not a legal subject, models of criminal liability for AI-related offences are directed entirely at the humans and corporations who design, control, or benefit from the use of such technology. Criminal responsibility is imposed on programmers, manufacturers, users, and corporations through mechanisms such as vicarious liability and strict liability. This attribution pattern aligns with approaches developed in Europe, which consistently position AI as a tool rather than a perpetrator. European experience demonstrates that regulations grounded in functional control, corporate responsibility, and technological risk management correspond with the liability models previously discussed. It Includes the model that assigns responsibility to programmers when AI's actions stem from algorithmic errors; the model that directs liability to manufacturers when offences arise from design defects or failures in safety testing; the model that holds users or operators responsible when AI acts based on human instruction or negligence during operation; and the model that places corporations as subjects of criminal liability when AI is used in business activities and wrongdoing results from failures in supervision or internal risk management.

5. Acknowledgments

The author would like to thank the Institute for Research and Community Service, UIN Sunan Kalijaga Yogyakarta, for its support of this research through the Science-Based Research Cluster Study Program (Klaster Penelitian Berbasis Keilmuan Program Studi) in the 2025 fiscal year.

References

Alfarisi, I, and F Afriani. "Reconceptualization of The Competence to Be Held Responsible in National Criminal Code." *Law Reform: Jurnal Pembaharuan Hukum* 17, no. 1 (2021): 95–106. https://doi.org/10.14710/lr.v17i1.37555.

Alfaro Matos, M, K E Carrión León, S A Montecé Giler, and R Meléndez Carballido. "Budgets for the Activity of the Courts: Guarantees for Due Process of Law." *Universidad y Sociedad* 12, no. 5 (2020): 165–71. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85100889104&partnerID=40&md5=7fcd55bfa810ac7509fc700dd83f20ba.

Ali, M, M.O.D.P. Mulya, and W P N Permana. "Criminal Liability of Artificial Intelligence Crime in Indonesia: Challenges and Opportunities." *Pakistan Journal of Criminology* 15, no. 3 (2023): 45–59. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85173047758&partnerID=40&md5=23a3db780babfe430c722e3ea0594c05.

Balajanov, E. "Setting the Minimum Age of Criminal Responsibility for Cybercrime." *International Review of Law, Computers and Technology* 32, no. 1 (2018): 2–20. https://doi.org/10.1080/13600869.2018.1417764.

Beattey, Robert A., and Mark R. Fondacaro. "The Misjudgment of Criminal Responsibility." *Behavioral Sciences & the Law* 36, no. 4 (July 16, 2018): 457–69. https://doi.org/10.1002/bsl.2354.

Bekkum, M van. "Using Sensitive Data to De-Bias AI Systems: Article 10(5) of the EU AI Act." *Computer Law and Security Review* 56 (2025). https://doi.org/10.1016/j.clsr.2025.106115.

Campbell, Mat, and Bobby Lindsay. "Refining Vicarious Liability." *Edinburgh Law Review* 28, no. 2 (May 2024): 174–206. https://doi.org/10.3366/elr.2024.0892.

Cappello, Giovanni, Arianna Defeudis, Valentina Giannini, Simone Mazzetti, and Daniele Regge. "Artificial Intelligence in Oncologic Imaging." In *Multimodality Imaging and Intervention in Oncology*, 585–97. Cham: Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-28524-0_24.

deArimatéiadaCruz, J. "The Legislative Framework of the European Union (EU) Convention on Cybercrime." In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 223–37, 2020. https://doi.org/10.1007/978-3-319-78440-3_5.

Erbežnik, A. "The Semi-Perfect AI Act – A Missed Opportunity for a Human Rights Centred Approach to AI and the Case of Facial Recognition." In *Data Protection, Privacy and Artificial Intelligence: To Govern or To Be Governed,That Is the Question*, 115–34, 2025. https://www.scopus.com/inward/record.uri?eid=2-s2.0-105014574043&partnerID=40&md5=816806e9675e97da2f383abb4606b774.

Escalante-Huisacayna, L, Y Riega-Virú, K Nilupú-Moreno, and J L Salas-Riega. "Criminal Liability and Artificial Intelligence: A Systematic Review of the Scientific Literature." In *Lecture Notes in Networks and Systems*, 1177:473–83, 2025. https://doi.org/10.1007/978-981-97-8695-4_43.

Fenwick, Peter. "Epilepsy, Crime and Legal Responsibility." In *Introduction to Epilepsy*, 585–86. Cambridge University Press, 2012. https://doi.org/10.1017/CBO9781139103992.138.

Ferguson, G. "Criminal Liability and Criminal Defenses." In *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, 219–26, 2015. https://doi.org/10.1016/B978-0-08-097086-8.86147-4.

Fernando, Z J, K Kristanto, A W Anditya, S Y Hartati, A Baskara, and M Bay. "Robot Lawyer in Indonesian Criminal Justice System: Problems and Challenges for Future Law Enforcement." *Lex Scientia Law Review* 7, no. 2 (2023): 489–528. https://doi.org/10.15294/lesrev.v7i2.69423.

Fitriani, Henny Yunita. "PERTANGGUNGJAWABAN PIDANA KORPORASI DALAM TINDAK PIDANA LINGKUNGAN HIDUP BERDASARKAN ASAS STRICT LIABILITY (STUDI KASUS PENCEMARAN LINGKUNGAN OLEH PT. RAYON UTAMA MAKMUR (RUM) KABUPATEN SUKOHARJO)." *Jurnal Hukum Dan Pembangunan Ekonomi* 8, no. 2 (July 16, 2021): 64. https://doi.org/10.20961/hpe.v8i2.49757.

Fomude, Akwi Helene, Chaoyu Yang, George K. Agordzo, Appiah Vincentia Serwah, and Linda Abangbila. "AI Model to Improve HR Decision-Making with Machine

Learning Predictions Algorithm." In *2023 25th International Conference on Advanced Communication Technology (ICACT)*, 206–12. IEEE, 2023. https://doi.org/10.23919/ICACT56868.2023.10079282.

Gbandi, M K, A Sachoulidou, and D Lima. "GREEK REPORT ON TRADITIONAL CRIMINAL LAW CATEGORIES AND AI." *Revue Internationale de Droit Penal* 2023 (2023): 223–51. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85192830987&partnerID=40&md5=72095fae2747059f06ff6e9230fe364f.

Giliker, Paula. "Comparative Law and Legal Culture: Placing Vicarious Liability in Comparative Perspective." *The Chinese Journal of Comparative Law* 6, no. 2 (December 1, 2018): 265–93. https://doi.org/10.1093/cjcl/cxy007.

Hamzani, Achmad Irwan, Tiyas Vika Widyastuti, Nur Khasanah, and Mohd Hazmi Mohd Rusli. "Implementation Approach in Legal Research." *International Journal of Advances in Applied Sciences* 13, no. 2 (June 1, 2024): 380. https://doi.org/10.11591/ijaas.v13.i2.pp380-388.

Hert, P De, G G Fuster, and B.-J. Koops. "Fighting Cybercrime in the Two Europes. the Added Value of the Eu Framework Decision and the Council of Europe Convention." *Revue Internationale de Droit Penal* 77, no. 3 (2006): 503–24. https://doi.org/10.3917/ridp.773.0503.

Lakkshmanan, Ajanthaa, R. Seranmadevi, P. Hema Sree, and Amit Kumar Tyagi. "Engineering Applications of Artificial Intelligence," 166–79, 2024. https://doi.org/10.4018/979-8-3693-5261-8.ch010.

Lima, G, M Cha, C Jeon, and K S Park. "The Conflict Between People's Urge to Punish AI and Legal Systems." *Frontiers in Robotics and AI* 8 (2021). https://doi.org/10.3389/frobt.2021.756242.

Mahardhika, V, P Astuti, and A Mustafa. "Could Artificial Intelligence Be the Subject of Criminal Law?" *Yustisia* 12, no. 1 (2023). https://doi.org/10.20961/yustisia.v12i1.56065.

Maskanah, U. "Artificial Intelligence in Civil Justice: Comparative Legal Analysis and Practical Frameworks for Indonesia." *Jambura Law Review* 7, no. 1 (2025): 225–42. https://doi.org/10.33756/jlr.v7i1.27786.

Moore, Michael S. "The Strictness of Strict Liability." *Criminal Law and Philosophy* 12, no. 3 (September 29, 2018): 513–29. https://doi.org/10.1007/s11572-017-9438-5.

Narayanan, Vijaykrishnan, Yu Cao, Priyadarshini Panda, Nagadastagiri Reddy Challapalle, Xiaocong Du, Youngeun Kim, Gokul Krishnan, et al. "Overview of Recent Advancements in Deep Learning and Artificial Intelligence." In *Advances in Electromagnetics Empowered by Artificial Intelligence and Deep Learning*, 23–79. Wiley, 2023. https://doi.org/10.1002/9781119853923.ch2.

Nemeth, C P. *CRIMINAL LAW, SECOND EDITION*. *Criminal Law, Second Edition*, 2011. https://doi.org/10.1201/b11684.

Osmani, Nora. "The Complexity of Criminal Liability of AI Systems." *Masaryk University Journal of Law and Technology* 14, no. 1 (June 26, 2020): 53–82. https://doi.org/10.5817/MUJLT2020-1-3.

Praja, C B E, H A Hakim, Y Kurniaty, and E P Sari. "Legal Analysis of AI-Generated Creations: Copyright Law Perspectives." In *E3S Web of Conferences*, Vol. 622, 2025. https://doi.org/10.1051/e3sconf/202562203005.

Rahman, R A, and R Habibulah. "THE CRIMINAL LIABILITY OF ARTIFICIAL INTELLIGENCE: IS IT PLAUSIBLE TO HITHERTO INDONESIAN CRIMINAL SYSTEM?" *Legality: Jurnal Ilmiah Hukum* 27, no. 2 (2019): 147–60.

https://doi.org/10.22219/jihl.v27i2.10153.

Rajput, Sakshi, Deepak Sarangi, and Preeti Sehrawat. "Artificial Intelligence Technology in Different Fields," 161–83, 2023. https://doi.org/10.4018/978-1-6684-6418-2.ch009.

Rochman, Muhammad Habibur. "Juridical Analysis of Unlawful Acts in a Land Grabbing Case Without Ownership Rights." *TARUNALAW : Journal of Law and Syariah* 1, no. 02 (July 17, 2023): 166–74. https://doi.org/10.54298/tarunalaw.v1i02.157.

Sachoulidou, A. "AI Systems and Criminal Liability." *Oslo Law Review* 11, no. 1 (2024). https://doi.org/10.18261/olr.11.1.3.

Saputra, R, T Tiolince, and S K Sigh. "Artificial Intelligence and Intellectual Property Protection in Indonesia and Japan." *Journal of Human Rights, Culture and Legal System* 3, no. 2 (2023): 210–35. https://doi.org/10.53955/jhcls.v3i2.69.

Sayyed, H. "Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges." *Cogent Social Sciences* 10, no. 1 (2024). https://doi.org/10.1080/23311886.2024.2343195.

Simester. *Appraising Strict Liability*. Edited by Andrew Simester. Oxford University Press, 2005. https://doi.org/10.1093/acprof:oso/9780199278510.001.0001.

Subagiyo, D T, and H Wibisono. "THE URGENCY OF ARTIFICIAL INTELLIGENCE REGULATION FROM A JOINT AUTHORSHIP PERSPECTIVE ON COPYRIGHT INFRINGEMENT." *Indonesia Private Law Review* 5, no. 2 (2024): 135–56. https://doi.org/10.25041/iplr.v5i2.3962.

Swart, M. "Constructing 'Electronic Liability' for International Crimes: Transcending the Individual in International Criminal Law." *German Law Journal* 24, no. 3 (2023): 589–602. https://doi.org/10.1017/glj.2023.28.

Taniady, Vicko. "AI-Induced Fatalities: A Criminal Law Perspective from Indonesia and International Perspective." *Yustisia Jurnal Hukum* 14, no. 2 (August 13, 2025): 126. https://doi.org/10.20961/yustisia.v14i2.101636.

Wisnubroto, A, and H Tegnan. "Preventing AI Crime Towards A New Legal Paradigm: Lessons From United States." *Journal of Human Rights, Culture and Legal System* 5, no. 2 (2025): 630–58. https://doi.org/10.53955/jhcls.v5i2.606.