

Criminal Liability for the Misuse of Personal Data by Corporations: A Criminal Law and Corporate Liability Perspective

Lebrina Wonlele¹, Appe Hutaauruk², Hotman Sinambela³, Sunarno⁴

Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Mpu Tantular, Indonesia

Article Info

Article history:

Accepted: 19 Agustus 2026

Publish: 2 September 2026

Keywords:

Criminal Law;

Corporate Criminal Liability;

Corporate Culture Model;

Data Misuse;

Personal Data Protection.

Abstract

The rapid expansion of digital technologies has significantly increased the risk of personal data misuse by corporations, creating complex legal challenges in determining corporate criminal liability. Although Indonesia enacted Law Number 27 of 2022 on Personal Data Protection, the practical application of criminal liability against corporations remains problematic due to the limitations of traditional criminal law doctrines in attributing actus reus and mens rea to corporate entities. This study aims to analyze the formulation of corporate criminal liability for the misuse of personal data and to examine future criminal law policies that can strengthen legal enforcement against corporate offenders. This research employs a normative legal method using statutory, conceptual, and comparative approaches. Primary legal materials consist of Indonesian legislation concerning personal data protection and corporate criminal liability, while secondary materials are derived from recent national and international scholarly journals. The findings demonstrate that conventional doctrines, particularly the Identification Theory, are insufficient to address decentralized digital corporations operating through automated decision-making systems. Instead, the Corporate Culture Model provides a more appropriate framework by evaluating organizational policies, governance structures, and institutional compliance in determining corporate fault. Furthermore, the study recommends integrating strict liability with a due diligence defense, strengthening digital forensic standards, recognizing AI-generated evidence, and adopting proportional turnover-based financial sanctions as effective mechanisms to enhance deterrence. These reforms are expected to establish a more adaptive and effective corporate criminal liability system capable of protecting personal data rights while ensuring legal certainty and accountability within Indonesia's digital economy.

This is an open access article under the [Lisensi Creative Commons Atribusi-BerbagiSerupa 4.0 Internasional](https://creativecommons.org/licenses/by-sa/4.0/)



Corresponding Author:

Appe Hutaauruk

Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Mpu Tantular, Indonesia

Email Coresspondent: appehturuk@gmail.com

1. INTRODUCTION

The rapid advancement of information and communication technology has transformed personal data into one of the most valuable assets in the digital economy. Corporations increasingly collect, process, and commercialize personal data to improve business performance and competitiveness. However, the extensive processing of personal data has also increased the risk of unauthorized access, data breaches, and misuse of personal information, creating serious legal challenges regarding corporate accountability and the protection of individual privacy rights (Falevi, 2024).

Indonesia responded to these challenges by enacting Law Number 27 of 2022 concerning Personal Data Protection, which recognizes corporations as legal subjects that may be held criminally liable for unlawful personal data processing. Nevertheless, the implementation of corporate criminal liability remains problematic because conventional criminal law doctrines were originally designed to attribute criminal responsibility to natural persons rather than complex corporate entities operating through decentralized organizational structures and automated decision-making systems (Azhar & Mahyani, 2023).

Previous studies have demonstrated that Indonesia's legal framework for personal data protection still requires substantial improvement. Comparative research indicates that Indonesia's enforcement mechanisms remain less comprehensive than those adopted in several developed jurisdictions, particularly regarding the attribution of corporate fault, the imposition of criminal sanctions, and the effectiveness of legal enforcement against corporations responsible for personal data breaches (Anggriani *et al.*, 2026).

Recent scholarship also emphasizes that corporate liability should not merely focus on individual employees who commit violations but should evaluate organizational governance and institutional failures that enable unlawful processing of personal data. Weak internal controls, inadequate cybersecurity measures, and poor compliance systems frequently become the primary causes of large-scale personal data breaches committed by corporations (Guntoro *et al.*, 2022).

Furthermore, the doctrine of piercing the corporate veil has received increasing attention as a mechanism for preventing directors and senior management from avoiding criminal responsibility when institutional negligence contributes to personal data protection failures. This approach seeks to ensure that corporate structures cannot be misused to shield decision-makers from legal accountability (Simanullang & Yustika, 2026).

From an international perspective, the implementation of the General Data Protection Regulation (GDPR) demonstrates that effective corporate accountability requires strict enforcement supported by substantial financial penalties capable of creating deterrent effects. Turnover-based sanctions have significantly improved corporate compliance with personal data protection obligations throughout the European Union (Ruohonen & Hjerpe, 2020).

Although previous studies have substantially contributed to the development of personal data protection law and corporate criminal liability, most of them focus on regulatory compliance, comparative legal analysis, or administrative enforcement. Limited research has comprehensively reconstructed the doctrinal framework for attributing criminal liability to corporations responsible for personal data misuse within Indonesia's criminal law system (Buckley *et al.*, 2024).

Therefore, the novelty of this study lies in reconstructing corporate criminal liability by integrating the Corporate Culture Model, systemic negligence, due diligence defense, digital forensic standards, and AI-generated evidence into a comprehensive framework for determining criminal responsibility under Indonesia's Personal Data Protection Law (Ismaidar & Ula, 2025).

Based on these considerations, this study aims to analyze the formulation of corporate criminal liability for the misuse of personal data under Indonesia's Personal Data Protection Law and to formulate future criminal law policies capable of strengthening corporate accountability while ensuring effective protection of personal data rights in the digital era.

2. METHOD

This study employed a normative legal research method to examine corporate criminal liability for the misuse of personal data under Indonesia's Personal Data Protection Law. Normative legal research emphasizes the analysis of legal norms, statutory regulations, legal doctrines, and judicial concepts to evaluate the adequacy of existing legal frameworks in addressing corporate responsibility for personal data violations. This approach is appropriate because the study focuses on the interpretation and reconstruction of criminal law doctrines rather than empirical observation or quantitative measurement (Falevi, 2024).

The research adopted three complementary approaches: the statutory approach, the conceptual approach, and the comparative approach. The statutory approach examined Law Number 27 of 2022 concerning Personal Data Protection, the Indonesian Criminal Code, the Electronic Information and Transactions Law, and Supreme Court Regulation Number 13 of 2016 concerning corporate criminal liability. The conceptual approach analyzed legal doctrines related to corporate criminal liability, including Identification Theory, Vicarious Liability, Strict Liability, and the Corporate Culture Model. The comparative approach compared Indonesia's legal framework with international standards, particularly the European Union's General Data Protection Regulation (GDPR), to identify best practices for strengthening corporate accountability (Anggriani *et al.*, 2026).

The legal materials used in this study consisted of primary, secondary, and tertiary legal sources. Primary legal materials included statutes and regulations governing personal data protection and corporate criminal liability. Secondary legal materials consisted of recent peer-reviewed national and international journal articles discussing personal data protection, cybercrime, corporate liability, and criminal law policy. Tertiary legal materials included legal dictionaries, encyclopedias, and other supporting references used to clarify legal terminology and concepts (Azhar & Mahyani, 2023).

Data collection was conducted through a comprehensive literature study by identifying, selecting, and reviewing relevant legal documents, legislation, scholarly journal articles, and international legal instruments related to corporate misuse of personal data. The selected materials were systematically classified according to the research objectives to ensure consistency in legal interpretation and doctrinal analysis (Guntoro *et al.*, 2022).

3. RESULTS AND DISCUSSION

a. Formulation and Application of Corporate Criminal Liability for Personal Data Misuse under Indonesia's Personal Data Protection Law

The analysis demonstrates that Indonesia's Personal Data Protection Law has established corporations as independent subjects of criminal law capable of bearing criminal responsibility for unlawful processing and misuse of personal data. This finding indicates a significant shift from the traditional criminal law paradigm that primarily focused on individual offenders toward a modern corporate accountability framework. Nevertheless, the implementation of this legal framework remains limited because the statutory provisions do not provide comprehensive guidance for attributing criminal intent and unlawful conduct to corporate entities operating through complex organizational structures. Consequently, law enforcement authorities continue to experience substantial difficulties in identifying the legal basis for imposing criminal sanctions directly upon corporations involved in personal data misuse (Falevi, 2024).

The present study further reveals that the principal challenge lies in determining the relationship between corporate decision-making mechanisms and the criminal elements of *actus reus* and *mens rea*. Conventional criminal law generally attributes criminal liability to individuals who intentionally commit prohibited acts. However, corporate misconduct involving personal data frequently results from

collective organizational decisions, automated processing systems, and institutional policies rather than direct actions performed by a single individual. This organizational complexity creates evidentiary barriers in proving that the corporation itself possessed criminal intent, thereby reducing the effectiveness of criminal law enforcement under the Personal Data Protection Law (Azhar & Mahyani, 2023).

Another important finding concerns the limitations of the Identification Theory in addressing contemporary corporate structures. The research indicates that identifying directors or senior executives as the sole embodiment of corporate intent is increasingly inadequate because modern corporations often distribute decision-making authority across multiple managerial levels while relying extensively on algorithmic systems and digital automation. As a consequence, responsibility for unlawful personal data processing may become fragmented among several organizational units, allowing corporations to avoid criminal liability by arguing that no single individual intentionally committed the offence. This situation weakens legal certainty and reduces the deterrent function of criminal sanctions (Guntoro *et al.*, 2022).

The findings also demonstrate that organizational negligence constitutes one of the most significant causes of personal data misuse by corporations. Weak cybersecurity governance, insufficient internal supervision, inadequate employee training, and ineffective compliance mechanisms frequently contribute to large-scale personal data breaches. Rather than representing isolated technical failures, these incidents illustrate institutional deficiencies within corporate governance systems. Accordingly, corporate liability should be assessed by evaluating whether organizational policies, risk management procedures, and compliance systems adequately prevented foreseeable violations of personal data protection obligations (Ismaidar & Ula, 2025).

Comparative analysis with previous studies indicates substantial consistency regarding the necessity of expanding corporate accountability beyond individual offenders. Similar to earlier research emphasizing institutional responsibility, the present study finds that criminal liability should reflect the collective organizational conduct that enables unlawful processing of personal data. Nevertheless, this study extends previous scholarship by demonstrating that organizational governance and compliance structures should become the principal indicators for attributing criminal fault within Indonesian criminal law. This broader perspective enables law enforcement authorities to evaluate institutional behavior rather than relying exclusively on evidence against individual employees or corporate directors (Suartha & Ivory, 2024).

Based on these findings, this study concludes that the current formulation of corporate criminal liability requires doctrinal reconstruction to ensure more effective protection of personal data rights. The research demonstrates that criminal responsibility should no longer depend exclusively upon proving the subjective intention of individual corporate officers but should also encompass institutional negligence reflected in organizational culture, governance quality, and compliance systems. Such an approach provides greater legal certainty, strengthens criminal law enforcement, and better reflects the realities of contemporary digital corporations operating within Indonesia's rapidly evolving information society (Haditama & Sugianto, 2025).

b. Future Criminal Law Policy for Strengthening Corporate Liability in Personal Data Protection

The findings of this study indicate that Indonesia's current criminal law policy has not fully adapted to the rapidly evolving characteristics of digital crime

involving corporate misuse of personal data. Although the Personal Data Protection Law establishes criminal sanctions for corporations, its enforcement framework remains largely dependent on conventional criminal law doctrines that emphasize individual liability rather than institutional accountability. This limitation reduces the effectiveness of criminal enforcement because contemporary personal data violations are frequently committed through complex organizational processes, automated information systems, and cross-border digital infrastructures. Consequently, future criminal law policy should prioritize institutional accountability by developing legal standards capable of addressing corporate misconduct within an increasingly digitalized business environment (Anggriani *et al.*, 2026).

Another significant finding concerns the need to reconstruct the evidentiary framework applied in corporate criminal proceedings involving personal data misuse. Traditional criminal investigations primarily rely upon documentary evidence, witness testimony, and individual confessions. However, digital crimes involving corporate data processing generate sophisticated electronic evidence, including server logs, algorithmic decision records, cloud computing activities, and automated transaction histories. Therefore, criminal procedure should recognize digital forensic standards and technologically advanced methods of evidence examination to ensure that complex organizational misconduct can be investigated objectively without relying solely on direct human actions. Such reforms would substantially improve the effectiveness of criminal investigations involving digital corporations (Velasco, 2022).

The present research also demonstrates that integrating the doctrine of Strict Liability with a Due Diligence Defense provides a more balanced framework for determining corporate criminal responsibility. Under this approach, corporations may initially be presumed responsible for unlawful personal data processing resulting from organizational failures. Nevertheless, corporations should retain the opportunity to demonstrate that comprehensive compliance mechanisms, cybersecurity systems, employee supervision, and preventive risk management measures had been properly implemented before the incident occurred. This balanced approach simultaneously strengthens personal data protection while maintaining fairness for corporations that have genuinely fulfilled their legal obligations (Krol, 2023).

Comparative analysis with international regulatory practices further indicates that Indonesia may benefit from adopting more effective corporate sanctioning mechanisms similar to those implemented under the European Union's General Data Protection Regulation. Rather than imposing relatively modest criminal fines, sanctions should reflect the economic capacity of corporate offenders by calculating financial penalties based on annual corporate turnover. Such proportional sanctions create stronger deterrent effects because they eliminate the economic incentives that may encourage corporations to prioritize commercial profits over investments in personal data protection and cybersecurity infrastructure (Ruohonen & Hjerpe, 2020).

The findings further reveal that future criminal law policy should strengthen preventive corporate governance alongside punitive sanctions. Effective protection of personal data cannot rely exclusively upon criminal punishment imposed after violations occur. Instead, corporations should be legally required to establish comprehensive compliance programs, conduct periodic cybersecurity audits, implement continuous employee training, perform privacy impact assessments, and maintain transparent internal reporting mechanisms. These preventive obligations enable corporations to identify organizational risks before personal data breaches occur,

thereby reducing both legal violations and economic losses resulting from inadequate data governance (Buckley *et al.*, 2024).

Finally, this study demonstrates that future reforms of Indonesia's corporate criminal liability system should move beyond conventional punishment by integrating technological developments into criminal justice administration. The recognition of AI-generated evidence, standardized digital forensic procedures, stronger international cooperation for cross-border investigations, and institutional evaluation through the Corporate Culture Model collectively provide a more adaptive legal framework capable of responding to emerging forms of corporate cybercrime. Compared with previous studies that primarily emphasize administrative enforcement or comparative regulation, this research proposes a comprehensive reconstruction of criminal law policy that combines institutional accountability, technological evidence, proportional sanctions, and preventive corporate governance. Such an integrated framework is expected to strengthen legal certainty, improve corporate compliance, and ensure more effective protection of personal data rights within Indonesia's expanding digital economy (Haryanto & Heliany, 2026).

4. CONCLUSION

This study concludes that the existing framework of corporate criminal liability under Indonesia's Personal Data Protection Law has established corporations as subjects of criminal responsibility but has not yet provided an adequate doctrinal foundation for attributing criminal fault in cases involving the misuse of personal data. The research demonstrates that traditional doctrines, particularly the Identification Theory, are insufficient to address the organizational complexity of modern digital corporations, where unlawful personal data processing frequently results from institutional decision-making, automated systems, and systemic governance failures rather than the actions of individual corporate officers. Consequently, corporate criminal liability should be reconstructed by emphasizing organizational accountability through the Corporate Culture Model, which evaluates institutional governance, compliance systems, and systemic negligence as the primary basis for determining criminal responsibility.

Furthermore, the study finds that future criminal law policy should move beyond conventional approaches by integrating technological and institutional developments into the corporate liability framework. Strengthening corporate accountability requires the adoption of strict liability combined with a due diligence defense, the recognition of digital forensic standards and AI-generated evidence, as well as proportional turnover-based sanctions capable of producing effective deterrence while maintaining legal certainty. These findings contribute to the development of a more adaptive and comprehensive model of corporate criminal liability that is better suited to protecting personal data rights and supporting sustainable digital governance in Indonesia.

5. BIBLIOGRAPHY

- Anggriani, D., Febriyani, E., & Situmeang, A. (2026). Pertanggungjawaban pidana korporasi atas kebocoran data pribadi di Indonesia: Studi komparatif dengan Amerika Serikat dan Uni Eropa. *Fundamental Justice*, 7(1). <https://doi.org/10.30812/fundamental.v7i1.6237>
- Azhar, D. P., & Mahyani, A. (2023). Pertanggungjawaban pidana korporasi sebagai pelaku tindak pidana penyebaran data pribadi. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3(1), 640–651. <https://doi.org/10.53363/bureau.v3i1.200>

- Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, 10(1), tyae017. <https://doi.org/10.1093/cybsec/tyae017>
- Falevi, Y. (2024). Corporate criminal liability for misuse of personal data. *Syiah Kuala Law Journal*, 8(3), 485–499. <https://doi.org/10.24815/sklj.v8i3.43280>
- Guntoro, M. A., Sanusi, & Sudewo, F. A. (2022). Corporate criminal liability for leakage of personal data. In *Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education (MALAPY 2022)*. <https://doi.org/10.4108/eai.28-5-2022.2320539>
- Haditama, T. K., & Sugianto, F. (2025). A comparative analysis of corporate criminal liability for AI-based malware: A study of Indonesian and European Union law. *Indonesia Law Reform Journal*, 5(2). <https://doi.org/10.22219/ilrej.v5i2.39901>
- Haryanto, S. E., & Heliany, I. (2026). Corporate liability for cybercrime: A legal analysis of the protection of personal data subjects. *FOCUS: Journal of Social Studies*, 7(1), 14–20. <https://doi.org/10.37010/fcs.v7i1.2165>
- Ismaidar, & Ula, R. F. (2025). Pertanggungjawaban pidana korporasi terhadap kebocoran data pribadi konsumen dalam perspektif hukum pidana siber di Indonesia. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, 2(3). <https://doi.org/10.62383/humif.v2i3.1802>
- Krol, K. (2023). Corporate criminal liability for AI-enabled cybercrime: A case study of a ransomware attack. *Journal of Cybersecurity and Privacy*, 3(1), 1–15. <https://doi.org/10.3390/jcp3010001>
- Ruohonen, J., & Hjerpe, K. (2020). The GDPR enforcement fines at glance. *arXiv*. <https://doi.org/10.48550/arXiv.2011.00946>
- Simanullang, B. R. H., & Yustika, L. (2026). Piercing the corporate veil: The urgency of criminal liability of directors in personal data protection law. *International Journal of New Approaches to Law and Rationality in Nationhood, Governance, and Rights Advocacy*, 1(2). <https://doi.org/10.56861/nalarnagara.v1i2.266>
- Suartha, I. D. M., & Ivory, J. (2024). Corporate crime liability: Beyond rule reform on Indonesia criminal policy. *Focus Journal Law Review*, 4(2). <https://doi.org/10.62795/fjl.v4i2.281>
- Velasco, C. (2022). Cybercrime and artificial intelligence: An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, 23, 109–126. <https://doi.org/10.1007/s12027-022-00702-z>
- Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, 89(1). <https://doi.org/10.1140/epjb/e2015-60754-4>
- Yang, L., Tian, M., Xin, D., Cheng, Q., & Zheng, J. (2024). AI-driven anonymization: Protecting personal data privacy while leveraging machine learning. *arXiv*. <https://doi.org/10.48550/arXiv.2402.17191>