Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

RECONSTRUCTION OF CRIMINAL LIABILITY DOCTRINE IN THE *ARTIFICIAL INTELLEGENCE ECOSYSTEM* IN INDONESIA: ANALYSIS OF NORMS' VAPOR, REINTERPRETATION OF *MENS REA AND HYBRID LIABILITY* MODEL BASED ON SUBTANTIVE JUSTICE

Agus Priyanto [1a], Fero Sanjaya [2b*], Herlita Eryke [3c]

[123] Master of Laws, Bengkulu , Bengkulu , Indonesia

[a] *aguspriyanto512@gmail.com*
[b] *samjayafero@gmail.com*
[c] *Bengkulu, ike_unib@gmail.com*

(*) Corresponding Author
samjayafero@gmail.com

ARTICLE HISTORY
Received : 20-01-2026
Revised : 07-02-2026
Accepted : 25-05-2026

KEYWORDS
Artificial Intelligence;
Criminal Liability;
Mens Rea;
Normative Gap;
Hybrid Criminal Liability;

ABSTRACT
This study addresses a critical normative deficiency in Indonesian criminal law in responding to Artificial Intelligence (AI)-based crimes. Existing legal frameworks remain anthropocentric and fail to accommodate the autonomous, multi-actor, and algorithm-driven nature of AI systems, resulting in uncertainty in attributing criminal liability. The core problem lies in the inadequacy of the mens rea doctrine and the absence of a structured liability framework capable of capturing distributed causation within AI ecosystems. Using a normative legal approach with statutory, conceptual, and comparative analysis, this study demonstrates that current regulations, including the Criminal Code, the amended ITE Law (Law No. 1 of 2024), and the Personal Data Protection Law (Law No. 27 of 2022), are structurally incapable of addressing AI-driven criminality. This study makes a distinct contribution by reconstructing criminal liability through a Hybrid Criminal Liability model that redistributes responsibility among developers, operators, and users based on their causal roles. It further advances a reconceptualization of mens rea by extending fault beyond individual intent to include systemic and design-based negligence. Unlike existing studies that remain descriptive or sectoral, this research offers a coherent doctrinal framework that integrates multi-actor liability with a risk-based approach. The proposed model provides a normatively grounded and operationalizable framework for Indonesian criminal law reform, bridging the gap between classical doctrine and technological reality while strengthening legal certainty and accountability in AI-based crimes.

INTRODUCTION

The rapid development of Artificial Intelligence (AI) has fundamentally transformed the structure of crime from individual-based actions into complex, automated, and multi-actor systems. AI no longer functions merely as a

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

tool but actively shapes decision-making processes through algorithmic autonomy. This shift disrupts the classical construction of criminal law, which is traditionally grounded in human agency as the sole subject of liability. Indonesian criminal law, as reflected in the Criminal Code and related regulations, remains anthropocentric and has not yet adapted to the structural complexity of AI-driven crimes. This mismatch creates a growing tension between technological reality and existing legal norms (Sumadi 2023; Hildebrandt 2023).

The escalation of cybercrime in Indonesia reinforces the urgency of this issue. Reports from the National Cyber and Crypto Agency indicate a significant increase in automated and adaptive cyberattacks, including deepfakes and algorithm-based manipulation. Existing regulations, such as Law Number 1 of 2024 concerning amendments to the ITE Law and Law Number 27 of 2022 concerning Personal Data Protection, primarily focus on human conduct and fail to address the distributed and system-based nature of AI-related offenses. This limitation results in regulatory fragmentation and weakens the capacity of criminal law to effectively respond to emerging forms of digital crime (BSSN 2024; Santoso and Permata 2023; Kominfo 2024).

The core doctrinal problem lies in the inadequacy of the *mens rea* concept in addressing AI-based actions. Traditional criminal law requires intent and awareness as the basis of fault, yet AI systems operate without psychological consciousness while still producing legally relevant consequences. Provisions on participation under Articles 55 and 56 of the Criminal Code are insufficient to explain the interaction between human actors and technological systems. This ambiguity creates difficulties in attributing criminal responsibility and increases the risk of impunity. The absence of a coherent liability framework further complicates law enforcement in cases involving multiple actors within an AI ecosystem (Abbott 2022; Shafira 2025).

Existing studies on AI and law in Indonesia largely focus on data protection, cybercrime policy, or ethical governance, without providing a systematic reconstruction of criminal liability doctrine. Prior research tends to remain descriptive and sectoral, emphasizing regulatory shortcomings without addressing the doctrinal limitations of *mens rea* or proposing an integrated liability model. There is a lack of analysis that connects normative gaps, doctrinal reconstruction, and multi-actor accountability within a single analytical framework (Mulyadi et al. 2026; Yeung 2023). Based on these issues, this study formulates the following research questions:

1. How do normative gaps in Indonesian criminal law limit the attribution of criminal liability in AI-based crimes?
2. To what extent is the mens rea doctrine inadequate in addressing the autonomous and system-based nature of AI?
3. How can a Hybrid Criminal Liability model be formulated to provide a coherent and adaptive framework for criminal responsibility in the AI ecosystem?

This study reconstructs criminal liability doctrine through a Hybrid Criminal Liability model that integrates multi-actor responsibility and expands fault into systemic negligence. This model provides a doctrinal and operational framework aligned with AI complexity (Barfield and Pagallo 2023; OECD 2024).

This research employs a normative legal method using statutory, conceptual, and comparative approaches. The analysis focuses on identifying doctrinal limitations and constructing a new framework of criminal liability that aligns with the complexity of AI systems. The findings are expected to contribute both theoretically and practically to the reform of Indonesian criminal law, particularly in strengthening legal certainty, accountability, and victim protection in the digital era (Marzuki 2023; Soekanto and Mamudji 2023).

METHOD

This study employs a normative legal research approach aimed at examining and reconstructing the doctrine of criminal liability within the context of Artificial Intelligence (AI)-based crimes. The normative approach is used because the primary issue lies in the inadequacy of existing legal norms and the absence of a clear framework for attributing liability in AI ecosystems. This research is prescriptive in nature, focusing on generating legal arguments and formulating adaptive doctrinal solutions. The analysis emphasizes the reinterpretation of classical criminal law concepts, particularly mens rea and liability, in response to the structural complexity of AI-driven systems (Marzuki 2023; Soekanto and Mamudji 2023).

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

The study applies three main approaches: statutory, conceptual, and comparative. The statutory approach examines relevant legal instruments, including the Criminal Code, Law Number 1 of 2024 concerning amendments to the ITE Law, and Law Number 27 of 2022 on Personal Data Protection. The conceptual approach is used to analyze doctrines of criminal liability, fault, and causation within modern criminal law theory. The comparative approach explores regulatory developments in other jurisdictions, particularly risk-based and multi-actor liability frameworks in AI governance. These approaches are integrated to produce a comprehensive and multidimensional analysis capable of supporting the formulation of a Hybrid Criminal Liability model (Ibrahim 2023; OECD 2024).

Legal materials in this study consist of primary, secondary, and tertiary sources. Primary materials include statutory regulations, while secondary materials comprise scholarly books, peer-reviewed journals, and recent research relevant to criminal law and AI. Tertiary materials, such as legal dictionaries and encyclopedias, are used to clarify key concepts. Data collection is conducted through a systematic literature study using credible academic databases, with priority given to recent and relevant sources. The analysis employs a qualitative juridical method, involving interpretation of legal norms, identification of normative gaps, and construction of legal arguments. This analytical process is conducted deductively, linking legal theory with contemporary technological developments to produce a coherent and applicable model of criminal liability (Diantha 2023; Ali 2023).

RESULT AND DISCUSSIONS

Normative Gaps in Indonesian Criminal Law

The current Indonesian criminal law framework demonstrates a structural inability to regulate AI-based criminality. The Criminal Code (KUHP) remains grounded in an anthropocentric paradigm that presumes a human actor as the sole subject of liability. This construction fails to capture the distributed and system-based nature of AI-driven crimes. The absence of explicit norms addressing algorithmic conduct creates a regulatory vacuum that cannot be resolved through conventional interpretation alone. This ambiguity weakens the effectiveness of law as a mechanism of social control and undermines legal certainty (Diantha 2023; Asshiddiqie 2023). This condition also reflects a deeper doctrinal rigidity, where legal reasoning remains confined to classical assumptions of linear causation and individual culpability, despite the emergence of non-linear and system-based interactions within AI ecosystems (Marzuki 2023; Hildebrandt 2023). As a result, the legal system is not only normatively incomplete but also conceptually misaligned with the evolving structure of technological harm.

Sectoral regulations further reinforce this gap. Law Number 1 of 2024 concerning amendments to the ITE Law focuses on conventional cybercrime patterns such as illegal access and data manipulation, without addressing autonomous decision-making systems. Law Number 27 of 2022 on Personal Data Protection introduces criminal sanctions but remains limited to human actors. This fragmentation produces legal loopholes that allow responsibility to diffuse across technological systems without clear attribution. As a result, enforcement becomes reactive and inconsistent. The persistence of this normative gap confirms that Indonesian criminal law lacks a systemic framework capable of addressing AI-based risks (Santoso and Permata 2023; BSSN 2024). Moreover, the absence of integration between these regulatory instruments prevents the formation of a coherent liability structure, thereby limiting the ability of law enforcement institutions to establish clear chains of responsibility in complex digital environments (Mulyadi et al. 2026; OECD 2024).

This normative deficiency also has direct implications for the functional capacity of criminal law in ensuring accountability and deterrence. When legal norms fail to identify responsible actors within AI ecosystems, enforcement mechanisms lose their precision and credibility. This situation increases the likelihood of selective or ineffective prosecution, particularly in cases involving multi-layered technological processes. In addition, the lack of anticipatory regulation weakens the preventive dimension of criminal law, as legal rules are unable to address risks embedded in the design and deployment of AI systems. Consequently, the persistence of this gap not only undermines legal certainty but also challenges the legitimacy of criminal law as an adaptive instrument capable of responding to contemporary technological transformations (Yulia 2023; UK Government 2023).

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Limitations of Mens Rea in AI Context

The doctrine of *mens rea* constitutes a fundamental limitation in attributing criminal liability within AI ecosystems. Classical criminal law requires intention (*dolus*) or negligence (*culpa*) grounded in human consciousness as the basis of fault. However, AI systems operate through algorithmic processes without psychological awareness, yet are capable of producing legally significant consequences. This ontological mismatch prevents the direct application of traditional fault concepts and creates a conceptual gap in linking human intent to machine-generated outcomes (Abbott 2022; Hildebrandt 2023). As a result, the doctrinal foundation of criminal liability becomes unstable when confronted with autonomous decision-making systems that function beyond immediate human control.

The limitations of *mens rea* are further reflected in the inadequacy of existing participation doctrines. Articles 55 and 56 of the Criminal Code are designed to address human-to-human interactions and assume linear causation between actors and outcomes. In contrast, AI-based crimes involve multi-layered and non-linear causal chains in which developers, operators, and users interact with autonomous systems. This complexity disrupts conventional attribution models and creates ambiguity in determining culpability. Consequently, the evidentiary process becomes significantly more difficult, as intent cannot be easily traced within distributed technological processes (Shafira 2025; Saleh 2023).

Beyond evidentiary challenges, the persistence of a rigid *mens rea* framework risks producing systemic impunity. When criminal liability depends solely on demonstrable intent, actors involved in the design or deployment of AI systems may evade responsibility by relying on the autonomous nature of the technology. This creates a structural loophole in which harmful outcomes lack attributable fault within the existing legal framework. Such a condition undermines both the deterrent and retributive functions of criminal law, as accountability cannot be effectively enforced in technologically mediated contexts (Barfield and Pagallo 2023; OECD 2024).

Therefore, the limitations of *mens rea* are not merely technical but fundamentally doctrinal. A reinterpretation of fault is required to expand liability beyond subjective intent toward a broader framework that includes systemic and design-based negligence. This shift enables criminal law to capture the realities of AI-driven harm while maintaining its normative foundations. Without such a transformation, criminal law will remain structurally incapable of addressing the complexity of contemporary digital crime (Marzuki 2023; Yulia 2023).

Hybrid Criminal Liability Model

The Hybrid Criminal Liability model is proposed as a structural response to the normative and doctrinal limitations identified in the previous sections. This model departs from the classical single-actor paradigm by introducing a multi-actor liability framework that reflects the distributed nature of AI-based crimes. Rather than concentrating responsibility on a single perpetrator, liability is allocated proportionally among developers, operators, and users based on their respective causal contributions. This approach aligns legal attribution with the systemic characteristics of AI ecosystems, where harm emerges from the interaction of multiple actors and technological processes (Suseno 2024; Barfield and Pagallo 2023).

The model is grounded in a functional analysis of roles within the AI lifecycle. Developers are responsible for the design and architecture of algorithms, including potential risks embedded in system functionality. Operators are accountable for the deployment, monitoring, and control of AI systems in real-world applications. Users bear responsibility for the manner in which AI is utilized within specific contexts. This differentiation allows for a more precise identification of fault, as liability is linked to concrete acts or omissions within each stage of the technological process. Consequently, the model overcomes the ambiguity inherent in conventional doctrines that fail to distinguish between layered contributions to harm (Mulyadi et al. 2026; OECD 2024).

A central feature of this model lies in the reconceptualization of *mens rea*. Fault is expanded beyond subjective intention to include systemic and design-based negligence, particularly in situations where risks are foreseeable yet insufficiently mitigated. This approach ensures that liability is not avoided merely because harmful outcomes are mediated through autonomous systems. At the same time, the model maintains the principle that AI itself is not recognized as an independent legal subject, but rather as an instrument that extends human agency. This balance preserves the normative foundation of criminal law while adapting it to technological complexity (Abbott 2022; Hildebrandt 2023).

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

The Hybrid Criminal Liability model also enhances the operational capacity of criminal law by providing a clearer framework for evidence and attribution. By linking liability to identifiable roles and risk-based obligations, the model facilitates a more structured assessment of causation and fault. This reduces evidentiary uncertainty and strengthens prosecutorial effectiveness in cases involving AI systems. Furthermore, the model supports a shift from reactive enforcement toward a more preventive orientation, as actors are incentivized to anticipate and mitigate risks at each stage of AI development and use (Yulia 2023; UK Government 2023).

Thus, the proposed model does not merely fill a normative gap but offers a coherent doctrinal reconstruction that integrates multi-actor accountability, expanded fault, and system-based causation. It provides both theoretical legitimacy and practical applicability, positioning criminal law as an adaptive instrument capable of responding to the evolving landscape of AI-driven crime (Marzuki 2023; OECD 2024).

Comparative Legal Analysis

Comparative analysis demonstrates that contemporary legal systems have shifted toward adaptive and risk-based approaches in regulating Artificial Intelligence. The European Union, through the Artificial Intelligence Act, adopts a risk-based regulatory framework that classifies AI systems according to their potential impact and allocates responsibilities across actors within the AI lifecycle. This approach moves beyond traditional fault-based models by imposing ex ante obligations on developers and operators, particularly in high-risk systems. As a result, liability is not solely reactive but also preventive, reflecting a broader understanding of accountability in technologically mediated environments (Veale and Borgesius 2021; European Parliament 2023).

The United States, while lacking a unified AI statute, promotes algorithmic accountability through sectoral governance and regulatory initiatives. This approach emphasizes transparency, auditability, and corporate responsibility in automated decision-making systems. Liability is not constructed through doctrinal reconstruction but through strengthening institutional oversight and compliance obligations. This model reflects a pragmatic orientation that prioritizes governance mechanisms over formal legal categorization, indicating a shift toward functional accountability within complex technological systems (Citron 2008; Selbst et al. 2019).

The United Kingdom adopts a principle-based regulatory approach that emphasizes flexibility and sectoral adaptability. Rather than imposing rigid statutory rules, the UK framework relies on core principles such as safety, accountability, and transparency, which are interpreted across regulatory bodies. This model allows the legal system to remain responsive to technological change without requiring constant legislative amendment. However, its effectiveness depends on institutional coherence and regulatory coordination, highlighting the importance of governance capacity in AI regulation (Casey, Farhangi, and Vogl 2019; Floridi et al. 2018).

In contrast, Indonesia has not yet developed a comparable framework capable of addressing the complexity of AI-based crimes. Existing regulations remain fragmented and reactive, focusing on isolated aspects of cybercrime and data protection without integrating a comprehensive liability structure. This condition places Indonesia in a lagging position within the global legal landscape, particularly in terms of anticipating systemic risks and distributing responsibility across AI actors. The absence of a risk-based and multi-actor approach limits the effectiveness of criminal law in responding to emerging technological challenges (Rahim 2022; Prasetyo 2021).

This comparative perspective confirms that the Hybrid Criminal Liability model aligns with global regulatory trends while addressing the specific limitations of Indonesian law. By integrating multi-actor liability with an expanded concept of fault and a risk-based orientation, the model reflects the direction taken by advanced legal systems without requiring a fundamental departure from national legal principles. Therefore, the proposed model is not only normatively justified but also comparatively validated as a relevant framework for reforming Indonesian criminal law in the context of Artificial Intelligence (Binns 2018; Calo 2015).

Implications for Indonesian Legal Reform

The implementation of the Hybrid Criminal Liability model carries significant implications for the reform of Indonesian criminal law, particularly in aligning legal structures with the complexity of AI-based crimes. At the legislative level, the model necessitates a shift from a purely individualistic liability framework toward a multi-actor and risk-based approach. This requires explicit recognition of role-based responsibility within statutory provisions, ensuring that developers, operators, and users are normatively positioned as accountable actors. Without such

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

reformulation, existing laws will continue to produce ambiguity in liability attribution and limit the effectiveness of criminal enforcement in technologically mediated contexts (Gless, Silverman, and Weigend 2016; Ebers 2020).

At the doctrinal level, the implications extend to the reconstruction of the concept of fault within Indonesian criminal law. The expansion of *mens rea* to include systemic and design-based negligence introduces a more adaptive standard of culpability that reflects contemporary technological realities. This shift enables the legal system to address harm arising not only from intentional acts but also from failures in system design, oversight, and risk management. As a result, criminal law evolves from a reactive instrument into a framework capable of addressing embedded risks within technological infrastructures (Danaher 2016; Pagallo 2017).

Institutionally, the adoption of this model requires a transformation in the capacity of law enforcement agencies. Investigative and prosecutorial processes must incorporate technical expertise in algorithmic systems, digital forensics, and AI governance. The absence of such capacity will render doctrinal reform ineffective in practice, as legal norms cannot be operationalized without institutional readiness. Furthermore, coordination between regulatory bodies, law enforcement, and technological experts becomes essential to ensure consistent application of the law in complex cases involving AI systems (Bathaee 2018; Kroll et al. 2017).

From a policy perspective, the model supports a transition toward a preventive and governance-oriented approach in criminal law. By emphasizing risk allocation and responsibility across the AI lifecycle, the law can function not only as a mechanism of punishment but also as a tool for risk mitigation. This approach encourages proactive compliance among actors involved in AI development and deployment, thereby reducing the likelihood of harm before it materializes. Such a shift is critical in addressing the anticipatory nature of risks embedded in autonomous systems (Marchant and Wallach 2015; Wallach and Marchant 2019).

Overall, the implications of the Hybrid Criminal Liability model extend beyond doctrinal reconstruction toward a broader transformation of the Indonesian criminal law system. The model provides a structured pathway for integrating technological considerations into legal norms while maintaining the fundamental principles of criminal responsibility. Its implementation has the potential to enhance legal certainty, strengthen accountability, and ensure that criminal law remains relevant in the face of rapid technological change. Without such reform, the gap between law and technological reality will continue to widen, undermining the effectiveness and legitimacy of the legal system.

CONCLUSION

Indonesian criminal law remains structurally inadequate in addressing AI-based crimes due to its anthropocentric orientation and the limitations of the *mens rea* doctrine in capturing system-based and multi-actor causation. This condition creates legal uncertainty and increases the risk of impunity in cases involving autonomous and algorithm-driven systems.

This study contributes by formulating a Hybrid Criminal Liability model that redistributes responsibility among developers, operators, and users based on their causal roles, while expanding the concept of fault to include systemic and design-based negligence. The model provides a coherent doctrinal framework that aligns criminal liability with the complexity of AI ecosystems without departing from the fundamental principles of criminal law.

The findings imply the need for legislative reform to incorporate multi-actor liability and risk-based approaches into the Indonesian legal system, as well as institutional strengthening to ensure effective enforcement in technologically complex cases. These reforms are essential to enhance legal certainty, accountability, and victim protection in the digital era.

This study is limited by its normative approach and does not include empirical analysis of AI-based criminal cases. Future research should examine the practical implementation of the proposed model and evaluate its effectiveness within the Indonesian criminal justice system.

REFERENCES

Abbott, R. (2022). The reasonable computer: Disrupting the paradigm of tort liability. *Boston University Law Review, 102*(1), 1–52. https://www.bu.edu/bulawreview/files/2022/02/ABBOTT.pdf

Ahdiat, A. (2024). Government sector most vulnerable to cyber incidents. *Databoks*. https://databoks.katadata.co.id

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Ali, Z. (2023). *Legal research methods*. Sinar Grafika.
Asshiddiqie, J. (2023). *The Indonesian constitution and constitutionalism*. Sinar Grafika.
Badan Siber dan Sandi Negara. (2024). *Laporan keamanan siber nasional 2024*. https://bssn.go.id
Baihaqy, A. H. A., et al. (2025). Analisis dampak kebocoran data pusat data nasional 2024 dalam perspektif HAM. *Wicarana, 4*(1), 31–37. https://ejournal-kumhamdiy.com/wicarana/article/view/167
Barfield, W., & Pagallo, U. (2023). *Research handbook on the law of artificial intelligence*. Edward Elgar Publishing. https://doi.org/10.4337/9781789905140
Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent. *Harvard Journal of Law & Technology, 31*(2), 889–938.
Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. *Proceedings of Machine Learning Research, 81*, 1–11.
Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review, 103*(3), 513–563.
Casey, B., Farhangi, A., & Vogl, R. (2019). Rethinking explainable machines. *Fordham Law Review, 88*(1), 137–172.
Citron, D. K. (2008). Technological due process. *Washington University Law Review, 85*(6), 1249–1313.
Danaher, J. (2016). Robots, law, and the retribution gap. *Ethics and Information Technology, 18*(4), 299–309. https://doi.org/10.1007/s10676-016-9403-3
Diantha, I. M. P. (2023). *Metodologi penelitian hukum normatif dalam justifikasi teori hukum*. Kencana.
Ebers, M. (2020). Regulating AI and robotics: Ethical and legal challenges. *European Review of Private Law, 28*(2), 273–302.
European Commission. (2024). *Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu
European Parliament. (2023). Artificial intelligence act: Overview of the EU framework. https://www.europarl.europa.eu
Floridi, L., et al. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines, 28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
Gless, S., Silverman, E., & Weigend, T. (2016). If robots cause harm, who is to blame? *New Criminal Law Review, 19*(3), 412–436. https://doi.org/10.1525/nclr.2016.19.3.412
Handayani, I. G. A. K. R., et al. (2023). Pendekatan normatif dalam penelitian hukum kontemporer. *Jurnal Hukum Ius Quia Iustum, 30*(1), 1–15. https://doi.org/10.20885/iustum.vol30.iss1.art1
Hernoko, A. Y. (2023). *Hukum perjanjian: Asas proporsionalitas dalam kontrak komersial*. Prenadamedia Group.
Hildebrandt, M. (2023). Bias and data protection in AI. *Computer Law & Security Review, 48*, 105790. https://doi.org/10.1016/j.clsr.2022.105790
Ibrahim, J. (2023). *Teori dan metodologi penelitian hukum normatif*. Bayumedia Publishing.
Kementerian Komunikasi dan Informatika. (2024). *Laporan isu perlindungan data dan keamanan siber 2024*. https://kominfo.go.id
Kroll, J. A., et al. (2017). Accountable algorithms. *University of Pennsylvania Law Review, 165*(3), 633–705.
Lembaga Perlindungan Saksi dan Korban. (2023). *Laporan tahunan perlindungan korban 2023*. https://lpsk.go.id
Marchant, G. E., & Wallach, W. (2015). Coordinating technology governance. *Science and Engineering Ethics, 21*(2), 463–477. https://doi.org/10.1007/s11948-014-9537-9
Marzuki, P. M. (2023). *Penelitian hukum*. Kencana.
Mulyadi, D., et al. (2026). Implementasi kebijakan pemerintah terhadap pencegahan kebocoran data pribadi dalam pelayanan publik berbasis digital. *Jurnal ISO*. https://penerbitadm.pubmedia.id/index.php/iso/article/view/3473
OECD. (2024). *Artificial intelligence, digital economy outlook 2024*. OECD Publishing. https://www.oecd.org
Pagallo, U. (2017). The laws of robots: Crimes, contracts, and torts. Springer.
Prasetyo, T. (2021). Hukum dan teknologi digital di Indonesia. *Jurnal Hukum, 28*(2), 145–160.
Rahim, A. (2022). Regulation of artificial intelligence in Indonesia: Challenges and prospects. *Journal of Indonesian Legal Studies, 7*(2), 201–220.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Saleh, R. (2023). *Perbuatan pidana dan pertanggungjawaban pidana*. Ghalia Indonesia.

Santoso, B., & Permata, R. R. (2023). Kekosongan norma dalam kejahatan siber berbasis AI. *Jurnal Legislasi Indonesia, 20*(1), 15–28. https://ejurnal.peraturan.go.id

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 59–68. https://doi.org/10.1145/3287560.3287598

Shafira, F. M. (2025). Analisis kasus kebocoran data Dukcapil 2023–2024. *Jurnal Edu Research*. https://iicls.org/index.php/jer/article/view

Soekanto, S., & Mamudji, S. (2023). *Penelitian hukum normatif: Suatu tinjauan singkat*. Rajawali Pers.

Sumadi, A. F. (2023). Tantangan hukum pidana dalam era artificial intelligence. *Jurnal Hukum & Pembangunan, 53*(2), 245–260. https://doi.org/10.21143/jhp.vol53.no2.3500

Suseno, S. (2024). Kebijakan hukum pidana dalam penanggulangan kejahatan siber. *Jurnal Hukum Ius Quia Iustum, 31*(1), 45–60. https://journal.uii.ac.id/IUSTUM/article

UK Government. (2023). *AI regulation policy paper*. https://www.gov.uk

Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International, 22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Wallach, W., & Marchant, G. E. (2019). Toward the agile governance of AI. *AI and Ethics, 1*(1), 1–9.

Waluyo, B. (2023). *Pidana dan pemidanaan*. Sinar Grafika.

World Bank. (2024). *Cybersecurity and digital trust report 2024*. https://www.worldbank.org

Yeung, K. (2023). Algorithmic regulation: A critical interrogation. *Regulation & Governance*. https://doi.org/10.1111/rego.12450

Yulia, R. (2023). *Viktimologi: Perlindungan hukum terhadap korban kejahatan*. Graha Ilmu.