

Criminal Liability For Algorithmic Manipulation in The Dissemination of Information in The Digital Era

Hartomi^{1*}, Muhamad Adystia Sunggara², Wijayono Hadi Sukrisno³

Faculty of Law, Universitas Pertiba, Pangkalpinang
thomebs1986@gmail.com; dr.m.adistyasunggara@gmail.com;
whsukrisno@gmail.com

**Corresponding Author*

Article info

Received: 4 Jun 2026

Revised: 12 Jul 2026

Accepted: 10 Aug 2026

DOI: <https://doi.org/10.31599/krtha.v20i2.5544>

Abstract : *The development of digital technology has encouraged the emergence of algorithmic manipulation as a new form of cybercrime that has a significant impact on the integrity of digital public spaces. Practices such as bot army, astroturfing, and algorithmic amplification show that algorithms are no longer just tools, but play an active role in expanding the impact of an action. The main problem of this study is related to the unclear construction of the subject of criminal law and the limits of liability in the context of criminal acts mediated by algorithmic systems. This study aims to analyze the construction of subject and criminal law accountability to algorithmic manipulation according to Indonesian positive law and formulate a more adaptive criminal liability model. The method used is normative legal research with legislative, conceptual, and comparative legal approaches. The results of the study show that the Criminal Code and the ITE Law have not been able to accommodate the complexity of the agency chain in the algorithmic system, thus creating an accountability gap. To address this, the study proposes a "risk-based layered liability" model that integrates fault, risk, and liability based liability. This model allows for a proportionate distribution of responsibilities between developers, platform operators, and users. The implementation of this model requires a reformulation of norms in the ITE Law, strengthening the capacity of law enforcement officials, and establishing a structured algorithmic supervision mechanism.*

Keywords : *Algorithmic manipulation, criminal liability, legal subject, accountability gap, cyber law*

Abstrak : Perkembangan teknologi digital telah mendorong munculnya manipulasi algoritmik sebagai bentuk baru kejahatan siber yang berdampak signifikan terhadap integritas ruang publik digital. Praktik seperti bot army, astroturfing, dan algorithmic amplification menunjukkan bahwa algoritma tidak lagi sekadar alat, tetapi berperan aktif dalam memperluas dampak suatu perbuatan. Permasalahan utama penelitian ini berkenaan dengan belum jelasnya konstruksi subjek hukum pidana serta batas pertanggungjawaban dalam konteks tindak pidana yang dimediasi oleh sistem algoritmik. Penelitian ini bertujuan



menganalisis konstruksi subjek dan pertanggungjawaban hukum pidana terhadap manipulasi algoritmik menurut hukum positif Indonesia serta merumuskan model pertanggungjawaban pidana yang lebih adaptif. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan hukum. Hasil penelitian menunjukkan bahwa KUHP dan UU ITE belum mampu mengakomodasi kompleksitas rantai keagenan dalam sistem algoritmik, sehingga menimbulkan kesenjangan akuntabilitas (accountability gap). Untuk mengatasi hal tersebut, penelitian ini mengusulkan model “pertanggungjawaban berlapis berbasis risiko” yang mengintegrasikan pertanggungjawaban berbasis kesalahan, risiko, dan kewajiban. Model ini memungkinkan distribusi tanggung jawab yang proporsional antara pengembang, operator platform, dan pengguna. Implementasi model ini memerlukan reformulasi norma dalam UU ITE, penguatan kapasitas aparat penegak hukum, serta pembentukan mekanisme pengawasan algoritmik yang terstruktur.

Kata kunci : manipulasi algoritmik, pertanggungjawaban pidana, subjek hukum, kesenjangan akuntabilitas, hukum siber

Introduction

Digital transformation has fundamentally and thoroughly changed the landscape of public communication. The development of information technology, especially in the form of algorithm-based digital platforms, has reconfigured the way people access, produce, and distribute information.¹ Social media algorithms and search engines now not only serve as technical instruments, but have evolved to be the main mechanism in determining the visibility of information in digital public spaces.² In practice, algorithms work by processing user behavior data to present content that is considered relevant, thereby indirectly shaping people's preferences, perceptions, and even political attitudes. Digital platforms such as Facebook, X (formerly Twitter), Instagram, and Google can no longer be positioned as neutral mediums. Instead, the platform operates as an active actor that, through its algorithmic system, can amplify, filter, and prioritize certain content based on computational logic that is often not transparent. This condition suggests that power in the information ecosystem has shifted from human actors to technological systems controlled by digital corporate interests.³

However, the algorithm's ability to manage the flow of information at the same time opens space for structured and massive manipulative practices. Algorithmic manipulation comes in many forms, such as the use of bot armies to create the illusion of popularity, the practice of astroturfing that disguises

¹ Budi Gautama Siregar Eka Lestari, *Pengaruh Servicescape dan Kualitas Pelayanan Frontliner Terhadap Kepuasan Nasabah (Studi Kasus Pada PT. Bank Muamalat KCU Padangsidimpuan)*, May 31, 2025, <https://doi.org/10.5281/ZENODO.15564449>.

² Mo Egan, “Remote Justice: Information Rights as a Tool of Empowerment,” *International Review of Law, Computers & Technology* 36, no. 2 (2022): 202–22, <https://doi.org/10.1080/13600869.2022.2060465>.

³ Ismail Zaky Al Fatih, “Peran Algoritma Media Sosial Dalam Penyebaran Propaganda Politik Digital Menjelang Pemilu,” *Jurnal Kajian Stratejik Ketahanan Nasional* 7, no. 1 (2024), <https://doi.org/10.7454/jkskn.v7i1.10090>.

certain interests as organic public opinion, as well as algorithmic amplification that disproportionately magnifies the reach of certain content.⁴ These practices are often used to spread disinformation, political propaganda, and polarizing narratives that have the potential to undermine the quality of democracy.⁵ In the Indonesian context, this phenomenon is increasingly seen in political moments such as general elections, where the digital space is used as an arena for opinion contestation that does not always take place fairly. Algorithmic manipulation not only impacts individuals as consumers of information but also threatens the structure of public deliberation that is the foundation of modern democracy.⁶ Therefore, this phenomenon can no longer be seen as a mere technical problem, but rather as a legal and public policy issue that requires a systemic response.

The legal problems posed by algorithmic manipulation are rooted in the inability of conventional criminal law frameworks to accommodate the complexity of agency chains in digital systems. In classical criminal law doctrine, the legal subjects to which accountability can be held are limited to the human being as the main actor and, in subsequent developments, the corporation as a collective entity. This concept assumes that every criminal act is the result of human will and consciousness. However, this assumption becomes problematic when faced with algorithmic systems that can operate semi-autonomously. Modern algorithms, especially those based on artificial intelligence, have the ability to process data at scale, identify patterns, and generate decisions without direct human intervention at every stage of their operation.⁷ Although algorithms remain a product of human design, the level of autonomy it has creates a distance between the system designers and the concrete impact it generates in the field. In this situation, the attribution of responsibility becomes not simple, since there are many actors that play a role in the life cycle of algorithmic systems.⁸

The lack of clarity about criminal law in this context has direct implications for the emergence of an accountability gap. This gap occurs when an act causes significant harm or negative impact, but no party can be clearly held accountable under applicable law. In the context of algorithmic manipulation, the gap arises because criminal law has not been able to identify exactly who should be responsible for the impact generated by algorithmic systems.⁹ Algorithm developers can argue that the system they create is neutral and only

⁴ Syafri Hariansah and Laila Qhistina, "Toward Algorithmic Due Process: Constitutional Challenges and Human Rights Risks in Indonesia's Digital State," *Jurnal Pembangunan Hukum Indonesia* 8, no. 1 (2026): 25–45, <https://doi.org/10.14710/jphi.v8i1.25-25>.

⁵ Bambang Mudjiyanto et al., *Politik Kontestasi: Antara Narasi Digital, Algoritma Politik, Dan Plot Twist Politik Dalam Dinamika Pemilu Indonesia Pasca Reformasi*, n.d.

⁶ Massimo Airoidi and Joonas Rokka, "Algorithmic Consumer Culture," *Consumption Markets & Culture* 25, no. 5 (2022): 411–28, <https://doi.org/10.1080/10253866.2022.2084726>.

⁷ Sihong Li et al., "From Algorithmic Recommendations to GAI Recommendations: Consumers' Intention to Switch Shopping Recommendation Channels," *International Journal of Human-Computer Interaction*, February 23, 2026, 1–28, <https://doi.org/10.1080/10447318.2026.2623222>.

⁸ Simon Egbert and Elena Esposito, "Algorithmic Crime Prevention. From Abstract Police to Precision Policing," *Policing and Society* 34, no. 6 (2024): 521–34, <https://doi.org/10.1080/10439463.2024.2326516>.

⁹ Rachel Moylan and Jillianne Code, "Algorithmic Futures: An Analysis of Teacher Professional Digital Competence Frameworks through an Algorithm Literacy Lens," *Teachers and Teaching* 30, no. 4 (2024): 452–70, <https://doi.org/10.1080/13540602.2023.2263732>.

follows programming logic. Platform operators can state that they only provide technology infrastructure without directly controlling any content that circulates. Meanwhile, users can argue that they are only taking advantage of the available features. This situation creates a gray space that allows manipulative practices to take place without adequate legal consequences, thereby weakening the effectiveness of criminal law as an instrument of social control.

In Indonesia's positive legal framework, this problem is increasingly complex because no regulation explicitly recognizes the existence and role of algorithmic systems in the construction of criminal accountability. The Criminal Code, as the main codification of criminal law, is still based on the classical paradigm that places humans as the main subjects. Although the New Criminal Code has recognized corporate criminal liability, the regulation has not specifically anticipated the role of algorithmic technology in the process of criminal action.¹⁰ Similarly, the ITE Law, which specifically regulates activities in the digital space, still focuses on acts carried out by humans, such as the spread of false information or hate speech. Existing provisions have not been able to reach a situation where algorithms play an active role in strengthening or expanding the impact of an action. As a result, law enforcement tends to be reactive and limited to individual perpetrators, without touching the structural roots of existing problems.¹¹

Based on an academic literature review, several previous studies are closely related to the present research. For instance, Beckers and Teubner's study, *Three Liability Regimes for Artificial Intelligence: Algorithmic Actants, Hybrids, Crowds*, examines legal liability regimes for artificial intelligence through the concepts of algorithmic actants, hybrids, and crowds.¹² This study is important because it reveals the existence of a responsibility gap where legal acts or consequences arise from algorithmic systems that are not entirely subject to direct human control. However, the study primarily focuses on legal liability regimes in general, particularly within the framework of civil and institutional liability, rather than on the construction of criminal liability for algorithmic manipulation in the dissemination of digital information.

Another relevant study is Taher's *The Responsibility Gap in Algorithmic Governance: A Legal Analysis of Criminal Liability and Due Process in Automated Administrative Decisions*, which discusses the responsibility gap in the use of algorithms in automated administrative decision-making.¹³ Although it is closely related to the present research insofar as both address the problem of responsibility gaps and criminal liability in algorithmic

¹⁰ Soetardi Tri Cahyono et al., "Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia," *Dame Journal of Law* 1, no. 1 (2025): 1–23, <https://doi.org/10.64344/djl.v1i1.6>.

¹¹ Rohayanti Rohayanti, "Ujaran Kebencian Dan Berita Bohong Berdasarkan Perspektif Sosiologi Hukum Ditinjau Dari Undang - Undang Informasi Dan Transaksi Elektronik," *Jurnal Syntax Admiration* 5, no. 8 (2024): 2956–63, <https://doi.org/10.46799/jsa.v5i8.1377>.

¹² Anna Beckers and Gunther Teubner, *Three Liability Regimes for Artificial Intelligence: Algorithmic Actants, Hybrids, Crowds* (Hart Publishing, 2021), <https://doi.org/10.5040/9781509949366>.

¹³ Mohamed Imam Mohamed taher Hala, "The Responsibility Gap in Algorithmic Governance: A Legal Analysis of Criminal Liability and Due Process in Automated Administrative Decisions," *Journal of Daoist Studies* 19-2s (2026) 19, no. 2 (n.d.).

systems, Taher's study focuses on automated administrative decisions. By contrast, the present research specifically examines algorithmic manipulation in the dissemination of information in the digital era. Therefore, the novelty of the study entitled "Criminal Liability for Algorithmic Manipulation in the Dissemination of Information in the Digital Era" lies in its attempt to construct a criminal liability framework for the use of algorithms as instruments of information manipulation, particularly in relation to mens rea, causation, attribution of fault, participation, negligence, and the criminal liability of digital corporations.

In a global context, several jurisdictions have developed specific regulatory frameworks to address legal accountability in the digital ecosystem.¹⁴ The European Union, Singapore, and Australia are selected as comparative jurisdictions because they represent three distinct regulatory approaches to governing algorithmic systems and online information.¹⁵ The European Union has adopted a comprehensive risk-based regulatory model through the Digital Services Act and the Artificial Intelligence Act, which impose obligations on digital platforms to conduct risk assessments, enhance algorithmic transparency, and mitigate systemic risks.¹⁶ Singapore, through the Protection from Online Falsehoods and Manipulation Act (POFMA), represents a state-centered approach that grants public authorities extensive powers to address online disinformation.¹⁷ Meanwhile, Australia emphasizes a co-regulatory framework that places proactive responsibilities on digital platforms to prevent the dissemination of harmful content while maintaining cooperation between regulators and technology companies. These jurisdictions were selected because they have established dedicated legal instruments that directly address the governance of algorithmic systems and digital platforms, making them relevant benchmarks for comparative legal analysis. Although each jurisdiction adopts a different regulatory model, they share a common recognition that algorithmic systems generate significant societal risks and therefore require specific legal safeguards. The comparative analysis of these regulatory approaches provides valuable insights for identifying regulatory gaps and formulating a more effective legal framework for algorithmic accountability in Indonesia.

From the perspective of criminal law, the fundamental problem faced is not simply the absence of the word "algorithm" in the text of the law, but the absence of a delicate construction that is able to reach the acts mediated by the algorithmic system. Indonesia's positive criminal law, both the Criminal Code and the ITE Law, is built on the paradigm that every criminal act is the result

¹⁴ Hiroshi Ito and Kazuhiko Kato, "Biometric Authentication as a Platform Strategy: The Case of Tobu Railway's Digital Identity Ecosystem," *Asian Journal of Technology Innovation*, November 3, 2025, 1–20, <https://doi.org/10.1080/19761597.2025.2583066>.

¹⁵ Saeed M. Alghamdi et al., "Navigating Ethical Challenges in Digital Transformation: Insights on Climate Adaptation, Microbiology, Healthcare, Robotics, and AI under the EU AI Act: An Experts Panel Discussion," *Global Bioethics* 36, no. 1 (2025): 2550823, <https://doi.org/10.1080/11287462.2025.2550823>.

¹⁶ Alghamdi et al., "Navigating Ethical Challenges in Digital Transformation."

¹⁷ Terence Lee, "Artificial Intelligence: Governing Singapore's Smart Digital Journey," *Communication Research and Practice* 10, no. 3 (2024): 307–15, <https://doi.org/10.1080/22041451.2024.2346430>.

of human actions and will that can be directly identified.¹⁸ This paradigm creates a structural vacuum when dealing with algorithmic systems that operate semi-autonomously: there are no norms that explicitly govern what acts are prohibited in the context of the design, operation, or utilization of algorithms; there is no threshold that establishes when an algorithmic impact can qualify as a criminal consequence; and there is no adequate mechanism for attributing responsibility when autonomous computational systems intersperse the chain of causality between humans and impacts.¹⁹ These three gaps are cumulative and mutually reinforcing, resulting in regulatory gaps that cannot be resolved by extensive interpretation of existing norms alone.

This regulatory gap is not only a technical issue of legislation but reflects a fundamental mismatch between the ontology of classical criminal law and the realities of contemporary algorithmic technology. In the doctrine of criminal law, the principle of legality requires that an act can only be punished if it has been expressly formulated in the law before the act is committed (*nullum crimen sine lege stricta*). Consequently, if Indonesia's criminal law has not explicitly formulated acts related to algorithmic manipulation as a criminal offense, law enforcement officials do not have a sufficient normative basis to prosecute, even though the resulting social impact is very real and detrimental. Therefore, efforts to reform criminal law in this context cannot be carried out partially through interpretation but rather require a substantive and systematic reformulation of norms, including the definition of prohibited acts, the establishment of prudent standards for algorithmic system managers, and the regulation of proportionate accountability mechanisms for each actor in the digital ecosystem.

Based on this description, this research is directed to answer two main questions that are fundamental. First, how is the construction of the subject and the liability of criminal law in algorithmic manipulation according to Indonesian positive law? Second, what is the ideal criminal accountability model to overcome these problems while still being based on the fundamental principles of criminal law? Through a normative juridical approach combined with comparative analysis, this research is expected to make a theoretical contribution to the development of criminal law, as well as practical contributions in the form of policy recommendations that lawmakers and law enforcement officials can implement.

The urgency of this research is increasing along with the increasing intensity of the use of digital technology in people's daily lives. Digital public spaces have become the main arena in the formation of public opinion, so any distortion that occurs in it will have a far-reaching impact on social and political life. Algorithmic manipulation, in this case, not only harms individuals as users, but can also disrupt social stability and the legitimacy of the democratic process. Therefore, legal intervention is needed that is not only repressive, but also preventive and structural. Criminal law must be able to

¹⁸ Sih Yuliana Wahyuningtyas, "Regulating Algorithms in the Digital Market: A Revisit of Indonesian Competition Law and Policy," *International Review of Law, Computers & Technology* 38, no. 1 (2024): 21–42, <https://doi.org/10.1080/13600869.2023.2202290>.

¹⁹ Tressyalina Tressyalina et al., "Enhancing Students' Critical Thinking in Criminal Case Solving: An AI-Based Pragmatic Application for Analyzing Authentic Indonesian Texts and Videos," *Interactive Learning Environments* 34, no. 2 (2026): 543–75, <https://doi.org/10.1080/10494820.2025.2504062>.

adapt to technological developments without losing its basic principles, such as the principle of legality, the principle of error, and the principle of legal certainty.

Methods

This research is normative legal research that aims to analyze the construction of the subject and the liability of criminal law to algorithmic manipulation according to Indonesian positive law. The approaches used include the statute approach and the conceptual approach. The legislative approach is carried out by examining the provisions of the Criminal Code (KUHP), Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE), and other related regulations. Meanwhile, a conceptual approach is used to examine legal theories and doctrines related to legal subjects, criminal liability, the principle of error, and the concept of algorithmic agency.

In addition, this study uses a comparative approach by examining regulations in several jurisdictions, such as the Digital Services Act in the European Union, the Protection from Online Falsehoods and Manipulation Act (POFMA) in Singapore, and the Online Safety Act in Australia. This approach aims to gain a comprehensive perspective, identify best practices, and assess their relevance and likelihood of adoption in the Indonesian legal system. The legal materials used consist of primary legal materials in the form of laws and regulations, secondary legal materials in the form of scientific literature and research results, and tertiary legal materials such as legal dictionaries and encyclopedias.

The technique of collecting legal materials is carried out through systematic library research by inventorying and classifying relevant sources. The analysis of legal materials uses a qualitative method with a prescriptive-analytical approach, namely by interpreting legal norms, identifying regulatory gaps, and formulating normative solutions that are in accordance with the development of algorithmic technology. Through this method, the research is expected to produce juridical arguments that not only explain the applicable law but also provide directions for adaptive and applicable criminal law reform in dealing with the phenomenon of algorithmic manipulation in Indonesia.

Result And Discussion

The Construction of Criminal Law Accountability in the Context of Algorithmic Manipulation

An analysis of the construction of criminal law subjects in Indonesia's positive legal system shows that the prevailing paradigm remains rooted in the classical framework that places human actors at the center of criminal liability. Under traditional criminal law doctrine, criminal liability is imposed primarily on natural persons and, in its subsequent development, has been extended to corporations as legal entities. This expansion reflects the practical need to address modern forms of crime committed through organizations and

business entities. Nevertheless, the underlying framework remains anthropocentric because criminal liability ultimately depends on human intent, conduct, or organizational control. Consequently, Indonesia's criminal law has not fully adapted to the emergence of digital technologies, particularly algorithmic systems that operate with varying degrees of autonomy and are capable of significantly shaping social reality.²⁰

In the Indonesian Criminal Code, both the old and the new (Law Number 1 of 2023), the recognition of criminal law subjects is still limited to individuals and corporations. Article 59 of the New Criminal Code recognizes that corporations can be the subject of criminal acts, but the regulation focuses more on the organizational aspect as a collection of people and/or wealth, rather than on the technological system used by corporations in carrying out their activities.²¹ Thus, although corporations have been recognized as the subject of criminal law, the law has not explicitly linked such liability to the use of algorithmic systems that are the main instruments in the operation of digital platforms. The same can be seen in the ITE Law, where the regulation regarding electronic system operators is more oriented towards administrative aspects and general responsibility, without providing a clear framework regarding criminal liability for the impact generated by the algorithm operated.²²

Academically, the regulatory gap in question does not solely stem from the absence of the term "algorithm" in the text of the law, but from the inability of the existing normative structure of criminal law to capture acts mediated by algorithmic systems as criminal acts that can be accounted for. In the dogmatics of criminal law, a new act can be qualified as a criminal act if it meets two main elements: *actus reus* (forbidden outward act) and *mens rea* (the perpetrator's subjective fault).²³ These two elements are designed to reach out to conscious and willful human action. The problem becomes fundamental when algorithms — as systems that operate on autonomous computational logic — produce criminal impacts without being identifiable as a willful perpetrator in the classical criminal law sense. In such a situation, algorithms cannot be categorized as legal subjects, nor can it be enough to simply treat them as "tools", given that their level of operational autonomy far exceeds that of conventional instruments such as weapons or vehicles.²⁴

A normative analysis of Indonesia's positive criminal law provisions shows concretely where the vacancy of the regulation lies. Article 27 paragraph (1) and paragraph (3) of the ITE Law prohibit the act of transmitting or making accessible information that has certain content that is prohibited. This

²⁰ M. Ali Zaidan, *Menuju Pembaruan Hukum Pidana* (Sinar Grafika, 2022).

²¹ Mia Amalia et al., *Kitab Undang Undang Hukum Pidana Tahun 2023* (PT. Sonpedia Publishing Indonesia, 2025).

²² Husain Husain et al., "Kajian Etika Dan Hukum Siber Dalam Pemanfaatan Artificial Intelligence Di Indonesia," *Jurnal Fundamental Justice* 7, no. 1 (2026): 147–62, <https://doi.org/10.30812/fundamental.v7i1.6093>.

²³ Miguel Díaz Y García Conlledo, "Criminal Law and Legal Theory: Not Just Legal Dogmatics, but Never Without It," in *Crisis of the Criminal Law in the Democratic Constitutional State*, vol. 6, ed. Eduardo Demetrio Crespo et al., Legal Studies in International, European and Comparative Criminal Law (Springer International Publishing, 2023), https://doi.org/10.1007/978-3-031-13413-5_5.

²⁴ Rudi Nopiansyah CNLPTc S. H. ., M. H. ., CPM ., CHTc, *Hukum Dan Kecerdasan Buatan: Menyongsong Era Baru Dunia Hukum* (Penerbit Kbm Indonesia, 2025).

formulation requires that there be "actions" that are actively carried out by "everyone". Consequently, algorithmic systems that automatically amplify the prohibited content are not covered by the formulation of this article, because no human being directly performs the act of transmission in every amplification cycle carried out by the algorithm. Similarly, Article 28 paragraph (1) of the ITE Law prohibits the spread of fake news — the formulation refers to human actors as a single subject, without accommodating scenarios where algorithmic systems act as multipliers of distribution massively and systematically.²⁵

Meanwhile, Article 15 of the ITE Law regulates the obligation of electronic system operators to ensure that the systems they operate function as they should. However, normatively, this provision is administrative and does not come with proportionate criminal sanctions for failure to mitigate algorithmic risks. In other words, even if a platform operator is proven to have allowed its algorithms to systematically amplify the spread of disinformation, the provisions of Article 15 of the ITE Law do not provide a sufficient basis for imposing a criminal penalty for such structural negligence. It is this emptiness that normatively distinguishes between "algorithm as a tool" within the framework of *instrumentum sceleris* — which is already known in criminal law — and "algorithm as an object of criminal regulation in its own right" that has not yet been recognized in the Indonesian legal system. This difference is not just terminological, but has a direct impact on whether an act can be reached by the criminal law and who can be held accountable for it.

Comparisons with other jurisdictions reinforce this argument. The European Union, through the AI Act (Regulation (EU) 2024/1689), has explicitly categorized artificial intelligence systems — including recommendation algorithms — into risk levels that each come with different legal obligations and sanctions. Article 5 of the AI Act even outright prohibits certain AI practices, such as systems that manipulate human behavior beyond their awareness, and establishes administrative and criminal sanctions for violators. This approach suggests that the regulation of algorithms as separate regulatory objects — not just human instruments — is a normative necessity that has been recognized at the supranational level. On the other hand, in the Indonesian legal system, there is no equivalent norm that independently defines "algorithmic manipulation" as a prohibited act, establishes algorithm design standards that must be met, or regulates the criminal consequences of failure to meet these standards. The absence of these three normative elements—definitions, standards, and sanctions—is what is rightly referred to as the regulatory gap in the academic perspective of criminal law.

The limitations of this construction become even more evident when faced with the phenomenon of algorithmic manipulation involving various actors with different levels of role and control. In practice, algorithmic manipulation is not carried out by a single actor, but rather is the result of complex interactions between algorithm developers, platform operators, and users. Algorithm developers are responsible for the design of the system, including the parameters and logic that determine how the algorithm works. Platform operators implement such systems at scale and derive economic benefits from

²⁵ Yoanda Widi Pranata, "Rekonstruksi Pasal 27 Ayat (3) UU ITE Dan Implikasinya Terhadap Kebebasan Berpendapat Di Indonesia," *IJOLARES: Indonesian Journal of Law Research* 3, no. 2 (2025): 41–47, <https://doi.org/10.60153/ijolares.v3i2.164>.

increased user engagement. Meanwhile, users can take advantage of loopholes in the system to distribute manipulative content in a structured manner.²⁶ In this condition, attribution of responsibility becomes difficult if criminal law focuses only on the direct perpetrator without considering the structural role of the other actors involved.

This condition creates what in the legal literature is called an accountability gap, which is a situation in which an act has a real impact on the community, but no party can clearly be held accountable under the applicable law.²⁷ In the context of algorithmic manipulation, this gap arises because criminal law does not have adequate instruments to link human actions to the impact generated by complex algorithmic systems. Algorithms can amplify or expand the impact of content exponentially, so that the consequences go far beyond the initial intentions of individual actors. However, because algorithms are not recognized as legal subjects, and because of limitations in tracing the causal relationship between system design and concrete impact, accountability often stops at the operational level.²⁸

Furthermore, the development of artificial intelligence technology has strengthened the autonomy character of algorithmic systems. Machine learning-based algorithms not only execute predetermined instructions but are also able to adjust their behavior based on the data received. This creates a high level of uncertainty in predicting system outputs, making it difficult to determine responsibility. From a criminal law perspective, this poses a serious challenge to the concepts of *mens rea* (malicious intent) and *actus reus* (criminal acts), which have been the basis for determining guilt. Algorithms do not have awareness or will in the traditional sense, so they cannot fulfill the subjective element in criminal liability. However, the impact produced by algorithms remains real and can cause significant losses to society.²⁹

In such a situation, maintaining a conventional approach that is entirely human-oriented as the sole subject of criminal law has the potential to create a serious and systematic legal vacuum. Therefore, it is necessary to reconstruct the concept of criminal law subjects that are more adaptive to technological developments. This reconstruction does not necessarily mean recognizing algorithms as independent legal subjects, but it can be done by broadening the scope of human and corporate accountability to include the impact generated by the systems they create and operate.³⁰ In other words, the focus is no longer only on who performs the act directly, but also on who has the control, capacity, and profit of the system that produces that impact.

This approach is in line with developments in comparative law, where various jurisdictions have begun to adopt the concept of algorithmic accountability as

²⁶ Oki Arifin et al., *Dasar Pemrograman : Teori & Aplikasi* (PT. Sonpedia Publishing Indonesia, 2023).

²⁷ Andi Mirdah and Gugus Irianto, *Analisis Fenomena Expectation Gap Dan Tanggung Jawab Hukum Auditor*, n.d.

²⁸ Wenly R. J. Lolong and Irene R. H. T. Tangkawarow, *Ketika Algoritma Membajak Demokrasi: Rekonstruksi Regulasi Pemilu Indonesia Menghadapi Manipulasi Digital* (Unima Press, 2025).

²⁹ Aniek Perian et al., "Artificial Intelligence Sebagai Pelaku Kejahatan," *Wijayakusuma Law Review* 7, no. 2 (2025), <https://doi.org/10.51921/wlr.25qk5w45>.

³⁰ Safaruddin Harefa et al., "Transformasi Kebijakan Pidana Dalam Kuhp Nasional: Menuju Sistem Pidana Yang Berkeadilan Dan Humanis," *Simbur Cahaya*, December 31, 2025, 283–306, <https://doi.org/10.28946/sc.v32i2.5050>.

a basis for regulating the responsibility of digital platforms.³¹ The European Union, through the Digital Services Act, requires platforms to conduct a risk assessment of the algorithmic systems they use, as well as take the necessary mitigation measures to prevent negative impacts. This approach represents a shift from a fault-based accountability model to a model that emphasizes more on structural and preventive responsibility. Thus, liability arises not only after a breach occurs, but also before the occurrence of a loss, through the obligation to manage the risks inherent in the use of technology.³²

In the context of Indonesian law, the adoption of this kind of approach requires careful adjustment to the basic principles of criminal law, in particular the principles of legality and the principle of wrongdoing. Any expansion of the concept of the subject of law must still be based on the formulation of clear and firm norms, so as not to create legal uncertainty.³³ In addition, it is necessary to ensure that the accountability imposed remains proportional to the level of involvement and control ability of each actor. In this regard, it is important to distinguish between the responsibilities of developers who focus on system design, operators who focus on implementation and supervision, and users who focus on system utilization.³⁴

Based on the above analysis, it can be concluded that the construction of the subject of criminal law in the context of algorithmic manipulation can no longer be understood narrowly as a direct relationship between the individual perpetrator and the criminal act.³⁵ Instead, such constructs should be understood as a network of relationships between the various actors involved in the life cycle of algorithmic systems. This approach allows criminal law to reach the complexity of agencies in digital systems, while reducing the accountability gap that has been a major obstacle in law enforcement. Thus, the reconstruction of the concept of the subject of criminal law is a crucial first step in formulating a more comprehensive and adaptive criminal accountability model to technological developments in the digital era.

Criminal Accountability Models for Algorithmic Manipulation

The *accountability gap* in the context of algorithmic manipulation requires a reconstruction of the criminal accountability model that is not only based on the classical paradigm of individual error but is also able to accommodate the complexity of the relationship between humans, corporations, and technological systems. The ideal criminal accountability model must be able to bridge the tension between the fundamental principles of criminal law, such

³¹ Melanie Nicholle, "Pertanggung-Jawaban Hukum Atas Keputusan Otomatis Berbasis Kecerdasan Buatan: Studi Komparatif Antara Uni Eropa Dan Asia Tenggara," *Jaksa : Jurnal Kajian Ilmu Hukum Dan Politik* 3, no. 4 (2025): 65–79, <https://doi.org/10.51903/ejr3ep34>.

³² Dian Alan Setiawan, "Strategi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi: Studi Komparatif Antara Indonesia, Amerika, Dan Eropa," *Masalah-Masalah Hukum* 53, no. 1 (2024): 78–89, <https://doi.org/10.14710/mmh.53.1.2024.78-89>.

³³ Mutiara Putri Nirwanawati, *Transformasi Pengaturan Tindak Pidana Perzinaan Dalam Perspektif Pembaruan Hukum Pidana Indonesia*, 14, no. 2337 (2026).

³⁴ Lenny Marlina and Mulyawan Safwandi Nugraha, *Analisis Komponen Utama Dalam Sistem Informasi Manajemen : Konsep, Fungsi, Dan Implementasi*, 09 (2024).

³⁵ Beryl Helga Fredella Hibatulloh, "Upaya Penegakan Hukum Terhadap AI (Artificial Intelligence) Sebagai Subjek Hukum Pidana dalam Perspektif Kriminologi," *Tarunalaw: Journal of Law and Syariah* 3, no. 01 (2025), <https://doi.org/10.54298/tarunalaw.v3i01.300>.

as the principles of legality and the principle of wrongdoing, and the need to respond to the dynamics of rapidly evolving digital technologies.³⁶ In this context, a monolithic approach is no longer adequate. Instead, an integrative model is needed that can combine various accountability bases systematically and proportionally.

This study proposes a criminal liability model called "*stratified risk-based liability*". This model is built on three main pillars, namely *fault-based liability*, *risk-based liability*, and *duty-based liability*. These three pillars do not stand alone but complement each other in forming a comprehensive accountability framework. The integration of these three approaches allows criminal law to reach various dimensions of actions involving algorithmic systems, ranging from technology design and operational implementation to utilization by users.

The first pillar, fault-based accountability, remains a key foundation in criminal law. The principle of *geen straf zonder schuld* requires that there be an error as a basis for imposing a penalty.³⁷ In the context of algorithmic manipulation, mistakes can appear in the form of intentionality (*dolus*) or negligence (*culpa*). Intentionality can be proven when a developer or operator knowingly designs or operates an algorithm with the intent to amplify the spread of manipulative content, such as disinformation or political propaganda. In practice, this can happen through algorithmic parameter settings that systematically prioritize sensational or polarizing content to increase user engagement, even though it is known that such content has the potential to harm the public interest.

In addition to intentionality, another relevant form of error is negligence. Negligence occurs when a developer or operator fails to take steps that should be possible to prevent the negative impact of the algorithmic system they manage. In this context, the standard used is a professional standard, namely whether the perpetrator has acted in accordance with best *practices* in the technology industry. If a platform is known to have a high risk of spreading disinformation, but does not undertake adequate mitigation efforts, then it can be said that there is negligence that can be criminally accounted for.³⁸ Thus,

³⁶ "Ai & Ethical Human Resource Management (Hrm) - Penelusuran Google," accessed July 9, 2026, <https://www.google.com/search?udm=36&q=AI+%26+ETHICAL+HUMAN+RESOURCE+MANAGEMENT+%28HRM%29>.

³⁷ Masitoh Siagian and Muhammad Irwan Palli Nasution, *Bertanggung Jawab dalam Data yang Salah Jika yang Dikumpulkan Bersumber dari Sistem InformasI*, 3, no. 3 (2026).

³⁸ "Digital Society (Pemahaman Dan Inspirasi Dalam Beradaptasi Pada Era Digital - Penelusuran Google," accessed July 9, 2026, https://www.google.com/search?q=Digital+Society+%28Pemahaman+dan+Inspirasi+dalam+Beradaptasi+Pada+Era+Digital&sca_esv=5b9fe4ed574a9c86&udm=36&ei=Kh9PaqmROdWQnesPsOug0Qs&biw=1280&bih=561&ved=0ahUKEwipztPq3MSVAXVVSGcHHbA1KLoQ4dUDCA8&oq=Digital+Society+%28Pemahaman+dan+Inspirasi+dalam+Beradaptasi+Pada+Era+Digital&gs_lp=EhBnd3Mtd2l6LW1vZGVsZXNzIktEaWdpdGFsIFNvY2lIdHkgKFBlbWFOYW1hbiBkYW4gSW5zcGlyYXNpIGRhbgGFtIEJlcmFkYXB0YXNpIFBhZGEgRXJhIERpZ2l0YWxIllocCUOEQWOH3AXADeACQAQCYAVagAVaqAQExuAEMyAE A-AEB-AECmAIBoAIRqAIAwgIIEAAY7wUYsAPCAgsQABiABBiiBBiWA5gDBOIDBRIBMSBA8QWewr8WMmSwYYgGAZAGBJIHATGgB12yBwC4BwDCBwMzLTHIBwqACAE&sclint=gws-wiz-modeless.

fault-based liability remains relevant, but it needs to be interpreted more broadly in order to reach the context of modern technology.

However, relying on a fault-based approach alone is not enough to overcome the complexity of algorithmic manipulation.³⁹ This is due to the characteristics of algorithmic systems that are often opaque and *unpredictable*. Machine learning algorithms can generate outputs that are not fully comprehensible even to the developers themselves. In conditions like this, proving subjective errors becomes very difficult to do. Therefore, a second pillar is needed, namely risk-based accountability.

Risk-based accountability puts the focus on the impact produced by a system, not solely on the intentions or mistakes of the perpetrators.⁴⁰ In this model, digital platforms can be held accountable for the negative impacts generated by the algorithms they operate, if those risks can be identified and should be mitigated. This approach has similarities to the principle of *strict liability* in criminal law, where liability can be imposed without the need to prove subjective wrongdoing. However, in the context of algorithmic manipulation, the application of this principle must be done carefully so as not to contradict the principle of error.

To maintain this balance, risk-based liability in this model is not applied absolutely but is conditional. This means that the platform can only be held accountable if it is proven that it does not carry out the obligation to identify and manage the risks inherent in its algorithmic system. Thus, focus not only on the result, but also on the risk management process carried out by the actor. This approach encourages platforms to proactively evaluate the social impact of the technology they use, so that the preventive function of criminal law can run optimally.⁴¹

The third pillar is liability-based liability, which emphasizes violations of certain pre-established legal obligations. In this context, platform operators have an obligation to ensure that the algorithmic systems they operate are not misused for manipulative purposes.⁴² This obligation covers several important aspects. First, the obligation of algorithmic transparency, which is the obligation to provide adequate information about how the algorithm works to users and regulators. This transparency is important to enable public oversight and accountability.

Second, the obligation to conduct periodic algorithmic audits. This audit aims to identify potential biases, vulnerabilities to manipulation, as well as social impacts that may arise from the use of algorithms. Third, the obligation to moderate effective content. The platform must have adequate mechanisms in place to detect and control the spread of content that is manipulative or harmful in nature. Fourth, the obligation to provide a reporting and dispute

³⁹ Andi Agussalim and Yusring Sanusi Baso, *Mengukur Dimensi Kognisi: Pendekatan Algoritma Dalam Analisis Bahasa*, n.d.

⁴⁰ Mas Achmad Hardiansyah et al., *Prinsip Keadilan Dan Kepastian Hukum Dalam Penentuan Tingkat Risiko Usaha Dan Pemberian Sanksi Administratif di Provinsi Lampung*, n.d.

⁴¹ Abdul Rauf et al., "Tanggung Jawab Perdata Penyedia Platform AI Terhadap Pelanggaran Hak Cipta Karya Digital Di Indonesia," *SISITI : Seminar Ilmiah Sistem Informasi Dan Teknologi Informasi* 15, no. 1 (2026): 72–80, <https://doi.org/10.36774/sisiti.v15i1.2141>.

⁴² Abdul Rauf et al., "Tanggung Jawab Perdata Penyedia Platform AI Terhadap Pelanggaran Hak Cipta Karya Digital Di Indonesia."

resolution mechanism that is easily accessible to users. These obligations reflect the principle of *duty of care*, which places responsibility on those who have control over the system.

The integration of the three pillars results in an accountability model that is tiered and proportional. Each actor in the digital ecosystem is subject to responsibilities according to their roles and capacities. The algorithm developer is responsible for the design of the system, the platform operator is responsible for the implementation and supervision, while the user is responsible for the use of the system. This model allows for a fairer and more realistic distribution of responsibilities, while avoiding concentrating the legal burden on just one party.

To operationalize this model in the Indonesian legal system, it is necessary to reformulate norms in laws and regulations, especially the ITE Law. The reformulation can be done through the addition of criminal provisions that specifically regulate liability for algorithmic manipulation. The criminal offense formulated must include several forms of acts, including: (1) deliberately designing or operating an algorithmic system that amplifies the systematic spread of disinformation; (2) negligence that causes the algorithmic system to produce adverse impacts, even though the risk is predictable; and (3) failing to comply with transparency, audit, or moderation obligations set forth by law.

In formulating the criminal offense, it is important to pay attention to the principle of clarity of norms (*lex certa*) so as not to cause multiple interpretations. Therefore, it is necessary to include operational definitions of key concepts, such as "algorithmic manipulation", "disproportionate amplification", and "systemic risk". In addition, it is necessary to set a clear threshold to determine when an action can be categorized as a criminal act. This is important to maintain a balance between the protection of the public interest and legal certainty for business actors in the technology sector.

The proof aspect is also an important challenge in the application of this model. Proving in the case of algorithmic manipulation requires a different approach than conventional proof. Law enforcement officials must have the ability to analyze algorithmic systems, including access to *source code*, training *datasets*, and internal company documentation.⁴³ Therefore, it is necessary to strengthen the technical capacity of law enforcement officials, including through training in the fields of digital forensics and data science. In addition, it is necessary to establish a cooperation mechanism with independent expert institutions that can provide objective technical analysis.

The jurisdictional dimension also needs to be considered, considering that many digital platforms operate cross-country. In this case, the principle of *substantial connection* can be used as a basis for establishing jurisdiction. This means that a platform can be held accountable in Indonesia if its activities have a significant impact on Indonesian society.⁴⁴ The application of this principle requires international cooperation, both in the form of bilateral and

⁴³ Prof Dr Rudi Margono M.Hum S. H., *Regulasi Artificial Intelligence (AI): Tantangan Penegakan Hukum Masa Depan* (Profesor Rudi Margono, 2026).

⁴⁴ Muhammad Raihan Alim et al., *Implikasi Yuridis Penutupan Konten Digital dalam Perspektif Nasional & Internasional*, 2025.

multilateral agreements, to facilitate the exchange of information and cross-border law enforcement.

In addition to normative and law enforcement aspects, the implementation of this model also requires institutional strengthening. An independent supervisory agency is needed that has the authority to conduct audits of algorithmic systems, provide policy recommendations, and impose administrative sanctions as a preventive measure.⁴⁵ This approach allows for a gradual *enforcement system*, where administrative sanctions are used as an initial mechanism to encourage compliance, while criminal sanctions are used as the ultimate remedy for serious and systematic violations.⁴⁶

Thus, the risk-based layered criminal liability model proposed in this study offers a more adaptive and comprehensive approach to dealing with the challenges of algorithmic manipulation. This model not only expands the scope of accountability but also strengthens the preventive function of criminal law through an emphasis on risk management and the duty of care. Through the integration of classical criminal law principles and modern technology-based approaches, this model is expected to be the basis for Indonesia's criminal law reform that is more responsive to the times.

Conclusion

This study concludes that Indonesia's existing criminal law framework has not adequately addressed algorithmic manipulation because it still relies on a conventional construction of criminal liability centered on natural persons and corporations. This framework fails to capture the systemic role of algorithmic systems in amplifying harmful content and obscuring responsibility among developers, platform operators, and users. As a result, a serious accountability gap emerges, particularly when criminal harm is produced through complex and semi-autonomous digital systems.

To address this gap, this study proposes the stratified risk-based liability model as a more adaptive framework for criminal accountability. The model integrates fault-based, risk-based, and duty-based liability, allowing responsibility to be distributed proportionately according to each actor's control, knowledge, capacity, and benefit from the algorithmic system. Its theoretical contribution lies in shifting criminal liability from a purely individual and linear model toward a relational and systemic model of accountability.

Practically, this model provides a basis for reforming Indonesia's criminal law, particularly the ITE Law, by introducing clearer norms on algorithmic manipulation, disproportionate amplification, systemic risk, transparency obligations, algorithmic audits, and risk mitigation duties. Criminal sanctions should be applied as an *ultimum remedium* for serious and systematic failures, while preventive administrative mechanisms should be strengthened.

⁴⁵ Fakhрина Wardina Athiroh, *Peran Audit Hukum dalam Mencegah Penyalahgunaan Kewenangan pada Pengadaan Barang dan Jasa*, n.d.

⁴⁶ Eka Ayu Safitri et al., "Batasan Dan Mekanisme Penerapan Sanksi Pidana Perpajakan Di Indonesia Dalam Perspektif Asas *Ultimum Remedium*," *Jurnal Hukum Statuta* 4, no. 3 (2025): 144–58, <https://doi.org/10.35586/jhs.v4i3.11160>.

Future research should further develop evidentiary standards for causation, negligence, and control in algorithmic manipulation cases.

Recommendation

First, in the legislative aspect, it is necessary to improve Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) through the addition of norms that specifically regulate criminal liability for algorithmic manipulation. The regulation can be placed as an expansion of the provisions regarding the implementation of electronic systems in Article 15 of the ITE Law, by adding a paragraph that requires electronic system operators to carry out algorithmic transparency, periodic audits of the recommendation system and amplification of content, and mitigate the risk of spreading disinformation and manipulation of public opinion. In addition, it is necessary to add new criminal provisions after Article 45A of the ITE Law, which regulate sanctions against developers or platform operators who intentionally or due to their negligence operate an algorithmic system that systematically amplifies the spread of disinformation, manipulative propaganda, or content that disturbs public order. The formulation of these norms must be carried out clearly and measurably so that it remains in line with the principles of legality, legal certainty, and protection of technological innovation.

Second, in the institutional aspect, it is necessary to strengthen the capacity of law enforcement officials through the development of competencies in the fields of digital forensics, artificial intelligence, and algorithmic system analysis on an ongoing basis. In addition, it is necessary to establish an independent supervisory institution that has the authority to conduct algorithmic audits, supervise digital platforms, and provide recommendations and administrative sanctions as a preventive instrument before criminal law enforcement.

Third, in the academic aspect, follow-up empirical research is needed to test the effectiveness of the risk-based layered accountability model in law enforcement practices in Indonesia. Research also needs to be directed at the preparation of objective and measurable indicators to identify algorithmic manipulation, so that it can be the basis for the formation of legal policies and evidence in the criminal justice process.

References

- Abdul Rauf, Annah, and Hardi. "Tanggung Jawab Perdata Penyedia Platform AI Terhadap Pelanggaran Hak Cipta Karya Digital Di Indonesia." *SISITI: Seminar Ilmiah Sistem Informasi Dan Teknologi Informasi* 15, no. 1 (2026): 72–80. <https://doi.org/10.36774/sisiti.v15i1.2141>.
- Agussalim, Andi, and Yusring Sanusi Baso. *Mengukur Dimensi Kognisi: Pendekatan Algoritma Dalam Analisis Bahasa*. n.d.
- "Ai & Ethical Human Resource Management (Hrm) - Penelusuran Google." Accessed July 9, 2026.

- <https://www.google.com/search?udm=36&q=AI+%26+ETHICAL+HUMAN+RESOURCE+MANAGEMENT+%28HRM%29>.
- Airoidi, Massimo, and Joonas Rokka. "Algorithmic Consumer Culture." *Consumption Markets & Culture* 25, no. 5 (2022): 411–28. <https://doi.org/10.1080/10253866.2022.2084726>.
- Alghamdi, Saeed M., Okpala Charles Chikwendu, Okafor Ugochukwu Chukwuma, et al. "Navigating Ethical Challenges in Digital Transformation: Insights on Climate Adaptation, Microbiology, Healthcare, Robotics, and AI under the EU AI Act: An Experts Panel Discussion." *Global Bioethics* 36, no. 1 (2025): 2550823. <https://doi.org/10.1080/11287462.2025.2550823>.
- Alim, Muhammad Raihan, Briliana Ridhowati, Daryl James Choirul, and Syafar Hurairah Muslim. *Implikasi Yuridis Penutupan Konten Digital dalam Perspektif Nasional & Internasional*. 2025.
- Amalia, Mia, Frans Reumi, and Kiki Kristanto. *Kitab Undang Undang Hukum Pidana Tahun 2023*. PT. Sonpedia Publishing Indonesia, 2025.
- Aniek Perian, Arka Atyanta, and Muhammad Syamsudin. "Artificial Intelligence Sebagai Pelaku Kejahatan." *Wijayakusuma Law Review* 7, no. 2 (2025). <https://doi.org/10.51921/wlr.25qk5w45>.
- Arifin, Oki, Fathurrahman Kurniawan Ikhsan, Randi Farmana Putra, et al. *Dasar Pemrograman : Teori & Aplikasi*. PT. Sonpedia Publishing Indonesia, 2023.
- Athiroh, Fakhrina Wardina. *Peran Audit Hukum dalam Mencegah Penyalahgunaan Kewenangan pada Pengadaan Barang dan Jasa*. n.d.
- Beckers, Anna, and Gunther Teubner. *Three Liability Regimes for Artificial Intelligence: Algorithmic Actants, Hybrids, Crowds*. Hart Publishing, 2021. <https://doi.org/10.5040/9781509949366>.
- Beryl Helga Fredella Hibatulloh. "Upaya Penegakan Hukum Terhadap AI (Artificial Intelligence) Sebagai Subjek Hukum Pidana dalam Perspektif Kriminologi." *Tarunalaw: Journal of Law and Syariah* 3, no. 01 (2025). <https://doi.org/10.54298/tarunalaw.v3i01.300>.
- CNLPTc, Rudi Nopiansyah, S. H. ., M. H., CPM. CHTc. *Hukum Dan Kecerdasan Buatan: Menyongsong Era Baru Dunia Hukum*. Penerbit Kbm Indonesia, 2025.
- Díaz Y García Conlledo, Miguel. "Criminal Law and Legal Theory: Not Just Legal Dogmatics, but Never Without It." In *Crisis of the Criminal Law in the Democratic Constitutional State*, vol. 6, edited by Eduardo Demetrio Crespo, Alfonso García Figueroa, and Gema Marcilla Córdoba. Legal Studies in International, European and Comparative Criminal Law. Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-13413-5_5.
- "Digital Society (Pemahaman Dan Inspirasi Dalam Beradaptasi Pada Era Digital - Penelusuran Google." Accessed July 9, 2026. https://www.google.com/search?q=Digital+Society+%28Pemahaman+dan+Inspirasi+dalam+Beradaptasi+Pada+Era+Digital&sca_esv=5b9fe4ed574a9c86&udm=36&ei=Kh9PaqmROdWQnesPsOug0Qs&biw=1280&bih=561&ved=0ahUKEwipztPq3MSVAXVVSgCHHbA1KLoQ4dUDC

A8&eq=Digital+Society+%28Pemahaman+dan+Inspirasi+dalam+Berad
aptasi+Pada+Era+Digital&gs_lp=EhBnd3Mtd2l6LW1vZGVsZXNzIktEa
WdpdGFsIFNvY2lldHkgKFB1bWFOYW1hbiBkYW4gSW5zcGlyYXNpI
GRhbGFtIEJlcmFkYXB0YXNpIFBhZGEgRXJhIERpZ2l0YWwXIlocCUOE
QWOH3AXADeACQAQCYAVagAVaqAQExuAEMyAEA-AEB-
AECmAIBoAIRqAIAwgIIEAAY7wUYsAPCAgsQABiABBiiBBiwA5gD
BOIDBRIBMSBA8QWewr8WMmSwYYgGAZAGBJIHATGgB12yBwC4
BwDCBwMzLTHIBwqACAE&scient=gws-wiz-modeless.

- Egan, Mo. "Remote Justice: Information Rights as a Tool of Empowerment." *International Review of Law, Computers & Technology* 36, no. 2 (2022): 202–22. <https://doi.org/10.1080/13600869.2022.2060465>.
- Egbert, Simon, and Elena Esposito. "Algorithmic Crime Prevention. From Abstract Police to Precision Policing." *Policing and Society* 34, no. 6 (2024): 521–34. <https://doi.org/10.1080/10439463.2024.2326516>.
- Eka Lestari, Budi Gautama Siregar. *Pengaruh Servicescape dan Kualitas Pelayanan Frontliner Terhadap Kepuasan Nasabah (Studi Kasus Pada PT. Bank Muamalat KCU Padangsidimpuan)*. May 31, 2025. <https://doi.org/10.5281/ZENODO.15564449>.
- Hala, Mohamed Imam Mohamed taher. "The Responsibility Gap in Algorithmic Governance: A Legal Analysis of Criminal Liability and Due Process in Automated Administrative Decisions." *Journal of Daoist Studies* 19-2s (2026) 19, no. 2 (n.d.).
- Hardiansyah, Mas Achmad, FX Sumarja, and Zulkarnain Ridlwan. *Prinsip Keadilan Dan Kepastian Hukum Dalam Penentuan Tingkat Risiko Usaha Dan Pemberian Sanksi Administratif di Provinsi Lampung*. n.d.
- Harefa, Safaruddin, Sri Ismawati, and Mega Fitri Hertini. "Transformasi Kebijakan Pemidanaan Dalam Kuhp Nasional: Menuju Sistem Pemidanaan Yang Berkeadilan Dan Humanis." *Simbur Cahaya*, December 31, 2025, 283–306. <https://doi.org/10.28946/sc.v32i2.5050>.
- Hariansah, Syafri, and Laila Qhistina. "Toward Algorithmic Due Process: Constitutional Challenges and Human Rights Risks in Indonesia's Digital State." *Jurnal Pembangunan Hukum Indonesia* 8, no. 1 (2026): 25–45. <https://doi.org/10.14710/jphi.v8i1.25-25>.
- Husain, Husain, Ana Rahmatyar, Lanang Sakti, Muhammad Rosikhu, Saparudin Efendi, and Imam Alfurqan. "Kajian Etika Dan Hukum Siber Dalam Pemanfaatan Artificial Intelligence Di Indonesia." *Jurnal Fundamental Justice* 7, no. 1 (2026): 147–62. <https://doi.org/10.30812/fundamental.v7i1.6093>.
- Ito, Hiroshi, and Kazuhiko Kato. "Biometric Authentication as a Platform Strategy: The Case of Tobu Railway's Digital Identity Ecosystem." *Asian Journal of Technology Innovation*, November 3, 2025, 1–20. <https://doi.org/10.1080/19761597.2025.2583066>.
- Lee, Terence. "Artificial Intelligence: Governing Singapore's Smart Digital Journey." *Communication Research and Practice* 10, no. 3 (2024): 307–15. <https://doi.org/10.1080/22041451.2024.2346430>.
- Li, Sihong, Xiqing Han, Huawei Liu, and Min Zhang. "From Algorithmic Recommendations to GAI Recommendations: Consumers' Intention to Switch Shopping Recommendation Channels." *International Journal of*

- Human-Computer Interaction*, February 23, 2026, 1–28.
<https://doi.org/10.1080/10447318.2026.2623222>.
- Lolong, Wenly R. J., and Irene R. H. T. Tangkawarow. *Ketika Algoritma Membajak Demokrasi: Rekonstruksi Regulasi Pemilu Indonesia Menghadapi Manipulasi Digital*. Unima Press, 2025.
- Marlina, Lenny, and Mulyawan Safwandi Nugraha. *Analisis Komponen Utama Dalam Sistem Informasi Manajemen : Konsep, Fungsi, Dan Implementasi*. 09 (2024).
- M.Hum, Prof Dr Rudi Margono, S. H. *Regulasi Artificial Intelligence (AI): Tantangan Penegakan Hukum Masa Depan*. Profesor Rudi Margono, 2026.
- Mirdah, Andi, and Gugus Irianto. *Analisis Fenomena Expectation Gap Dan Tanggung Jawab Hukum Auditor*. n.d.
- Moylan, Rachel, and Jillianne Code. “Algorithmic Futures: An Analysis of Teacher Professional Digital Competence Frameworks through an Algorithm Literacy Lens.” *Teachers and Teaching* 30, no. 4 (2024): 452–70.
<https://doi.org/10.1080/13540602.2023.2263732>.
- Mudjiyanto, Bambang, Fit Yanuar, and Mochamad Mansur. *Politik Kontestasi: Antara Narasi Digital, Algoritma Politik, Dan Plot Twist Politik Dalam Dinamika Pemilu Indonesia Pasca Reformasi*. n.d.
- Nicholle, Melanie. “Pertanggung-Jawaban Hukum Atas Keputusan Otomatis Berbasis Kecerdasan Buatan: Studi Komparatif Antara Uni Eropa Dan Asia Tenggara.” *Jaksa : Jurnal Kajian Ilmu Hukum Dan Politik* 3, no. 4 (2025): 65–79. <https://doi.org/10.51903/ejr3ep34>.
- Nirwanawati, Mutiara Putri. *Transformasi Pengaturan Tindak Pidana Perzinaan Dalam Perspektif Pembaruan Hukum Pidana Indonesia*. 14, no. 2337 (2026).
- Rohayanti, Rohayanti. “Ujaran Kebencian Dan Berita Bohong Berdasarkan Perspektif Sosiologi Hukum Ditinjau Dari Undang - Undang Informasi Dan Transaksi Elektronik.” *Jurnal Syntax Admiration* 5, no. 8 (2024): 2956–63. <https://doi.org/10.46799/jsa.v5i8.1377>.
- Safitri, Eka Ayu, Ratih Damayanti, and Tri Sulistiyono. “Batasan Dan Mekanisme Penerapan Sanksi Pidana Perpajakan Di Indonesia Dalam Perspektif Asas Ultimum Remedium.” *Jurnal Hukum Statuta* 4, no. 3 (2025): 144–58. <https://doi.org/10.35586/jhs.v4i3.11160>.
- Setiawan, Dian Alan. “Strategi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi: Studi Komparatif Antara Indonesia, Amerika, Dan Eropa.” *Masalah-Masalah Hukum* 53, no. 1 (2024): 78–89.
<https://doi.org/10.14710/mmh.53.1.2024.78-89>.
- Siagian, Masitoh, and Muhammad Irwan Palli Nasution. *Bertanggung Jawab dalam Data yang Salah Jika yang Dikumpulkan Bersumber dari Sistem Informas*. 3, no. 3 (2026).
- Tressyalina, Tressyalina, Bima Mhd Ghaluh, Ella Wulandari, Ermawati Arief, and Ena Noveria. “Enhancing Students’ Critical Thinking in Criminal Case Solving: An AI-Based Pragmatic Application for Analyzing Authentic Indonesian Texts and Videos.” *Interactive Learning Environments* 34, no. 2 (2026): 543–75.
<https://doi.org/10.1080/10494820.2025.2504062>.

- Tri Cahyono, Soetardi, Wina Erni, and Taufik Hidayat. "Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia." *Dame Journal of Law* 1, no. 1 (2025): 1–23. <https://doi.org/10.64344/djl.v1i1.6>.
- Wahyuningtyas, Sih Yuliana. "Regulating Algorithms in the Digital Market: A Revisit of Indonesian Competition Law and Policy." *International Review of Law, Computers & Technology* 38, no. 1 (2024): 21–42. <https://doi.org/10.1080/13600869.2023.2202290>.
- Yoanda Widi Pranata. "Rekonstruksi Pasal 27 Ayat (3) UU ITE Dan Implikasinya Terhadap Kebebasan Berpendapat Di Indonesia." *IJOLARES: Indonesian Journal of Law Research* 3, no. 2 (2025): 41–47. <https://doi.org/10.60153/ijolares.v3i2.164>.
- Zaidan, M. Ali. *Menuju Pembaruan Hukum Pidana*. Sinar Grafika, 2022.
- Zaky Al Fatih, Ismail. "Peran Algoritma Media Sosial Dalam Penyebaran Propaganda Politik Digital Menjelang Pemilu." *Jurnal Kajian Strategik Ketahanan Nasional* 7, no. 1 (2024). <https://doi.org/10.7454/jkskn.v7i1.10090>.