



Reconstructing Criminal Liability for AI-Based Crimes in Indonesian Criminal Law: Rethinking Actus Reus, Mens Rea, and Culpability Attribution

Annisa Sabilla Sueni¹

¹ Faculty of Law, Universitas Bengkulu, Indonesia

Correspondence: annisa.sabillasueni@unib.ac.id

Article Info

Article history:

Received July 27th, 2026

Revised Sept 4th, 2026

Accepted Sept 14th, 2026

Keyword:

Artificial Intelligence; Criminal Liability; *Actus Reus*; *Mens Rea*; Culpability Attribution.

ABSTRACT

The development of Artificial Intelligence (AI) has transformed the nature and modalities of criminal conduct, including deepfakes, impersonation, digital fraud, information manipulation, and various forms of automated cybercrime. These developments present fundamental challenges to Indonesian criminal law, particularly in establishing the relationship between conduct, culpability, and criminal liability when AI functions as an instrument or intermediary in the commission of an offense. This study aims to examine the limitations of the concepts of *actus reus*, *mens rea*, and attribution of culpability in addressing AI-based crimes and to formulate a more adaptive framework of criminal liability in response to technological developments. This study employs a normative juridical method using statutory, conceptual, and comparative approaches. The findings indicate that a criminal liability framework centered primarily on human conduct and culpability encounters an attribution gap when AI systems operate with a high degree of automation. Accordingly, a reconstruction of criminal liability is required through parameters of control, knowledge, contribution, foreseeability, and the degree of culpability of actors within the AI ecosystem. Such reconstruction is essential to ensure legal certainty while preventing an accountability gap in addressing AI-based crimes.



© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>)

INTRODUCTION

The development of Artificial Intelligence (AI) has transformed the nature and modalities of criminal conduct through the use of deepfakes, impersonation, digital fraud, information manipulation, and increasingly automated cyberattacks. The developments pose significant challenges to criminal law because the relationship between human actors, AI systems, criminal conduct, and resulting harm has become increasingly complex. The central issue is therefore not merely whether AI-based conduct should be criminalized, but rather how criminal liability should be attributed when an offense occurs through a system characterized by a certain degree of automation and limited predictability.

This development directly challenges fundamental doctrines of criminal law, particularly *actus reus* and *mens rea*. AI systems lack human consciousness and intention, while their outputs may, under certain circumstances, not be specifically foreseeable to either users or developers. Consequently, an *accountability gap* may arise when criminal harm occurs but the causal and culpable connection between human conduct and the resulting offense is difficult to establish (Monga, 2023). Osmani demonstrates that increasingly autonomous AI systems challenge traditional approaches to criminal liability, particularly in determining attribution of conduct and culpability. Similarly, Fornasier argues that liability may potentially extend to users, developers, or corporations depending on their respective degree of involvement and culpability (Günsberg, 2022).

In Indonesia, previous studies have examined criminal liability arising from the use of AI, including the legal position of AI as an instrument of crime, the liability of users and developers, and the need for legal reform. Studies concerning deepfakes have likewise identified the need to strengthen the criminal liability framework for technology-enabled offenses. Nevertheless, existing scholarship has predominantly examined liability based on the identity of the relevant actor or the need for new regulatory frameworks, while an integrated analysis connecting *actus reus*, *mens rea*, and culpability attribution within the AI ecosystem remains limited (Sachoulidou, 2024).

Addressing this research gap, this study proposes a reconstructed model of criminal liability based on the degree of control, knowledge, contribution, foreseeability, and culpability of actors within the AI ecosystem. Rather than treating AI as a potential criminal-law subject, this study maintains the principle of human culpability while adapting the mechanism of attribution to the distinctive characteristics of AI technology. The study aims to examine the limitations of *actus reus* and *mens rea* in addressing AI – based crimes and to formulate a framework of criminal liability capable of closing the accountability gap without undermining the principle of legality and the fundamental principle of no punishment without culpability. Academically, this study contributes to the development of criminal law doctrine in responding to increasingly autonomous technologies, while practically, it provides a conceptual basis for legislators and law enforcement authorities in determining appropriate standards of criminal liability attribution for AI – based crimes.

RESEARCH METHODS

This research employs a normative juridical method to examine the legal framework governing criminal liability for Artificial Intelligence (AI)-based crimes in Indonesia. The normative approach is employed because the study focuses on legal norms, principles, doctrines, and regulatory frameworks governing *actus reus*, *mens rea*, and the attribution of criminal culpability in the context of AI-mediated criminal conduct. The research applies four approaches: statutory, conceptual, case, and comparative approaches.

The statutory approach examines relevant provisions of Indonesian criminal law, particularly the Indonesian Criminal Code (*Kitab Undang-Undang Hukum Pidana*), the Electronic Information and Transactions Law, the Personal Data Protection Law, and other relevant regulations concerning technology-facilitated criminal conduct. The conceptual approach is used to analyze the doctrines of *actus reus*, *mens rea*, causation, culpability, criminal attribution, foreseeability, and human agency in relation to AI-based crimes. The case approach examines relevant judicial decisions and documented cases involving AI-mediated offenses, particularly deepfakes, digital fraud, impersonation, and other forms of AI-enabled criminal conduct, to identify challenges in attributing criminal responsibility. Furthermore, the comparative approach examines legal developments and approaches adopted by selected jurisdictions in addressing AI-related criminal liability. Legal materials consist of primary legal sources, including legislation, judicial decisions, and international legal instruments, as well as secondary sources comprising scholarly books, peer-reviewed journal articles, legal commentaries, and relevant academic studies published primarily within the last ten years.

The collected legal materials are analyzed through qualitative juridical analysis using systematic interpretation and deductive reasoning. The analysis first identifies the limitations of the existing Indonesian criminal liability framework and subsequently examines whether conventional principles of *actus reus* and *mens rea* remain adequate for AI-mediated crimes. The research ultimately develops a normative reconstruction of criminal liability based on control, knowledge, contribution, foreseeability, and degree of culpability, while maintaining the principles of legality and *no punishment without culpability*. This approach is intended to formulate a legally coherent framework capable of addressing the emerging accountability gap associated with AI-based criminal conduct.

RESULTS AND DISCUSSION

1. The Construction of Criminal Liability for Artificial Intelligence Based Crimes under Indonesia Criminal Law

The development of *Artificial Intelligence* (AI) has generated new forms and modalities of criminal conduct. AI can be employed as an instrument to facilitate fraud, impersonation, information manipulation, deepfake production, identity-related offenses, and various forms of cybercrime. The legal challenge arising from these developments does not merely concern

whether conduct facilitated by AI can be classified as a criminal offense, but also concerns how criminal liability should be attributed when an offense is committed through an AI system that possesses a certain degree of automation and limited predictability (Maskur et al., 2025). This complexity arises because AI may operate at different levels, ranging from a conventional technological tool that remains fully controlled by its user to a semi-autonomous system capable of generating outputs based on algorithms, data, and previously established parameters (Janssen, 2025).

Under Indonesian criminal law, criminal liability remains fundamentally grounded in the principle of culpability. Law No. 1 of 2023 on the Criminal Code (*Kitab Undang-Undang Hukum Pidana* or KUHP), which came into force on 2 January 2026, provides the general framework for criminal law in Indonesia, including its application to offenses regulated outside the Criminal Code. The principle of culpability is significant because the imposition of criminal punishment cannot be based solely on the establishment of a prohibited act; rather, there must also be a legally recognizable basis for attributing fault to an accountable legal subject (Hardianto et al., 2024).

This framework raises a fundamental question regarding the legal status of AI itself. AI cannot readily be regarded as an independent subject of criminal liability because it does not possess consciousness, intention, or normative awareness in the same manner as a human being. Accordingly, when AI is employed to produce an outcome that constitutes a criminal offense, a more appropriate approach within the existing Indonesian criminal law framework is liability through AI, whereby criminal responsibility is attributed to the human or corporate actors who use, develop, control, or otherwise have a legally relevant relationship with the AI system, rather than treating AI itself as the perpetrator of a criminal offense (Tahir, 2025).

This approach requires a distinction among the principal actors within the AI ecosystem, namely users, developers, providers, and corporations. A user may be held criminally liable when the individual intentionally employs AI as an instrument for committing an offense. For example, a person who deliberately uses an AI system to create fraudulent deepfake content and subsequently distributes it for the purpose of deceiving another person may be held responsible on the basis of the individual's own conduct and culpability. In such circumstances, the AI system functions primarily as an instrument through which the user's criminal intent is realized (Wafi et al., 2025).

The position of developers and providers, however, requires a more careful assessment. A developer should not automatically incur criminal liability merely because a technology developed by that individual or entity is subsequently misused by another person. Criminal liability should instead depend upon the existence of a legally relevant connection between the developer's conduct and the criminal outcome, including factors such as knowledge of foreseeable risks, intentional facilitation of criminal use, or serious negligence in circumstances where a specific duty of care exists. Similarly, an AI provider should not be held automatically liable for every criminal act committed by its users. The existence of liability must be determined by examining the provider's degree of control, knowledge, contribution, and capacity to prevent or mitigate the relevant criminal harm (Pane et al., 2025).

Corporate criminal liability provides an additional dimension to this analysis. The Indonesian Criminal Code expressly recognizes corporations as subjects of criminal offenses and provides a framework for attributing criminal conduct to corporations through, among others, the actions of corporate management, persons exercising control, individuals giving orders, or beneficial owners under legally prescribed circumstances. This framework creates a potential legal basis for addressing AI-related crimes committed within corporate structures, particularly where the criminal conduct results from corporate policies, inadequate supervision, deliberate risk-taking, or organizational failures (Saipudin et al., 2025).

Nevertheless, the existence of legal subjects under Indonesian criminal law does not by itself resolve the central problem of AI-related criminal liability. The fundamental difficulty lies in establishing the normative connection between an AI-generated output and the conduct and culpability of a particular human or corporate actor. An AI system may generate an output that was not expressly specified by its user, and its operation may involve complex processes that are not fully transparent or predictable. Consequently, merely identifying the person who operated, developed, or provided the AI system is insufficient to establish criminal responsibility.

Existing Indonesian legislation provides several legal bases that may be applied to conduct involving AI. The Electronic Information and Transactions Law, as amended by Law No. 1 of 2024, regulates various forms of misuse of electronic information and documents, while Law No. 27 of 2022 on Personal Data Protection establishes criminal provisions concerning, among other matters, unlawful processing, disclosure, and misuse of personal data. These provisions may be relevant to AI-mediated offenses such as deepfake-based fraud, identity-related offenses, and unlawful use of personal information. However, these regulatory instruments do not yet provide a comprehensive framework specifically addressing the attribution of criminal liability where the harmful conduct or output is generated through AI (Maruli et al., 2026).

Therefore, the principal legal problem is not necessarily the absence of criminal prohibitions, but rather the absence of an adequate attribution mechanism capable of connecting AI-mediated conduct with the culpability of the relevant actor. Certain AI-enabled conduct may already fall within existing criminal offenses, but the more complex question concerns the determination of which actor possesses the requisite level of control, knowledge, contribution, and culpability to justify the imposition of criminal punishment.

Accordingly, the Indonesian criminal law framework requires a reconstruction of attribution rather than merely an expansion of criminalization. Such reconstruction should preserve the human-centered foundation of criminal responsibility while taking into account the distinctive characteristics of AI technology. The central premise is that the use of AI should neither automatically eliminate criminal responsibility nor automatically expand liability to every actor associated with the technology. Instead, criminal liability must remain contingent upon a demonstrable and proportionate relationship between the actor's conduct, the AI-mediated process, the resulting harm, and the actor's culpability.

2. Problem of Actus Reus, Mens Rea, and Attribution of Culpability in AI – Based Crimes

The emergence of Artificial Intelligence (AI) has generated significant challenges for the application of the conventional concepts of *actus reus* and *mens rea* in criminal law. In traditional criminal offenses, the attribution of criminal liability generally depends upon the existence of a prohibited human act accompanied by the requisite mental element. However, AI-based crimes may involve multiple actors and technological processes, ranging from the formulation of prompts and development of AI systems to the generation, modification, distribution, and utilization of AI-generated outputs. Consequently, determining which conduct constitutes the legally relevant *actus reus* and whose mental state satisfies the *mens rea* requirement becomes considerably more complex.

From the perspective of *actus reus*, the use of AI should not automatically result in the attribution of the entire criminal conduct to the individual who operates the system. The relevant conduct must instead be examined throughout the technological chain leading to the commission of the offense (Velasco, 2022). For instance, in a deepfake-based fraud, the legally relevant conduct may involve the creation of manipulated content, the intentional alteration of a person's identity, the distribution of the fabricated material, and its subsequent use to induce another person to transfer money or disclose personal information. Each stage may involve different actors with varying degrees of control and contribution. Therefore, the attribution of *actus reus* requires an assessment of whether a particular actor's conduct constituted a substantial and legally relevant contribution to the criminal outcome (Saud, 2023).

The complexity becomes even greater when AI systems operate with a significant degree of automation. An AI system may generate content that was not precisely anticipated by its user or developer. In such circumstances, the mere causal connection between the operation of an AI system and the resulting harm should not be sufficient to establish criminal liability. Criminal law requires a stronger normative connection between the conduct of an individual and the prohibited consequence. Accordingly, the assessment of *actus reus* should consider the actor's degree of control over the system, the nature of the instruction provided, the extent of the actor's intervention, and the contribution of the resulting AI output to the commission of the offense.

The concept of *mens rea* presents an equally fundamental challenge. AI systems do not possess human consciousness, moral awareness, or legally recognizable intention. Therefore, attributing *mens rea* directly to an AI system would be inconsistent with the traditional

foundation of criminal responsibility. The relevant inquiry must instead focus on the mental state of the human or corporate actors behind the AI-mediated conduct. This includes determining whether the actor possessed knowledge of the circumstances, intended the prohibited consequence, foresaw the potential harm, or consciously disregarded a substantial and foreseeable risk arising from the use or deployment of the AI system (Hashmi et al., 2025).

In this context, foreseeability becomes an important parameter in determining criminal culpability. Where an actor deliberately designs, configures, instructs, or deploys an AI system for the purpose of facilitating a criminal offense, the existence of criminal intent may be established more readily. By contrast, where an AI system produces an unexpected outcome despite reasonable precautions, the mere occurrence of a harmful consequence should not automatically establish *mens rea*. The distinction is particularly important for developers and providers, whose technological contribution may be several steps removed from the ultimate criminal act.

Accordingly, developers and AI service providers should not be held criminally liable solely because their technology has been misused by another person. Such an approach would create an excessively broad form of attribution and potentially undermine the principle of individual culpability. Criminal liability should instead depend upon the existence of a legally relevant relationship between the actor and the criminal outcome. Relevant factors may include the actor's knowledge of the potential misuse, the degree of control exercised over the system, the extent of contribution to the criminal conduct, the foreseeability of the resulting harm, and the existence of a specific duty to prevent or mitigate such harm.

The concept of attribution of culpability therefore functions as a bridge between *actus reus* and *mens rea*. In AI-based crimes, establishing a physical or causal connection between an actor and an AI-generated outcome is insufficient without demonstrating that the actor can normatively be held responsible for that outcome. Attribution must consequently be based on a combination of factual causation and normative responsibility. This approach prevents two opposite risks: the over-attribution of criminal liability to actors who merely provide legitimate technological infrastructure and the under-attribution of liability to actors who deliberately exploit AI systems or recklessly disregard foreseeable risks (Dremluga & Prisiekina, 2020).

Based on this analysis, five parameters may be employed in determining criminal culpability in AI-mediated offenses: (1) control, (2) knowledge, (3) contribution, (4) foreseeability, and (5) degree of culpability. Control determines the extent to which an actor was capable of directing or influencing the AI system. Knowledge concerns the actor's awareness of the relevant circumstances and potential misuse. Contribution assesses the extent to which the actor's conduct facilitated the commission of the offense. Foreseeability examines whether the criminal consequence could reasonably have been anticipated. Finally, the degree of culpability determines whether the actor acted intentionally, recklessly, negligently, or without sufficient fault to justify criminal punishment.

This framework is particularly important because AI-based criminal conduct often involves an ecosystem rather than a single identifiable perpetrator. Users, developers, providers, corporations, and other actors may occupy different positions within the technological chain and therefore possess different levels of control, knowledge, and responsibility. A uniform attribution model would consequently be unable to adequately reflect these differences. Criminal liability should instead be proportionate to each actor's actual relationship with the criminal conduct and the resulting harm.

Thus, the central challenge of AI-based criminal liability does not merely concern the identification of the person who technically operated an AI system. It concerns the reconstruction of the normative relationship between human conduct, technological operation, criminal consequence, and culpability. The application of *actus reus* and *mens rea* in the AI context therefore requires a more contextual and relational approach, while maintaining the fundamental principle that criminal punishment must be grounded in attributable human culpability. Such an approach provides the doctrinal foundation for developing a more proportionate and legally certain framework of criminal liability for AI-based crimes in Indonesia.

3. Reconstruction of Criminal Liability for AI – Based Crimes in Indonesia Criminal Law

The preceding analysis demonstrates that the principal challenge posed by AI-based crimes in Indonesia is not merely the absence of criminal prohibitions, but the inadequacy of existing mechanisms for attributing criminal responsibility in technologically mediated conduct. The increasing autonomy, complexity, and unpredictability of AI systems may create a gap between the person who initiates or controls the technological process and the criminal consequence ultimately produced. Accordingly, the reconstruction of criminal liability should focus on developing an attribution framework capable of connecting human conduct, AI-mediated processes, criminal consequences, and culpability without treating Artificial Intelligence as an independent criminal subject (Panji et al., 2024).

The reconstruction should begin by maintaining the fundamental principle that criminal liability must be based upon human culpability. AI should not be positioned as a substitute for the human subject of criminal responsibility because an AI system does not possess consciousness, moral judgment, or legally recognizable intention. Instead, AI should be understood as an instrument, intermediary, or technological mechanism through which human or corporate conduct may produce criminal consequences. This approach preserves the principle of *no punishment without culpability* while allowing criminal law to respond to technologically sophisticated forms of offending (Monga, 2023).

A reconstructed model should therefore move beyond a purely actor-centered approach toward a relationship – based attribution model. Under a conventional approach, the principal question is often who performed the prohibited act. In AI-mediated crimes, however, this question may be insufficient because the criminal outcome can emerge from interactions among users, developers, providers, operators, and corporate entities. The relevant inquiry should consequently examine the relationship between each actor and the AI system, particularly their degree of control, knowledge, contribution, foreseeability, and culpability.

On this basis, criminal liability for AI-based crimes may be reconstructed through five principal attribution parameters. **First, control** refers to the actor's ability to direct, configure, supervise, modify, or terminate the AI system or its relevant operation. The greater the actor's control over the technological process, the stronger the basis for attributing the resulting conduct to that actor. A user who deliberately instructs an AI system to generate fraudulent content, for example, possesses a substantially different level of control from an individual who merely encounters or receives AI-generated content without influencing its creation (Osmani, 2020).

Second, knowledge concerns the actor's awareness of the relevant circumstances and the potential criminal use or consequences of the AI system. Knowledge becomes particularly significant where the actor is aware that the system is being used to facilitate unlawful conduct but nevertheless continues to provide instructions, resources, or technological support. For developers and providers, however, general awareness that AI technology may be misused should not automatically constitute sufficient knowledge for criminal liability. The assessment should focus on whether there was specific or sufficiently foreseeable knowledge of the relevant misuse and whether the actor had a meaningful capacity to respond to it (Nersessian & Mancha, 2021).

Third, contribution concerns the extent to which an actor's conduct materially facilitated the commission of the offense. This parameter is necessary because AI-based crimes may involve distributed forms of participation. A developer who creates a general-purpose AI system, a provider that operates the infrastructure, and a user who intentionally employs the system to commit fraud may all contribute to the technological process, but their contributions are not necessarily equivalent in legal significance. Criminal attribution must therefore distinguish between legitimate technological contribution and contribution that is sufficiently connected to the commission of a specific offense (Tong, 2025).

Fourth, foreseeability evaluates whether the criminal consequence could reasonably have been anticipated based on the actor's knowledge, position, expertise, and control over the AI system. Foreseeability is particularly relevant in determining whether an unexpected AI-generated outcome can legitimately be attributed to a particular actor. Where a harmful consequence is highly predictable and the actor possesses the capacity to prevent or mitigate it, failure to take reasonable precautions may support a finding of culpability. Conversely, where the consequence is genuinely unforeseeable and the actor has exercised reasonable care, criminal attribution should be limited (Fraser & Suzor, 2025).

Fifth, degree of culpability determines the normative seriousness of the actor's conduct. The existence of a causal contribution alone should not automatically result in criminal punishment. The law must distinguish between intentional conduct, conscious disregard of substantial risks, negligence, and conduct lacking sufficient culpability. This parameter ensures proportionality between the actor's mental state and the severity of the criminal response (Dremluiga & Prisekina, 2020).

These five parameters can be integrated into a three-stage AI Criminal Liability Attribution Model. The first stage is attribution of conduct, which identifies the relevant human or corporate conduct within the AI technological chain. The second stage is attribution of culpability, which evaluates the actor's knowledge, intention, foreseeability, control, and contribution. The third stage is proportional attribution of criminal liability, which determines whether and to what extent the actor should bear criminal responsibility based on the degree of culpability established. Under this model, the liability of AI users should generally be assessed according to their direct involvement in the criminal conduct. Where a user intentionally employs AI to produce or facilitate an unlawful result, the existence of *actus reus* and *mens rea* may be established through the user's conduct and intention, with AI functioning merely as the technological means of execution. In such circumstances, the use of AI should not constitute a barrier to criminal liability.

The position of developers and providers requires a more differentiated approach. They should not be held criminally liable merely because their systems are capable of being misused. Liability may become relevant where there is evidence of intentional facilitation, actual knowledge of specific criminal misuse, substantial control over the relevant system, serious disregard of foreseeable criminal risks, or a legally recognized duty to implement reasonable safeguards. Such a framework avoids imposing excessive criminal responsibility on technological actors while ensuring that deliberate or seriously culpable forms of facilitation do not remain beyond the reach of criminal law.

Corporate liability also requires particular attention because AI systems are frequently developed, deployed, and controlled through organizational structures. Corporate criminal responsibility should therefore examine not only the conduct of individual employees but also the organizational decision-making processes that permitted, encouraged, or failed to prevent foreseeable criminal misuse. Relevant considerations may include managerial authority, internal compliance mechanisms, risk-management procedures, supervisory failures, and the corporation's ability to prevent or mitigate the relevant harm. This approach allows corporate liability to reflect the organizational nature of contemporary AI development and deployment (Tache & Valcu, 2025).

The reconstruction should nevertheless avoid the excessive expansion of strict liability. Making technological actors automatically responsible for every criminal consequence generated through their systems would undermine the principle of culpability and create an unreasonable burden on innovation and technological development. Strict or vicarious forms of liability should therefore remain exceptional and must be justified by clear statutory provisions and compelling legal considerations. The primary model should remain one of individualized and proportionate culpability.

The proposed reconstruction can consequently be formulated as follows: AI-based criminal conduct, identification of relevant human or corporate actors, assessment of control, assessment of knowledge, assessment of contribution, assessment of foreseeability, determination of culpability, and proportional criminal liability. This sequence provides a structured mechanism for courts and law enforcement authorities to determine responsibility without automatically attributing every AI-generated consequence to a single actor.

The originality of this reconstruction lies in shifting the focus from the question of whether AI itself should be criminally responsible toward the more fundamental question of how culpability should be attributed when human conduct is mediated by increasingly autonomous technological systems. Rather than creating a new criminal subject, the proposed framework adapts existing principles of criminal responsibility to the technological characteristics of AI. It therefore seeks to close the accountability gap while maintaining legality, culpability, proportionality, and legal certainty as fundamental principles of Indonesian criminal law.

Ultimately, the reconstruction of criminal liability for AI-based crimes should establish a balanced framework between technological innovation and criminal accountability. Indonesian criminal law should neither allow AI to become a mechanism for avoiding responsibility nor transform every participant in the AI ecosystem into a potential criminal offender. A differentiated attribution model based on control, knowledge, contribution, foreseeability, and culpability offers a more coherent basis for determining responsibility. Through this approach, Indonesian criminal law can remain human-centered while becoming sufficiently adaptive to address emerging forms of AI-mediated criminal conduct.

CONCLUSION

This study demonstrates that the emergence of AI-based crimes exposes a structural limitation in the Indonesian criminal liability framework, not primarily because existing criminal law lacks prohibitions applicable to AI-mediated conduct, but because conventional mechanisms of attributing *actus reus*, *mens rea*, and culpability are insufficiently equipped to address technologically distributed, automated, and potentially unpredictable forms of criminal conduct. The analysis confirms that Artificial Intelligence should not be constructed as an autonomous subject of criminal responsibility, since criminal liability must remain anchored in human or corporate culpability and the principle of *no punishment without culpability*. Nevertheless, maintaining a human-centered foundation does not require retaining an exclusively actor-centered attribution model. The principal contribution of this study is therefore the reconstruction of criminal liability through a relationship-based and proportionate attribution framework that assesses five cumulative parameters—control, knowledge, contribution, foreseeability, and degree of culpability—through three sequential stages: attribution of conduct, attribution of culpability, and proportional attribution of criminal liability. This model provides a normative basis for distinguishing the responsibility of users, developers, providers, and corporations according to their actual relationship with the AI-mediated offense, thereby preventing both excessive attribution to legitimate technological actors and accountability gaps for actors who intentionally facilitate or recklessly disregard foreseeable criminal risks. The proposed reconstruction contributes to the development of contemporary criminal law doctrine by adapting established principles of criminal responsibility to the distinctive characteristics of AI without creating an artificial criminal subject or resorting prematurely to strict or vicarious liability. For Indonesian criminal law, this framework implies the need for clearer statutory standards governing AI-related attribution, particularly regarding control, foreseeability, technological contribution, and organizational culpability, while preserving legality, proportionality, legal certainty, and culpability as fundamental safeguards. Ultimately, an adaptive yet restrained attribution framework offers Indonesia a more coherent basis for responding to AI-based crimes while maintaining an appropriate balance between technological innovation, individual rights, and effective criminal accountability.

REFERENCES

- Dremluga, R., & Prisekina, N. (2020). The Concept of Culpability in Criminal Law and AI Systems. *Journal of Politics and Law*, 13(3), 256–262. <https://doi.org/10.5539/jpl.v13n3p256>
- Fraser, H. L., & Suzor, N. P. (2025). Locating fault for AI harms : a systems theory of foreseeability , reasonable care and causal responsibility in the AI value chain. *Law, Innovation and Technology*, 17(1), 103–138. <https://doi.org/10.1080/17579961.2025.2469345>
- Günsberg, P. S. (2022). Automated vehicles – is a dilution of human responsibility the answer ? *New Journal of European Criminal Law*, 13(4), 439–451. <https://doi.org/10.1177/20322844221138049>
- Hardianto, A., Arief, B. N., Setiyono, J., Fernando, Zico, J., & Sabrina, N. (2024). Critical Analysis of Living Law Formulation in Law No. 1 of 2023 Concerning the Criminal Code: Towards Law Reform to Realize Justice with the Spirit of Pancasila. *Journal of Law and Legal Reform*, 5(3), 1029–1066. <https://doi.org/https://doi.org/10.15294/jllr.v5i3.13923>
- Hashmi, M. A. I., Butt, M. F., Jawad, M., & Sultan, S. (2025). The Critical Review of Social Sciences Studies Criminal Liability in the Age of Autonomous Systems : Rethinking Mens Rea Understanding Autonomous Systems and Criminal Law. *The Critical Review of Social Sciences Studies*, 3(3), 290–303. <https://doi.org/https://doi.org/10.59075/szbtkr93>
- Janssen, M. (2025). Responsible governance of generative AI : conceptualizing GenAI as complex adaptive systems. *Policy and Society*, 44(1), 38–51.

- <https://doi.org/https://doi.org/10.1093/polsoc/puae040>
- Maruli, S., Situmeang, T., & Pudjiastuti, D. (2026). ADEQUACY OF INDONESIAN CYBERCRIMINAL LAW AGAINST GENERATIVE AI-BASED SOCIAL ENGINEERING ATTACKS. *Res Nullis Law Journal*, 7(1), 82–97. <https://doi.org/https://doi.org/10.34010/rmlj.v6i1.19927>
- Maskur, M. A., Masyhar, A., Damayanti, R., Ramada, D. P., & Sanyal, S. (2025). Reimagining Criminal Liability in the Age of Artificial Intelligence: Toward a Comparative and Reform-Oriented Legal Framework. *Journal of Law and Legal Reform*, 6(4), 1805 = 1838. <https://doi.org/https://doi.org/10.15294/jllr.v6i4.35540>
- Monga, G. (2023). LEGAL ACCOUNTABILITY OF AUTONOMOUS AI SYSTEMS IN CRIMINAL JUSTICE. *Shodhkosh: Jurnal of Visual and Performing Arts*, 5848–5852. <https://doi.org/https://doi.org/10.29121/shodhkosh.v4.i2.2023.6172>
- Nersessian, D., & Mancha, R. (2021). From Automation to Autonomy: Legal and Ethical Responsibility Gaps in Artificial Intelligence Innovation. *Michigan Technology Law Review*, 27(2020). <https://doi.org/https://doi.org/10.36645/mtlr.27.1.from>
- Osmani, N. (2020). THE COMPLEXITY OF CRIMINAL LIABILITY OF AI SYSTEMS. *Masaryk University Journal of Law and Technology*, 14(1), 53–82. <https://doi.org/10.5817/MUJLT2020-1-3>
- Pane, M. D., Zein, M., & Permana, S. (2025). PERTANGGUNGJAWABAN PIDANA TERHADAP PENGEMBANG ARTIFICIAL INTELLIGENCE PADA KASUS PELANGGARAN PRIVASI DAN DATA PRIBADI. *Judge: Jurnal Hukum*, 06(03), 467–472. <https://doi.org/doi.org/10.54209/judge.v6i03.1593>
- Panji, K., Adi, K., Darma, I. M. W., & Kurniawan, I. G. A. (2024). Artificial Intelligence and Criminal Liability Challenges for Contemporary Penal Law. *Pena Justitia: Media Komunikasi Dan Kajian Ilmu Hukum*, 23(2), 5868–5879. <https://doi.org/https://doi.org/10.31941/pj.v23i2.7502>
- Sachoulidou, A. (2024). AI Systems and Criminal Liability. *Oslo Law Review*, 11(1), 1–10. <https://doi.org/https://doi.org/10.18261/olr.11.1.3>
- Saipudin, L., HS, S., Rodliyah, & Wulandari, L. (2025). The Concept of Corporate Criminal Liability in the Indonesian Criminal Law System. *Jurnal IUS Kajian Hukum Dan Keadilan*, 13(2), 2303–3827. <https://doi.org/https://doi.org/10.29303/ius.v13i2.1817>
- Saud, A. (2023). Criminal Liability about the Use of Artificial Intelligence : Investigating the Actus Reus Element of AI-driven Technology Criminal Liability about the Use of Artificial Intelligence : Investigating the Actus Reus Element of AI-driven Technology. *American Journal of Law*, 6(1), 1–25. <https://doi.org/https://doi.org/10.47672/ajl.1648>
- Tache, C. E. P., & Valcu, E. N. (2025). Artificial Intelligence and Corporate Liability Towards a New Legal-Ethical Contract in the Dynamics of Emerging Global Human Rights Convergences. *Juridical Tribune Review of Comparative and International Law*, 15(2), 281–305. <https://doi.org/10.62768/TBJ/2025/15/2/04>
- Tahir, A. (2025). Challenges of Criminal Liability Related to Artificial Intelligence (AI) in Indonesia: Lessons from European Law. *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, 12(2), 306–323. <https://doi.org/10.24252/jurisprudentie.v12i2.63121>
- Tong, M. (2025). The New Actor: Artificial Intelligence in Criminology and Criminal Justice. *Criminology, Criminal Justice, Law & Society*, 26(12), 12–22. <https://doi.org/https://doi.org/10.54555/CCJLS.13020.146572>
- Velasco, C. (2022). Cybercrime and Artificial Intelligence . An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, 23, 109–126. <https://doi.org/10.1007/s12027-022-00702-z>
- Wafi, M. S., Wisnubroto, A., & Prayudi, Y. (2025). Kejahatan Deepfake Berbasis Artificial Intelligence: Suatu Konsepsi pada Penggunaan Asas Culpabilitas Sebagai Pembaharuan Pertanggungjawaban Pidana. *Reformasi Hukum*, 29(2), 168–183. <https://doi.org/https://doi.org/10.46257/jrh.v29i2.1304>