



Overcoming Cybercrime and Artificial Intelligence: Difficulties in Indonesia's Criminal Law Reform

Sahat Maruli Tua Situmeang , Tri Mulqi Pra Fitri

Universitas Komputer Indonesia, Bandung, Indonesia
sahat@email.unikom.ac.id

Abstract. The landscape of cybercrime in the digital age has significantly changed due to the rapid development of artificial intelligence (AI). Novel criminal paradigms, including automated hacks, deepfake-based deceptions, algorithmic manipulations, and extensive data exploitation, have emerged as a result of AI-driven technologies. These developments put pressure on established legal frameworks, which were designed to address classic cyberthreats. The regulatory obstacles to controlling AI and cybercrime within Indonesia's criminal law system are examined in this study. It examines current laws on cybercrime, digital oversight, and emerging AI technologies using a normative juridical approach with statutory and conceptual lenses. The analysis incorporates perspectives from academics such as Luciano Floridi and Lawrence Lessig, who highlight the increasing influence of digital architectures and algorithms over human behavior and legal accountability. The findings show that Indonesia's current legislative framework, particularly those pertaining to electronic information and transactions, is insufficient to handle the complexities of cybercrime driven by artificial intelligence. There are still significant gaps in defining criminal responsibility, assigning blame for algorithmic choices, and addressing international digital violations. Therefore, in order to create robust regulatory frameworks that are sensitive to the dynamic nature of cybercrime in the context of AI spread, criminal law reform is essential.

Keywords: Artificial Intelligence; Cybercrime; Criminal Law Reform.

1 Introduction

The quick development of artificial intelligence (AI) has drastically changed the dynamics of cybercrime by making it possible for more complex, automated, and widespread types of digital crime, such as deepfake-based fraud, large-scale personal data exploitation, AI-assisted hacking, and algorithmically driven disinformation campaigns [1]. These innovations raise difficult issues about purpose, causality, and the distribution of liability in human-machine interactions because they put pressure on established criminal law concepts that were created for human-centered behavior and traditional cyber offenses in many countries [2]. This conflict is especially evident in the area of cybercrime within the Indonesian legal system, where AI is being utilized more and

more to both commit crimes and assist law enforcement, but the underlying regulatory framework is still disjointed and only partially responsive to concerns unique to AI [3].

The Law on Electronic Information and Transactions (Undang-Undang Informasi dan Transaksi Elektronik, UU ITE) and its implementing regulations, which are Indonesia's principal cyber-related legal instruments, were drafted in response to early-generation cyberthreats like online defamation, data interference, and unauthorized access [4]. While these provisions offer a fundamental legal framework for combating cybercrime, they do not fully account for AI-driven harms like deepfakes created by AI, autonomous malware, and sophisticated algorithmic systems whose outputs could cause serious harm without direct or ongoing human control [5]. Therefore, there are still significant gaps in the identification of the pertinent subject of criminal liability, the attribution of culpability to AI system developers, providers, and users, and the handling of cross-border, platform-based offenses that are enabled by globally dispersed digital infrastructures [6].

The emergence of AI and algorithmic systems calls into question long-held beliefs about how the law governs behavior, according to current theoretical discussions in cyber law and digital ethics. The regulatory potential of digital architecture and software design is highlighted by Lessig's concept that "code is law," which contends that technical artifacts can serve as normative restraints on par with or even more successfully than formal legal regulations [7]. Simultaneously, Floridi's research on information ethics and AI governance highlights the necessity of accountability frameworks that acknowledge the multi-layered nature of responsibility in socio-technical systems, where human agents, institutions, and autonomous or semi-autonomous systems interact in intricate ways [8]. These viewpoints offer a helpful conceptual framework for examining Indonesia's present strategy for combating AI-related cybercrime, which frequently relies on general laws while the underlying social and technological realities change quickly [9].

The current legal structure does not yet offer sufficient legal certainty or efficient accountability mechanisms for AI-based offenses, as recent Indonesian scholarship on AI, cybercrime, and criminal responsibility has started to map these issues more methodically [3]. Studies on criminal culpability for the use of AI in Indonesia contend that as AI is an electronic system, it cannot be regarded as a traditional legal topic and that those who create, implement, or run AI systems are still primarily responsible [1]. Additional studies on AI and criminal law reform emphasize how urgent it is to update cybercrime laws in order to make it clearer who is responsible for what, improve the definitions of offenses, and create more flexible legal guidelines for crimes enabled by AI [10]. At the same time, comparative studies with the EU and new evaluations of Indonesian cybercrime policy in the context of AI abuse show how risk-based and technology-sensitive approaches should guide future changes to Indonesia's criminal code [9].

In light of this, this paper explores the difficulties in regulating cybercrime and artificial intelligence within Indonesia's criminal justice system and makes the case for the need for conceptually sound and technologically advanced criminal law reform. The study examines current Indonesian rules on cybercrime, digital governance, and AI-

related activities using a normative juridical methodology with a statutory and conceptual approach. It then places these regulations within larger theoretical discussions on digital regulation and AI governance [4]. The ultimate goal is to develop fundamental ideas and strategies for criminal law reform that can better address Indonesia's changing AI-driven cybercrime landscape, bolster legal accountability and certainty, and improve the criminal justice system's ability to adapt to new technological advancements.

2 Literature Review

In modern legal study, both internationally and in Indonesia, the connection between artificial intelligence and cybercrime has grown in importance. Early research on cybercrime and criminal law in the AI era highlights how AI can be used to perform increasingly sophisticated and automated cybercrimes as well as to improve cybersecurity. These studies highlight how AI-driven cybercrime exposes the limitations of current doctrinal and regulatory approaches by challenging traditional criminal law ideas based on direct human activity, individual perpetrators, and territorially confined offenses [9].

The implications of AI on criminal law policy and cybercrime regulation are the subject of an increasing amount of Indonesian scholarship. The Electronic Information and Transactions Law (UU ITE) is currently insufficient to address developing AI-related threats, notably autonomous or semi-autonomous forms of digital harm, according to Novrianto's review of Indonesia's criminal law strategy on AI-based crimes [4]. In addition to recommending the creation of specific legislation on AI to supplement current cybercrime rules, his report highlights flaws in the definitions of offenses, the extent of regulated action, and the distribution of criminal liability [4]. In addition, Senjaya and others contend that AI-based cybercrimes reveal a more widespread "crisis of criminal responsibility" in Indonesian law since current paradigms that focus on individual offenders and traditional intent are becoming less and less equipped to account for digitally mediated wrongdoing [11].

The issue of criminal culpability for the use of AI in Indonesia is the subject of other studies. According to Purnomo's normative legal research, AI cannot be regarded as an autonomous legal subject within the current Indonesian criminal law framework since it lacks moral blameworthiness, willpower, and an awareness of norms [1]. As a result, natural and legal persons who create, manage, and implement AI systems are nonetheless held accountable, which presents complex issues regarding the allocation of culpability among developers, system providers, and end users [1].

Related research on the lack of criminal accountability standards for AI further emphasizes that the lack of clear regulations regarding AI as a source of risk and an object of regulation creates legal uncertainty, especially when AI systems operate with a high degree of autonomy or have unintended negative consequences [12]. According to these studies, Indonesia has a normative gap when it comes to determining who should be held responsible and under what circumstances when AI systems are connected to criminal activity [1].

However, Indonesian literature on the legal ramifications of AI for digital rights and personal data security expands the conversation beyond principles of criminal law. The application of AI in industries like finance, governance, and digital services increases the risks of widespread data misuse, profiling, and privacy violations, according to analyses of AI and personal data protection. This puts pressure on regulatory tools like the Personal Data Protection Law (UU PDP) [13]. These studies emphasize that a sectoral, compartmentalized approach is insufficient to address the cross-cutting nature of AI threats and that AI-related harms frequently appear as a continuum of administrative, civil, and criminal wrongs [13]. The results support the claim that any changes to Indonesia's criminal code pertaining to AI and cybercrime must be coordinated with more comprehensive frameworks on digital governance, consumer protection, and data protection [13].

An essential conceptual framework for these Indonesian discussions is provided by theoretical and international literature. Digital architectures, including AI and algorithmic systems, are framed by Lessig's seminal concept that "code is law" as regulatory frameworks that, along with laws, markets, and social conventions, shape and regulate behavior [7]. This viewpoint has been used extensively to explain how design, default settings, and technical affordances allow AI systems to successfully govern users and embed normative choices [7]. Simultaneously, Floridi and other scholars of information ethics have created frameworks for the governance of AI that emphasize the necessity of "soft ethics" and layered accountability mechanisms to supplement hard law, particularly in situations where traditional legal categories fall behind technological complexity [14]. These theoretical approaches have started to be used in Indonesian legal academia to support the idea that criminal law reform in the context of AI should address the design and governance of digital architectures as well as modify the definitions and penalties of offenses [5].

In order to address AI-driven cybercrime in a more methodical and technologically aware way, national criminal law must be reformed, according to recent Indonesian and comparative studies. The fragmentation of current rules, the absence of precise standards on AI safety and transparency, and the poor integration between criminal law and sectoral regulations are all highlighted in works on cybersecurity and AI regulation in Indonesia [3]. To ensure effective enforcement and legal clarity, research on cybercrime law reform including evaluations of AI misuse and comparisons to European Union approaches suggests that risk-based regulation, more precise attribution regulations, and updated evidentiary standards are required [15]. These conclusions are supported by more recent research on "cyber crime and criminal law in the era of AI," which emphasizes the necessity of elucidating the legal status and responsibilities of AI within the national criminal law system and suggests doctrinal and policy avenues for future change [16].

When considered collectively, the literature shows that: (i) AI increases the scope and complexity of cybercrime; (ii) AI-specific risks have not yet been fully anticipated by Indonesian positive law, especially UU ITE and related instruments; (iii) there is a substantial normative gap regarding the attribution of criminal liability for conduct mediated by AI; and (iv) theoretical insights on code, architecture, and AI governance offer helpful guidance for creating more flexible and cohesive criminal law reforms.

By methodically analyzing how Indonesia's criminal code might be changed to combat AI-driven cybercrime, this paper places itself inside these discussions by referencing both domestic research and foreign theoretical contributions.

3 Methodology

In order to analyze law as a normative system made up of norms, principles, and doctrines, this study uses the normative juridical technique, which is frequently employed in Indonesian legal studies. This viewpoint approaches law as *das sollen* rather than *das sein*, so the main emphasis is on the internal coherence, systematic structure, and normative consequences of positive legal norms rather than empirical conduct or social practices [17]. Given that the primary goals of this study are to evaluate the effectiveness of current Indonesian rules in combating AI-driven cybercrime and to develop recommendations for criminal law reform, the selection of a normative juridical approach is appropriate [18].

This study's primary analytical frameworks are a statutory approach and a conceptual approach, both of which are in line with the normative juridical tradition. The Law on Electronic Information and Transactions (UU ITE), its amendments, implementing regulations, sectoral legislation, and other pertinent legal instruments governing cybercrime, electronic information and transactions, personal data protection, and related aspects of digital governance in Indonesia are examined using the statutory approach [19]. By using this method, the research methodically determines the extent of regulation, important legal definitions, offense definitions, and sanction structures, as well as possible normative gaps, overlaps, and inconsistencies with regard to AI-based behavior [15]. The examination also takes into account how well or poorly these statutory provisions reflect current advancements in AI technology and cybercrime enabled by AI [3].

Artificial intelligence, cybercrime, criminal responsibility, *mens rea*, autonomy, and accountability are just a few of the legal and theoretical concepts that are crucial to the topics under study and are clarified and critically evaluated using the conceptual method. According to Indonesian conceptual legal research, this method examines terms' meaning, structure, and significance for legal reasoning and regulation design rather than just describing them [20]. In order to place Indonesian law within larger scholarly discussions, the research engages with both Indonesian and international doctrinal and theoretical literature, including works on information ethics and AI governance as well as classic theories on the regulatory role of code and digital architecture [14]. A more accurate and logical framework for evaluating how the Indonesian criminal justice system should handle AI-driven cybercrime is constructed using this conceptual approach [21].

This study uses primary, secondary, and tertiary legal literature as its sources. Legislation, government rules, and other legally binding documents pertaining to cybercrime, electronic information and transactions, personal data protection, and criminal procedure in Indonesia are examples of primary legal resources [19]. Academic books, journal articles, research papers, and policy documents that address AI, cybercrime,

criminal culpability, and legal reform in Indonesia and other comparable countries are examples of secondary legal materials. Legal dictionaries, encyclopedias, and reliable online databases are examples of tertiary legal resources that are used to promote terminology clarification and cross-check interpretations of important ideas [17]. By methodically locating, choosing, and evaluating pertinent legal texts and scholarly works from libraries, official government websites, and reliable academic databases like Google Scholar and journal portals, data is gathered through literature study and document analysis. Qualitative normative analysis is the method of analysis employed in this study. The gathered legal resources are first arranged and categorized using topical categories, such as models of criminal law reform, forms of AI-driven cybercrime, regulatory scope of AI, and attribution of criminal liability [22].

The consistency, adequacy, and policy orientation of the current regulatory framework are then assessed by interpreting the materials using legal reasoning, particularly systematic, teleological, and comparative interpretations [20]. In order to demonstrate alternative regulatory models for AI and cybercrime that could guide Indonesian legal change, the study also, when appropriate, draws on comparative lessons from foreign and international instruments [15]. The analysis's findings are given in a descriptive-analytical style that combines normative reasoning, critical evaluation, and positive law exposition to suggest guidelines and principles for Indonesia's criminal law reform in response to AI-driven cybercrime [9].

4 Discussion

4.1 Limitations of Indonesia's Existing Cybercrime Framework for AI-Driven Offences

The Electronic Information and Transactions Law (UU ITE) and its implementing regulations serve as the foundation for Indonesia's current cybercrime law, which was written with an emphasis on traditional cybercrimes like online defamation, data interference, and unauthorized access rather than risks unique to artificial intelligence [15]. The normative framework of UU ITE is more appropriate for traditional types of hacking, data theft, and online fraud than for autonomous or semi-autonomous AI-driven operations since it requires direct human supervision over the relevant conduct, as multiple studies have demonstrated [15]. When AI systems produce dangerous outputs like deepfakes, automated phishing, or self-learning malware without constant human involvement at the time the harm manifests, this results in a structural mismatch [3].

This mismatch leads to substantial normative gaps in the definition and scope of offenses, according to research on AI-based cybercrime in Indonesia. For instance, Pakpahan's analysis of cybercrime laws pertaining to AI misuse finds that current regulations do not specifically acknowledge AI-generated content and autonomous AI behavior as separate regulatory objects, creating ambiguity regarding whether specific AI-mediated harms are covered by current offence formulations [15]. Similar to this, Anggraeny's work on the urgency of cybercrime law reform demonstrates that UU ITE is still fragmented and reactive, handling problems one at a time rather than offering a cogent, forward-looking framework for threats associated with AI. As a result, in order

to classify AI-mediated behavior within standard offense categories, law enforcement officials must "stretch" established norms or rely on analogical reasoning, which may jeopardize legal certainty and the legality principle [9].

The restriction is especially evident when cross-border AI-driven cybercrime is involved. While Indonesian law is still founded on territorial concepts of jurisdiction and infrastructure-based links, AI systems can be deployed in one jurisdiction, hosted in another, and harm many others at the same time. Many civil law systems, including Indonesia, have not yet completely adapted their cooperation and jurisdictional processes to the realities of global, platform-based AI operations, according to comparative studies on criminal responsibility for AI-based cybercrime. In actuality, this means that technical, institutional, and jurisdictional constraints not fully foreseen by the current regulatory framework frequently limit the ability to investigate, attribute, and punish AI-related offenses, even in cases when harm occurs within Indonesia [23].

4.2 The Crisis of Criminal Responsibility in AI-Related Cybercrime

The challenge of assigning criminal responsibility for AI-driven cybercrime is one of the main problems mentioned in the introduction. As a result of the conflict between conventional fault-based doctrines and the technological features of AI, Indonesian research is increasingly characterizing this as a "crisis of criminal responsibility" [24]. According to Purnomo's research on criminal liability for AI use in Indonesia, the current framework treats AI only as an electronic system or tool rather than as a separate legal entity with criminal accountability. Therefore, even when the negative result is partially caused by autonomous system behavior or intricate machine learning processes, human developers, operators, or users who design, program, or install AI systems are held accountable [1].

When AI systems function in ways that are opaque, unpredictable, or substantially disconnected from the original human input, this human-centered concept of liability becomes problematic. According to studies on the lack of AI criminal accountability standards, it is challenging to fit the resulting harm into the traditional concepts of intent (*dolus*), negligence (*culpa*), and causation as understood in Indonesian criminal law when AI operates with a high degree of autonomy or produces emergent behavior. Both offenders and victims may have legal confusion as a result of the lack of clear guidelines about the distribution of liability in such circumstances, which may lead to gaps where no party may be held completely liable under current doctrines [12].

Several potential models to address this dilemma are suggested by recent doctrinal work on the legal culpability of AI in criminal law. Some authors support a more sophisticated human-centered strategy that combines classic fault-based liability with ideas like strict liability for high-risk AI operations, vicarious liability, or risk management duties placed on developers and operators. Others propose investigating restricted functional or "quasi-subject" status for AI in particular regulatory circumstances, not to grant AI full legal personhood but rather to better organize accountability and insurance mechanisms [25].

Nonetheless, the majority of Indonesian observers concur that the current lack of precise normative guidelines on AI's place in the criminal law system causes inconsistencies in reality, with prosecutors and judges coming up with solutions on a case-by-case basis [26]. This supports the claim that explicit legislative action is necessary to address the criminal culpability dilemma in AI-related cybercrime rather than relying just on case law [27].

4.3 Digital Architecture, "Code as Law," and the Limits of Existing Regulatory Paradigms

Additionally, theoretical stances that stress the regulatory function of algorithmic systems and digital architecture were stressed in the introduction. In addition to formal legal regulations, markets, and social norms, Lessig's well-known theory that "code is law" views software design, platform architecture, and AI models as regulatory tools that influence and limit behavior. This implies that many pertinent "choices" regarding what is feasible, acceptable, or avoidable in the context of AI-driven cybercrime are integrated into the development and implementation of AI systems rather than being solely found in legal documents [7]. Building on this understanding, Floridi and other information ethics experts contend that multi-layered accountability systems that incorporate organizational rules, legal norms, and technical standards are necessary for effective AI governance [14].

The traditional "code is law" approach, however, has limitations in the era of sophisticated deep learning systems and generative AI, according to more recent research on AI governance. Judge and colleagues contend that behavior cannot be fully specified or controlled *ex ante* through code alone for opaque, data-driven models, undermining the notion that legal requirements can be easily converted into technical limitations. Because it is frequently impossible to link errors to specific code-level decisions or to prove complete compliance with normative specifications, the "black box" nature of modern AI hampers regulatory tactics that mainly rely on specification, auditing, and testing. This suggests that any attempt to control AI-driven criminality in Indonesia through design-based duties or *ex post* criminal fines is likely to be ineffective and reactive [28].

Indonesian legal study is starting to be influenced by these theoretical discussions. The existing framework does not systematically incorporate architecture-based regulation, such as technical norms for AI safety, transparency, or logging, into the criminal law response to AI-related offenses, according to authors discussing cybersecurity and AI legislation in Indonesia. Rather, the heart of regulation continues to be centered on human actors and *ex post* punishments, with architecture and code being viewed primarily as evidential or operational issues. This suggests that a more integrated strategy integrating criminal law, regulatory norms, and technical governance mechanisms is required because there is a gap between how AI systems really structure cyber risk and how the law conceptualizes control and responsibility [3].

4.4 Directions for Criminal Law Reform in Indonesia

The need for comprehensive criminal law change to combat AI-driven cybercrime is becoming more widely acknowledged in Indonesian academics due to these constraints and doctrinal conflicts. According to studies on the urgency of cybercrime law reform, it is crucial to update UU ITE and related provisions in order to establish distinct liability regimes for different actors in the AI lifecycle (developers, providers, deployers, and users), provide clear attribution rules, and improve offense definitions to cover harms caused by AI [9]. The benefits of a more structured, risk-based approach that categorizes AI applications based on their degree of risk and adjusts regulatory obligations accordingly including in the criminal law domain for high-risk or prohibited practices are highlighted by Pakpahan's comparison with the European Union [15].

Simultaneously, current research on AI's legal liability in criminal law suggests a hybrid paradigm that blends risk-based and preventive regulation with human-centered criminal culpability. Criminal law would continue to target corporate and human actors under such a model, but it would be supplemented by regulatory tools that impose ex ante responsibilities of care, security, and transparency on those who create and implement AI systems that pose serious cyber dangers. In addition to encouraging improved risk management and compliance, violations of these obligations may result in criminal culpability in situations involving significant harm [14]. Florida's proposal to combine hard law with "soft ethics" and governance tools is in line with this strategy, which acknowledges that while law cannot completely regulate sophisticated AI systems, it may shape incentives and accountability in the larger socio-technical context [28].

Additionally, a number of scholars stress that broader reforms in data protection, consumer protection, and digital governance should be synchronized with criminal law reform. Siloed reforms are unsuccessful because AI-related harms frequently cross administrative, civil, and criminal domains, according to research on the legal implications of AI for personal data protection in Indonesia. A more complete and cohesive response to AI-driven cyber dangers could be achieved by upgrading the criminal law framework and incorporating AI considerations into sectoral regulations and the Personal Data Protection Law (UU PDP) [29]. In order to restore legal certainty and guarantee sufficient victim protection, doctrinal work on the lack of AI accountability norms emphasizes the need for explicit legislative clarification of AI's place in the criminal law subject system, whether as an object of regulation, a risk-generating system, or a limited "quasi-subject" for allocation purposes [27].

This study backs the idea that Indonesia should adopt a more comprehensive, risk-aware, and technologically advanced model of criminal law regulation for AI-driven cybercrime in light of these discussions. Incorporating AI-generated and AI-mediated harms into the scope and content of cybercrime offenses; establishing clear guidelines for assigning liability to corporate and human actors involved in the AI lifecycle; integrating risk-based and architecture-based regulatory tools to supplement ex post criminal sanctions; and harmonizing criminal law reforms with data protection and digital governance frameworks are all possible under such a model [30].

These guidelines explicitly address the issues raised in the introduction: the need for adaptive criminal law reform in the age of artificial intelligence, the shortcomings of

the current legal framework, and the crisis of criminal liability in AI-related offenses [30].

5 Conclusion and Recommendation

The study comes to the conclusion that the complexity of AI-driven cybercrime has not been adequately anticipated by Indonesia's current criminal law framework, especially the clauses found in UU ITE and related regulations. Conceptually, autonomous or semi-autonomous AI systems, cross-border digital architectures, and opaque algorithmic decision-making are difficult to integrate under current criminal liability doctrines based on direct human action, clear intent, and territorially bounded offenses. As a result, there is a "crisis of criminal responsibility" wherein inventors, providers, deployers, and users of AI may not be held accountable, and the technology itself is not acknowledged as a legal subject but has the potential to cause or facilitate serious harm. However, there is a disconnect between how AI builds cyberthreats and how law views control and accountability since the regulatory role of digital architecture and "code" is not methodically incorporated into criminal law policy. Overall, the study demonstrates that in the absence of focused reform, Indonesia runs the risk of expanding doctrinal and regulatory gaps that compromise victim protection, legal clarity, and the preventative role of criminal law in the age of artificial intelligence.

In response, the research suggests a number of specific actions for Indonesian criminal code reform. In order to clearly identify AI-generated and AI-mediated behavior within cybercrime offence formulations, such as deepfakes, autonomous malware, and algorithmic manipulation, UU ITE and related criminal provisions should be amended. This would also provide clear guidelines for assigning liability to corporate and human actors throughout the AI lifecycle. Second, for high-risk AI systems whose failure could cause significant cyber harms, a risk-based regulatory approach should be implemented that imposes increased duties of care, transparency, security, and tracking. Violations of these duties can, when appropriate, establish criminal liability. Third, in order to ensure consistency between penalties for AI-related privacy and data abuses and more general cybercrime standards, criminal law reform should be integrated with data protection and digital governance tools. Lastly, in order to operationalize these reforms and guarantee that the criminal justice system can effectively and consistently respond to AI-driven cybercrime, Indonesia should develop technical and institutional capacities such as specialized cybercrime and AI units, forensic standards for AI systems, and guidelines for prosecutors and judges.

References

1. Purnomo, H.: Criminal liability for the use of artificial intelligence in Indonesia. *Jurnal Info Sains: Informatika dan Sains* **13**(03), 1109–1114 (2023).
2. Rahman, R.A., Habibulah, R.: The criminal liability of artificial intelligence: is it plausible to Hitherto Indonesian criminal system?. *Legality: Jurnal Ilmiah Hukum* **27**(2), 147–160 (2019).

3. Rohimi, U.E.: Artificial intelligence and cybersecurity regulation in Indonesia: Towards an Adaptive Legal Framework. *Indonesian Cyber Law Review* **2**(1), 29–38 (2025).
4. Novrianto, M.: Kebijakan hukum pidana terhadap cyber crime berbasis artificial intelligence di Indonesia. *Jurnal Kepastian Hukum dan Keadilan* (2), 150–170 (2025).
5. Fransisco, W., Gussman, A.A., Utomo, B.: Artificial intelligence and legal challenges in Indonesia. *Jurispro Law Review* **1**(1) (2024).
6. Perkasa, A., Siregar, A.P., Keliat, V.U.: The urgency of establishing legal instruments against potential artificial intelligence (AI) crimes. *Ilmu Hukum Prima (IHP)* **8**(1), 91–97 (2025).
7. Lessig, L.: Code: And other laws of cyberspace. ReadHowYouWant.com (2009).
8. Mökander, J., Floridi, L.: Operationalising AI governance through ethics-based auditing: an industry case study. *AI and Ethics* **3**(2), 451–468 (2023).
9. Anggraeny, K.D., Khakim, M., Sirojudin, M.R.: The urgency of cybercrime law reform in Indonesia: Resolving artificial intelligence criminal liability. *JUSTISI* **11**(1), 111–126 (2025).
10. Gustryan, M., Sulaiman, A.: The urgency of regulatory reformulation and strengthening the capacity of law enforcers in combating cybercrime through a criminal law approach in Indonesia. *Greenation International Journal of Law and Social Sciences* **3**(2), 221–229 (2025).
11. Obe, E.T., Sinurat, A., Fanggi, R.A.: Analisis yuridis perlindungan hukum terhadap korban kejahatan berbasis teknologi kecerdasan buatan/artificial intelligence (AI). *AKADEMIK: Jurnal Mahasiswa Humanis* **5**(2), 1144–1156 (2025).
12. Hasibuan, E.S., Rohman, A.N.: Scientific crime investigation and police reform in indonesia: integrating technology, law, and islamic ethics for institutional transformation. *Legal Transformation Muslim Soc'y* **2**, 18 (2025).
13. Fikri, A., Amelia, T.: Indonesia's legal policy on protecting personal data from artificial intelligence abuse. In: *SHS Web of Conferences*, Vol. 204, p. 07002. EDP Sciences (2024).
14. Floridi, L.: The ethics of artificial intelligence: Principles, challenges, and opportunities (2023)/.
15. Pakpahan, D.A.R., Widyawati, A.: Reformulation of cybercrime regulations in the misuse of artificial intelligence in Indonesia. *Law Research Review Quarterly* **12**(1), 139–163 (2026).
16. MURSHAL, S.: Cyber crime and criminal law in the era of artificial intelligence. *International Journal* **1**(4), 268–276 (2024).
17. LEGAL, T.A.S.N.N.: Research in Indonesia: Its origins and approaches. *Audit. Comp. Law J* **4**, 1–9 (2023).
18. Jubaidi, D., Khoirunnisa, K.: Political Configuration of Law in Law Enforcement in Indonesia. Available at SSRN 5068418 (2023).
19. Jonaedi Efendi, Prasetyo Rijadi: Metode Penelitian Hukum Normatif dan Empiris: Edisi Kedua. Prenada Media (2022).
20. Marzuki, P.M.: The essence of legal research is to resolve legal problems. *Yuridika* **37**(1), 37–58 (2022).
21. Floridi, L., Taddeo, M.: Moral vs Legal Norms: Soft and Hard Ethics. In: *A Companion to Digital Ethics*, pp. 11–23 (2025).
22. Sudrajat, T.: The Combination of Normative Juridical Methods and Literature in Educational Administration Research. In: *Proceedings of International Conference on Social Science, Political Science, and Humanities (ICoSPOLHUM)*, Vol. 3, pp. 00026–00026 (2022).
23. Hidayati, M.N., Surono, A., Pamungkas, E.: Criminal Liability For Ai-Based Cybercrime: Comparative Analysis Of Common Law And Civil Law Approaches. *Journal of Law, Politic and Humanities* **6**(2), 1064–1085 (2025).

24. Hastri, E.D., Huda, M., Yuza, E., Milia, J., Itasari, E.R., Miano, M.R.R., Kamilah, A.: *Hukum Internasional Era Society 5.0*. MEGA PRESS NUSANTARA (2025).
25. Singh, S., Kumar, D., Guleria, A., Sai, G., Srivastav, S., Soni, P., Singh, R.: Victims of artificial intelligence: Perspective on criminal and civil liability. *International Journal of Interdisciplinary Approaches in Psychology* **4**(3), 49–78 (2026).
26. Ong, H.W., Afdal, W.: Perbandingan pengaturan sanksi penipuan online berbasis artificial intelligence: Indonesia Vs Amerika. *Jurnal Hukum to-ra: Hukum Untuk Mengatur dan Melindungi Masyarakat* **11**(2), 448–464 (2025).
27. Ervitasari, D., Mayasari, R.T.: The void of artificial intelligence criminal accountability norms in indonesian criminal law reform. *Journal Scientia Iustitiae* **3**(2), 72–81 (2025).
28. Judge, B., Nitzberg, M., Russell, S.: When code isn't law: rethinking regulation for artificial intelligence. *Policy and Society* **44**(1), 85–97 (2025).
29. Solikhah, M.A.: Personal data protection in the era of digital transformation: Challenges and solutions in the indonesian cyber law framework. *Indonesian Cyber Law Review* **2**(1), 39–50 (2025).
30. Kingston, J.K.: Artificial intelligence and legal liability. In: *International Conference on Innovative Techniques and Applications of Artificial Intelligence*, pp. 269–279. Springer, Cham (2016).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

