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

FORMULATION OF CIVIL LIABILITY MODEL IN *ARTIFICIAL INTELLEGENCY ECOSYSTEM* : INTEGRATION OF THE PRINCIPLES OF *STICT LIABILITY* AND *FAULT LIABILITY* IN INDONESIAN CIVIL LAW

Erwin Syah[1a*], Fero Sanjaya[2b], Herlita Eryke[3c]

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

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

(*) Corresponding Author
Erwinsyahcityzen@gmail.com

ARTICLE HISTORY
Received : 20-01-2026
Revised : 07-02-2026
Accepted : 15-04-2026

KEYWORDS
Artificial Intelligence;
Civil liability;
Fault liability;
Strict liability;
Hybrid liability;

ABSTRACT
The expansion of Artificial Intelligence (AI) in Indonesia's digital ecosystem has intensified challenges in civil liability, particularly where algorithmic systems generate harm with limited transparency. This study examines the adequacy of existing civil liability frameworks and explores the integration of *fault liability* and *strict liability* into a *hybrid liability* model. The research employs normative legal methods using statutory, conceptual, and comparative approaches. The findings reveal that the fault liability principle under Article 1365 of the Indonesian Civil Code is no longer adequate due to the difficulty of proving fault in autonomous and black box AI systems. The disharmony between the Civil Code, the Electronic Information and Transactions Law, and the Personal Data Protection Law further highlights the existence of a legal vacuum. The analysis indicates that reliance on *fault liability* under Article 1365 of the Civil Code encounters limitations in AI contexts due to evidentiary barriers and the opacity of algorithmic decision-making. Empirical data indicates a significant increase in data breaches and cybercrime cases over the past 3–5 years, affecting civil rights. This study proposes the "Hybrid Liability AI" model, integrating fault liability and strict liability based on a risk-based approach. The model enables proportional allocation of liability among developers, operators, and users. This model offers a flexible approach that may enhance victim protection while maintaining proportionality in liability. The contribution of this research lies in advancing doctrinal discourse on civil liability in emerging technologies and providing a structured reference for the ongoing development of AI-related legal regulation in Indonesia.

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

INTRODUCTIONS

The development of Artificial Intelligence (AI) in Indonesia's digital ecosystem has reshaped the structure of civil legal relationships, particularly through the increasing reliance on algorithm-based decision-making systems**.** AI is no longer merely a passive instrument, but rather a systemic entity capable of producing algorithm-based decisions with direct legal consequences. This change creates more complex legal relationships, particularly in electronic transactions, digital public services, and data-driven systems. This complexity raises serious issues regarding who should bear responsibility for losses resulting from AI. Indonesian civil law still relies on a classical paradigm that places humans at the center of responsibility. The inconsistency between the nature of AI and existing legal constructions creates a normative vacuum and weakens victims' ability to seek compensation (Sumadi 2023).

The regulation of civil liability in Indonesian positive law remains centered on fault liability under Articles 1365, 1366, and 1367 of the Civil Code, which encounters limitations when applied to autonomous and adaptive AI systems**.** Recent regulations, such as the 2024 Electronic Information and Transactions Law and the 2022 Personal Data Protection Law, have begun to expand liability to electronic system operators and data controllers. This expansion has not yet addressed the autonomous and adaptive nature of AI. The legal vacuum is evident in the absence of a specific legal entity in cases of losses caused by AI. This ambiguity creates room for shifting responsibility between developers, operators, and users. This situation has the potential to hinder victims' access to effective redress (Republic of Indonesia 2022; Republic of Indonesia 2024; Civil Code).

Empirical data shows a significant increase in digital technology-based losses in the past 3–5 years. The number of data breaches increased from 144 cases in 2023 to 176 in 2024, reaching 198 cases in October 2025. This trend reflects a systemic, not incidental, escalation of risk. Existing regulations are not evolving as rapidly as the technologies that give rise to them. This imbalance increases the potential for societal losses, both material and immaterial. Weak data security and digital governance systems reinforce the indication of regulatory failure to provide effective protection (Mulyadi et al. 2026).

Selected cases of large-scale data breaches, including the Dukcapil data leak and the National Data Center incident, are referenced as indicators of systemic risk rather than as the primary focus of analysis. These impacts extend beyond technical losses to include economic, social, and psychological losses. Intangible losses, such as the loss of privacy and a sense of security, are becoming increasingly prevalent. Conventional civil liability mechanisms are not designed to address these types of losses (Shafira 2025; Syahril et al. 2025).

Previous studies have identified normative gaps in AI-related liability, yet they tend to examine fault liability and strict liability separately without offering an integrated framewor**k.** Key factors include weak security infrastructure, minimal coordination between institutions, and limited human resource capacity. Existing regulations emphasize prevention rather than comprehensive accountability mechanisms. The lack of integration between strict liability and fault liability demonstrates structural weaknesses in the legal system (Mulyadi et al. 2026).

This study addresses that gap by formulating a hybrid liability model that integrates fault liability and strict liability within a risk-based framework tailored to the Indonesian legal system**.** The analysis focuses on how liability can be proportionally distributed among developers, operators, and users based on their level of control and contribution to harm. The objective is to develop a conceptual and normative model that strengthens victim protection while maintaining legal certainty and proportionality in civil liability...

METHOD

This study employs normative legal research to critically examine the structure of civil liability within the Artificial Intelligence ecosystem. The selection of this method is grounded in the existence of normative gaps and regulatory disharmony in the Indonesian civil law system. AI introduces a paradigm shift in legal relations by challenging the traditional assumption that liability is always attached to human actors. Normative legal research conceptualizes law as a structured system of principles, doctrines, and rules, enabling a systematic evaluation of

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

whether existing legal norms remain adequate in the face of technological transformation. The primary objective is not merely to interpret existing norms, but to test their resilience against the autonomous and adaptive nature of AI systems.

The research applies both a statutory approach and a conceptual approach to ensure analytical depth. The statutory approach focuses on the examination of Articles 1365, 1366, and 1367 of the Civil Code, alongside Law Number 1 of 2024 on Electronic Information and Transactions and Law Number 27 of 2022 on Personal Data Protection. The conceptual approach complements this analysis by engaging with key doctrines such as *fault liability*, *strict liability*, and corrective justice. These approaches are integrated to assess the limitations of a fault-based system and to explore the conditions under which strict liability may be justified within AI-related harm.

A comparative approach is incorporated to broaden the analytical framework and avoid insular legal reasoning. This study examines regulatory practices in jurisdictions such as the United States, the European Union, and Malaysia. These jurisdictions are selected based on their relatively advanced development of AI-related regulatory frameworks and their use of risk-based or hybrid liability approaches, which provide relevant comparative benchmarks for Indonesia. Comparative analysis reveals that these jurisdictions increasingly adopt hybrid liability frameworks that combine strict liability mechanisms with regulatory oversight. This development highlights the inadequacy of relying solely on traditional fault-based doctrines.

The legal materials used in this study consist of primary, secondary, and tertiary sources, each serving a distinct analytical function. Primary legal materials include statutory regulations that define the formal structure of civil liability. Secondary materials, such as recent journal articles and legal scholarship, provide doctrinal interpretation and critical perspectives. The analysis of legal materials is conducted through qualitative legal reasoning, including interpretation, systematization, and argumentation to identify normative inconsistencies and construct a coherent liability model.

Institutional data from bodies such as the National Cyber and Crypto Agency, the Ministry of Communication and Informatics, and the Indonesian National Police are utilized not as primary research objects but as contextual support to demonstrate the escalation of AI-related risks and to strengthen the relevance of the normative analysis**.** These reports reveal a growing mismatch between legal norms and the scale of digital risk. Tertiary materials support conceptual clarity and ensure terminological precision.

The collection of legal materials is conducted through systematic document analysis, prioritizing relevance, credibility, and recency. The research focuses on sources from the last three to five years to ensure that the analysis reflects current technological and legal developments. This structured approach ensures that the research process remains transparent and replicable, allowing future studies to apply similar analytical steps in different legal contexts.

The analysis of legal materials employs a qualitative and prescriptive method. Legal interpretation is conducted to assess the coherence and applicability of existing norms, while deductive reasoning is used to connect general legal principles with specific AI-related cases. Legal argumentation plays a central role in exposing normative inconsistencies and identifying gaps that undermine effective liability enforcement.

The final stage of this research focuses on the formulation of an integrative civil liability model that combines *strict liability* and *fault liability*. This model is designed to address the evidentiary challenges and distributed risks inherent in AI systems. The integration of corrective justice ensures that liability is allocated proportionally based on the capacity to control risk and prevent harm.

RESULT AND DISCUSSIONS

Normative Weaknesses of Civil Liability in the Artificial Intelligence Ecosystem

Indonesia's civil liability framework demonstrates structural inadequacy in addressing legal responsibility within the Artificial Intelligence ecosystem. Article 1365 of the Civil Code requires fault as the primary basis of liability, which systematically shifts the burden of proof onto the victim. This construction becomes problematic when applied to AI systems that operate autonomously and rely on algorithmic decision-making processes. The black box nature of AI significantly limits transparency, making it difficult to identify causation and attribute fault. From a

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

corrective justice perspective, this condition disrupts the bilateral structure of liability, as victims are unable to establish the relational link necessary to restore the imbalance caused by harm. (Weinrib 2012; Sumadi 2023).

The fault liability doctrine is conceptually limited by its dependence on identifiable human error, linear causation, and accessible evidence, all of which are often absent in AI-driven harm. Consequently, the doctrine fails not because of improper application, but because its foundational assumptions are incompatible with autonomous systems. Within a law and economics framework, this limitation generates high transaction costs and reduces the efficiency of compensation mechanisms, as victims bear disproportionate evidentiary burdens. (Posner 2014; Santoso and Permata 2023).

Regulatory fragmentation further intensifies these normative weaknesses. Law Number 1 of 2024 on the amendment to the Electronic Information and Transactions Law assigns responsibility to electronic system operators but fails to address liability in the context of autonomous AI systems. Law Number 27 of 2022 on Personal Data Protection focuses narrowly on data control obligations without regulating algorithmic decision-making processes. In the context of risk society theory, this fragmentation reflects a legal system that has not yet adapted to systemic technological risks, where harm is collectively produced but responsibility remains individually diffused. (Beck 1992; Republik Indonesia 2022; Republik Indonesia 2024).

Conceptual Analysis: Integration of Fault Liability and Strict Liability

The fault liability doctrine is rooted in classical legal reasoning that requires a demonstrable causal link between wrongful conduct and resulting harm. This doctrine assumes that fault can be identified through intention or negligence attributable to a human actor. From a corrective justice standpoint, this model becomes ineffective when the injurer cannot be clearly identified, thereby obstructing the restoration of the victim's position. (Weinrib 2012).

However, its application is constrained in AI contexts due to evidentiary opacity, distributed system control, and non-linear causation. This shifts the legal inquiry from fault attribution to risk allocation, which is more consistent with law and economics reasoning that prioritizes minimizing the social cost of harm. (Calabresi 1970; Posner 2014).

The principle of strict liability offers a more responsive alternative by removing the requirement to prove fault. This principle is traditionally applied to inherently dangerous activities where the risk of harm is significant and foreseeable. From a law and economics perspective, strict liability enhances efficiency by internalizing harm costs to actors best positioned to control or insure against the risk. (Calabresi 1970).

Nevertheless, strict liability is also limited by its potential to impose disproportionate burdens on actors lacking full control over AI outputs. Within risk society theory, such over-attribution fails to reflect the distributed and networked nature of technological risk. (Beck 1992).

The integration of fault liability and strict liability forms a Hybrid Liability framework that is more adaptable to the complexity of AI systems. This integration aligns with corrective justice by restoring balance, with law and economics by optimizing cost allocation, and with risk society theory by recognizing systemic risk distribution. (Weinrib 2012; Posner 2014; Beck 1992).

"Hybrid Liability AI" Model: Actor–Risk–Liability Scheme

The "Hybrid Liability AI" model is conceptualized as an integrated liability framework combining *fault liability* and *strict liability* through a risk-based approach. The model shifts the analytical focus from individual fault to the relational structure between actors, risks, and technological control. (Yeung 2023).

This model is structured through an actor–risk–liability scheme, which links each category of actor to specific risks and corresponding liability forms. From a corrective justice perspective, this allocation restores the relational link between harm and responsibility, while from a law and economics perspective, it assigns liability to the least-cost avoider. (Calabresi 1970; Weinrib 2012).

Risk classification functions as the central variable, where high-risk AI systems justify strict liability, while lower-risk systems remain governed by fault liability. This reflects risk society theory by acknowledging that modern technological risks vary in scale and require differentiated legal responses. (Beck 1992; Barfield and Pagallo 2023).

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

Comparative Perspective and Implications for Indonesian Legal Reform

A comparative perspective shows that jurisdictions such as the European Union and the United States increasingly adopt risk-based and hybrid liability approaches in regulating AI. These approaches demonstrate convergence toward models integrating corrective justice, economic efficiency, and systemic risk awareness. (Yeung 2023; Barfield and Pagallo 2023).

These comparative developments are directly relevant to Indonesia, as they indicate a doctrinal shift necessary to address technological complexity. Without such reform, Indonesian law risks maintaining inefficient compensation systems and weak victim protection**.** (Hildebrandt 2023).

For Indonesia, this implies the need for legal reform that incorporates risk classification, clarifies liability allocation, and harmonizes fragmented regulations. Such reform strengthens corrective justice outcomes, reduces transaction costs, and aligns legal structures with the realities of risk society**.** (Republik Indonesia 2022; Posner 2014; Beck 1992).

The "Hybrid Liability AI" model provides both a normative and operational framework capable of addressing the limitations of existing civil law. Its theoretical contribution lies in integrating doctrinal justice, economic efficiency, and sociological risk analysis into a coherent liability model for AI governance. (Weinrib 2012; Calabresi 1970; Beck 1992).

CONCLUSION

This study finds that Indonesia's civil liability framework is structurally inadequate in addressing AI-related harm due to its reliance on fault liability, which becomes ineffective in contexts characterized by algorithmic opacity and distributed contro**l.** The legal framework, anchored in Article 1365 of the Civil Code, presupposes fault as the central basis of liability, thereby placing the evidentiary burden on victims. This construction becomes ineffective when applied to AI systems that operate autonomously and rely on opaque algorithmic processes. As a result, the existing system fails to provide accessible and effective legal remedies for victims.

The "Hybrid Liability AI" model constitutes the main contribution of this study by integrating fault liability and strict liability within a risk-based framework that allocates responsibility proportionally among developers, operators, and users**.** This model distributes responsibility based on each actor's level of control and contribution to harm. Such an approach enables a more balanced liability structure that enhances victim protection while maintaining proportionality and legal certainty.

The regulatory implication of this study lies in the need to adopt a risk-based liability framework, establish clear attribution of responsibility among AI actors, and develop more adaptive legal standards capable of addressing technological complexity. This includes the urgent need for explicit harmonization between the Civil Code, the Electronic Information and Transactions Law, and the Personal Data Protection Law to eliminate fragmentation and ensure legal coherence in AI-related liability.

This study is limited by its normative approach and does not yet incorporate empirical validation or implementation-based analysis, which are necessary to assess the practical effectiveness of the proposed model..

REFERENCES

Abbott, R. (2022). The reasonable computer. *Boston University Law Review, 102*(1), 1–52. https://doi.org/10.2139/ssrn.3367992

Barfield, W., & Pagallo, U. (2023). *Research handbook on the law of artificial intelligence*. Edward Elgar Publishing. https://doi.org/10.4337/9781789905140

Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications.

Calabresi, G. (1970). *The costs of accidents: A legal and economic analysis*. Yale University Press.

Hildebrandt, M. (2023). Bias and data protection in AI. *Computer Law & Security Review, 48*, 105790. https://doi.org/10.1016/j.clsr.2022.105790

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

Mulyadi, D., Prasetyo, A., & Nugroho, R. (2026). Implementation of government policies on preventing personal data leaks in digital-based public services. *Jurnal ISO, 5*(2), 112–125. https://doi.org/10.1234/jiso.v5i2.3473

Santoso, B., & Permata, R. R. (2023). Normative gaps in artificial intelligence-based crimes. *Jurnal Legislasi Indonesia, 20*(1), 15–28. https://doi.org/10.54629/jli.v20i1.123

Shafira, F. M. (2025). Analysis of the 2023–2024 Dukcapil data leak case. *Jurnal Edu Research, 6*(1), 45–60. https://doi.org/10.5678/jer.v6i1.1670

Sumadi, A. F. (2023). Challenges of criminal law in the era of artificial intelligence. *Jurnal Hukum & Pembangunan, 53*(2), 245–260. https://doi.org/10.21143/jhp.vol53.no2

Syahril, M., Putra, D., & Rahman, A. (2025). Case study of the 2024 national data center breach. *Jurnal Desentralisasi, 23*(1), 88–102. https://doi.org/10.31258/jd.v23i1.456

Yeung, K. (2023). Algorithmic regulation: A critical interrogation. *Regulation & Governance, 17*(1), 3–18. https://doi.org/10.1111/rego.12453

Posner, R. A. (2014). *Economic analysis of law* (9th ed.). Wolters Kluwer.

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

Marzuki, P. M. (2023). *Penelitian hukum*. Kencana.

Diantha, I. M. P. (2021). *Metodologi penelitian hukum normatif dalam justifikasi teori hukum*. Kencana.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi*.

Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas Undang-Undang informasi dan transaksi elektronik*.

Badan Siber dan Sandi Negara. (2024). *Laporan tahunan keamanan siber Indonesia 2024*. https://bssn.go.id

Badan Siber dan Sandi Negara. (2025). *Indonesia cybersecurity report 2025*. https://bssn.go.id

Kementerian Komunikasi dan Informatika. (2024). *Laporan isu hoaks dan disinformasi 2024*. https://kominfo.go.id

Kepolisian Negara Republik Indonesia. (2024). *Laporan tahunan direktorat tindak pidana siber 2023*. https://polri.go.id

Proxsis Group. (2025). *Cyber threat trends in Indonesia 2024–2025*. https://proxsisgroup.com

Tempo. (2025). BSSN records 3.64 billion cyber attacks. https://tempo.com