Journal of Scientific Insights
E-ISSN: 3062-8571
DOI: https://doi.org/10.69930/jsi.v3i2.739
Research Article

ScienceTech. Group

Vol. 3 (2), 2026
Page: 177-185

Weaknesses in the Construction of Corporate Criminal Liability in Article 70 of the Personal Data Protection Law

Abdul Azis Pangeran *, Tina Amelia

Faculty of Law, Borobudur University, Indonesia
*Email (corresponding author): pangeran_aziz@yahoo.com

Abstract. *The development of digital technology in Indonesia has increased the use of personal data by various corporations, from large companies to digital startups. This situation creates a significant risk of data breaches, necessitating clear and effective corporate criminal liability. Article 70 of the Personal Data Protection Law addresses corporate criminal liability; however, its structure reveals notable weaknesses. This provision primarily focuses on the faults of individual managers, overlooking the collective and systemic responsibilities of the organization; thus, the narrow perspective makes it challenging to prove and impose sanctions effectively. This study employs a qualitative normative method with a statutory and conceptual approach. The regulatory analysis examines the Personal Data Protection Law to assess its normative structure, forms of accountability, and types of sanctions. The conceptual approach highlights theories of corporate fault, liability, and the principle of data protection as a constitutional right, aiming to examine normative weaknesses and propose a normative reconstruction. The results show that Article 70 still lacks objective indicators, has the potential to lead to scapegoating, and underemphasizes preventive mechanisms (compliance-based liability). The proposed normative reconstruction includes a clear separation of corporate and managerial responsibilities, integration of compliance obligations, implementation of risk-based accountability, and expansion of types of sanctions in the form of compliance orders, data governance reform, and corporate probation. This approach is expected to improve the effectiveness of law enforcement, strengthen corporate accountability, and optimally protect data subjects' rights.*

Keywords: *Corporate Criminal Liability; Corporate Fault; Compliance Obligation; Data Governance*

1. Introduction

The development of digital technology has fundamentally changed the way personal data is collected, processed, and stored in Indonesia (Segara, 2025). Digital transformation is driving the growth of online services that utilize personal data as a strategic resource (Nugroho, 2025). The increase in digital transactions and online interactions has created a significant need for data protection. New regulations regarding personal data have been established to align national laws with the emerging challenges of digital business practices (Kinanti, 2025). The transformation demands a legal framework that balances the interests of corporations, individuals, and the state.

The growth of technology companies, including large corporations and digital startups, increases the risk of systemic personal data breaches (Hakim, 2024). Large companies manage data for millions of individuals, increasing risks of mismanagement, data leaks, and misuse(Hidayat, 2025). Rapidly growing digital startups tend to lack robust data governance, making operational errors more likely (Yuliani, 2025). This risk is

Received: 28 March 2026 / Accepted: 28 April 2026 / Available online: 30 April 2026

widespread because data breaches impact not only individuals but can also have social, economic, and political implications (Pakina, 2024). This highlights the need for strict law enforcement against personal data breaches.

Corporate criminal liability is a crucial instrument to ensure companies bear the legal consequences for violations committed through or on behalf of their organizations (Alfianda, 2024). Corporate criminal law allows sanctions to be directed not only at individuals but also at entities with the legal capacity to commit harmful acts (Herawati, 2025). This concept requires clear norms regarding organizational culpability and the limits of management responsibility. The existence of effective corporate criminal liability impacts corporate compliance with data management standards. Weak regulations have the potential to create structural impunity for business entities.

Article 70 of the Personal Data Protection Law (PDP Law) is the central norm governing corporate criminal liability for personal data breaches. This article stipulates that corporations can be punished if proven to have committed certain violations, but the formulation of the norm remains unclear (Sianturi, 2024). The article's formulation tends to emphasize the role of management as individual subjects without mapping organizational responsibility systematically. This ambiguity poses challenges for law enforcement officials in determining the elements of corporate culpability. This article also lacks indicators that can be used as measuring tools to assess structural negligence.

The construction of corporate criminal liability can be analyzed through identification theory, which emphasizes that management acts as a representative of the corporation. This theory asserts that management's actions can be considered corporate acts if they are carried out within the scope of the organization's interests and authority (Rodliyah, 2020). This approach links the element of individual culpability with the responsibility of the legal entity. While this theory facilitates the identification of legal subjects, it still faces difficulties when management does not act directly, but the organization still experiences violations. This understanding is relevant for assessing how Article 70 of the PDP Law positions management as the key to accountability.

Vicarious liability emphasizes that corporations are responsible for the actions of individuals acting in the organization's interests (Kurniawan, 2022). This model allows criminal sanctions to be transferred to the corporation even if specific individuals are not convicted, thus encouraging systemic compliance. This approach also requires an evaluation of internal procedures and organizational culture as contributing factors to violations. Vicarious liability emphasizes the importance of managerial control and operational compliance in preventing data breaches (Sari, 2023). National regulations need to adopt objective indicators to assess corporate involvement through this mechanism.

Strict liability and corporate fault emphasize organizational responsibility without requiring proof of individual subjective fault. This approach is relevant for personal data breaches because losses can occur due to systemic negligence (MULADI, 2023). Corporate fault emphasizes the role of governance, internal procedures, and organizational culture in preventing breaches (Latifah, 2025). This model also encourages corporations to establish oversight and risk mitigation mechanisms. Implementing this concept in the PDP Law will add a preventive dimension and ensure that corporations are structurally accountable.

Corporate cybercrime has unique characteristics, including being automated, systemic, and able to cross borders (Pakarti, 2025). This complexity makes it difficult for law enforcement to prove individual culpability. Violations can occur through failed system

programming, network configuration, or operational procedures. The impact of harm can be widespread and cumulative, posing a serious threat to data subjects' rights (Sabadina, 2021). The criminal law framework must adapt concepts of culpability and responsibility to effectively prosecute corporations.

Proving mens rea in the context of corporate cybercrime is a major challenge because harmful actions can be indirect or unintentional (Ar, 2024). Corporations can commit culpability through management decisions, flawed internal procedures, or oversight failures. The complexity of organizational structures makes it difficult to identify responsible parties. Law enforcement officials must be able to interpret the relationship between systemic negligence and data subject harm. This requires an integrated normative and analytical approach that integrates criminal theory and business practice.

Personal data is part of human rights and the right to privacy, so its violation has constitutional implications (Rianarizkiwati, 2022). The state has an obligation to protect citizens' data, and corporations, as legal entities, must fulfill a similar responsibility (Elza, 2025). This protection requires regulations that clearly define the responsibilities of organizations and individual administrators. The principle of protecting data subjects' rights must be the basis for constructing corporate criminal liability. Weaknesses in norms can reduce the effectiveness of protection, necessitating the reconstruction of articles that take constitutional rights into account.

2. Methods

This research employs a normative qualitative method emphasizing an in-depth study of relevant laws and regulations, legal doctrine, jurisprudence, and academic literature to analyze the construction of corporate criminal liability under Article 70 of the Personal Data Protection Law. The statutory regulatory approach is carried out by examining the legal provisions of the Personal Data Protection Law to identify normative structures, weaknesses, and potential disharmony between norms. The analysis is conducted systematically to understand how these norms regulate legal subjects, forms of liability, types of sanctions, and available enforcement mechanisms. A conceptual approach is employed to develop a theoretical framework concerning corporate criminal liability, corporate fault, compliance obligations, and risk governance. This framework also evaluates the significance of criminal law theory, corporate liability theory, and the principle of personal data protection as a constitutional right. By combining these approaches, the research offers a thorough critical analysis and normative reconstruction while providing practical legal recommendations that align with the evolving landscape of digital business practices and cybercrime law.

3. Results and Discussion

3.1 Normative Construction and Weaknesses of Corporate Criminal Liability in Article 70 of the Personal Data Protection Law

Article 70 of the PDP Law establishes corporations and their management as legal entities subject to criminal penalties for violations of personal data protection provisions. This article emphasizes that criminal liability can be imposed on legal entities other than individuals, but the formulation of the norm emphasizes the role of management. The forms of criminal liability regulated are still limited to the imposition of criminal sanctions and administrative fines, without specifying a mechanism for assessing systemic organizational

culpability. The types of sanctions listed are repressive in nature, thus providing little incentive for corporations to improve data governance preventively. This normative structure creates the impression that management is the only party factually accountable for violations.

The construction of Article 70 creates ambiguity regarding the basis of corporate culpability because it does not separate the individual responsibility of management from the responsibility of the organization. The formulation of the article tends to adopt an identification theory approach, but does not accommodate the concept of corporate fault, which emphasizes systemic errors. It makes it difficult for law enforcement officials to determine whether violations occurred due to management decisions or negligence in the corporation's internal procedures. This ambiguity creates legal risks for companies that have implemented compliance mechanisms but are still subject to sanctions due to structural negligence that is not explicitly regulated. This analysis emphasizes the need for objective standards to assess the overall involvement of corporations.

The ambiguous relationship between corporations and their management increases the risk of scapegoating, where certain individuals are held responsible while legal entities escape sanctions. Article 70 does not regulate the limits of management's authority or the mechanism for evaluating their role within the organizational structure. This opens up opportunities for corporations to blame management symbolically, while the root of the problem lies in the internal control system. This ambiguity undermines the effectiveness of criminal law as an instrument for enforcing data subjects' rights. Such legal practices have the potential to create injustice and undermine public trust in personal data regulations.

The absence of indicators of corporate accountability makes it difficult to consistently apply criminal sanctions. Article 70 does not specify the extent of systemic negligence, oversight procedures, or data governance standards that must be met. Law enforcement officials must interpret norms subjectively, leading to inconsistencies in court decisions. This uncertainty impacts legal certainty for corporations attempting to comply with data protection standards. Regulations that lack objective indicators also reduce corporate incentives to develop internal compliance systems.

The dominant approach is repressive, providing minimal mechanisms for preventing violations. Article 70 emphasizes criminal sanctions but does not encourage corporations to implement compliance-based liability or internal reform. This model fails to accommodate risk mitigation strategies based on governance and organizational culture. The lack of normative instructions regarding prevention allows large corporations to continue engaging in high-risk practices without tangible consequences. This suggests that the regulatory focus remains limited to retributive, rather than preventive, measures.

The potential for disharmony between Article 70 and other national criminal laws is an additional issue. The lack of synchronization with the Criminal Code, the Corruption Law, the Money Laundering Law, and the Supreme Court Regulation could lead to differing interpretations in court. These differing norms increase the risk of overlapping or legal loopholes that corporations could exploit. Harmonization of corporate accountability principles is necessary for effective implementation without creating normative conflicts. This disharmony also complicates the litigation process and hinders legal certainty for the parties involved.

The difficulty of proving the element of fault *(mens rea)* is a fundamental problem in enforcing Article 70. Corporate cybercrime often occurs through procedural negligence or

systemic decisions, making it difficult to attribute individual culpability. Law enforcement must interpret the relationship between management actions and organizational failure, which is often abstract and multi-level. The lack of normative guidance exacerbates these obstacles, resulting in many cases ending without clear corporate accountability. This complexity demands strengthening the theory and practice of proof in cybercorporate criminal law.

Uncertainty about law enforcement has the potential to weaken the deterrent effect of Article 70. Corporations may perceive the risk of sanctions as low due to a weak framework for constructing norms and evidentiary procedures. This uncertainty can also create an imbalance between corporate interests and the protection of data subjects' rights. The public and stakeholders lose confidence in the effectiveness of the regulation. The situation suggests that Article 70 requires clarification and reformulation of norms that emphasize enforcement mechanisms.

The weak deterrent effect raises the risk that corporations will continue practices that harm data subjects. Sanctions limited to fines or criminal penalties for specific managers do not always encourage companies to improve their governance. Unclear indicators of systemic negligence also reduce pressure on organizations to conduct regular audits and mitigate risks. The absence of structural deterrence implies the risk of repeated violations. This indicates the need to integrate preventive and retributive accountability into the regulations.

The risk of corporate impunity and injustice to data subjects is a real consequence of the weaknesses in Article 70. Corporations can escape sanctions despite serious violations, while individual managers face criminal penalties. This situation creates legal inequality and weakens the protection of data subjects' constitutional rights. This injustice also poses ethical challenges for law enforcement officials and the courts. Improved norms must emphasize the overall responsibility of legal entities so that corporations cannot escape legal consequences.

3.2 International Comparison and Normative Reconstruction of Corporate Criminal Liability

The European Union, through the GDPR, implements a hybrid administrative-criminal model to regulate corporate responsibility in personal data protection. This approach combines administrative sanctions with the possibility of criminal sanctions for corporations that fail to fulfill data management obligations. The GDPR emphasizes organizational responsibility for internal controls, compliance procedures, and risk mitigation. The application of this model demonstrates that a combination of preventive and repressive sanctions can improve corporate compliance. This system also provides clear guidance for law enforcement officials in assessing structural negligence.

The UK Data Protection Act regulates corporate liability through both criminal and civil mechanisms. This law allows data subjects to pursue civil damages, while law enforcement officials can impose criminal sanctions against violating corporations. This approach broadens the spectrum of corporate accountability and increases incentives to comply with regulations. Corporations are required to establish adequate internal governance to minimize the risk of violations. The model shows that the integration of layered legal mechanisms can balance the interests of protecting corporate rights and legal certainty.

Singapore, through its PDPA, emphasizes systems-based and governance-based corporate liability. This regulation emphasizes the evaluation of internal procedures, regular audits, and an organizational culture of compliance. Corporate misconduct can be identified through systemic failures, not solely the actions of individual managers. The method encourages corporations to build clear and accountable risk control structures. Singapore demonstrates that criminal liability can be effective when linked to systemic compliance and organizational culture.

Lessons from international comparisons emphasize the importance of integrating criminal sanctions and prevention. Criminal sanctions provide a deterrent effect, while prevention mechanisms encourage long-term compliance. Countries that adopt a hybrid model have shown a reduction in data breach incidents through stricter governance. The approach is relevant for Indonesia as a reference for strengthening Article 70 of the PDP Law. National regulations require objective standards to assess systemic corporate involvement.

The reconstruction of corporate criminal liability should be based on systemic failures, governance negligence, and organizational culture. This formulation allows law enforcement officials to objectively assess culpability without relying solely on the actions of individual managers. This system identifies the root causes of violations and forces corporations to develop internal mechanisms to prevent similar errors. Good governance and a culture of compliance are key indicators of accountability. Such a formulation will strengthen the effectiveness of law enforcement.

A clear separation of corporate and management liability is a crucial element of norm reconstruction. Corporations can be punished for structural failures, while management is responsible for individual decisions that violate the law. This separation prevents scapegoating practices and ensures fairness for all parties. This mechanism also provides legal certainty for managers who carry out proper governance. The separation of responsibilities strengthens the integrity of the criminal justice system.

The integration of compliance obligations and risk-based accountability encourages a preventative approach. Corporations must demonstrate concrete efforts in establishing oversight and risk mitigation mechanisms. These obligations serve as parameters for law enforcement officials in assessing organizational culpability. This model also fosters a culture of sustainable accountability. The implementation of compliance obligations reduces the likelihood of repeated data breaches.

Expanding the types of sanctions is an integral part of norm reconstruction. Sanctions can include compliance orders, data governance reform, and corporate probation to ensure internal improvements. The sanction model emphasizes structural improvements rather than simply financial penalties. Corrective sanctions force corporations to restructure their procedures and organizational culture. This approach increases the effectiveness of law enforcement and the protection of data subjects' rights.

Objective indicators of corporate accountability are an important tool for facilitating law enforcement. Parameters such as internal audits, compliance certifications, procedural documentation, and evidence of risk mitigation can form the basis for assessments. These indicators provide certainty for law enforcement, corporations, and data subjects. Objective standards also minimize subjective interpretations in litigation. Implementing such indicators will strengthen fairness and accountability.

Reconstructing norms that incorporate lessons from the GDPR, the UK Data Protection Act, and Singapore's PDPA will enhance the effectiveness of Article 70 of the Data Protection Act. The approach emphasizes structural responsibility, organizational culture, and preventative compliance. The integration of criminal, civil, and corrective sanctions puts pressure on corporations to build robust data governance. This model makes law enforcement more operational, fair, and sustainable. Such reconstruction can serve as a blueprint for corporate criminal regulation in the digital era in Indonesia.

Conclusions

Article 70 of the current PDP Law demonstrates significant weaknesses in constructing an effective framework for corporate criminal liability. The formulation of the norm tends to emphasize individual culpability of management without clearly addressing the corporation's structural and systemic responsibilities, creating difficulties in proving and imposing criminal sanctions. This ambiguity affects the effectiveness of law enforcement and weakens the protection of data subjects' rights. Corporations can exploit loopholes to evade accountability through unclear internal practices or unregulated procedural failures. Therefore, there is an urgent need for a normative reconstruction model that enables criminal law to assess culpability. Such a model would encourage improvements in governance and organizational culture, ensuring that corporations are fully accountable for personal data breaches that harm the public. This approach also increases legal certainty for law enforcement officials and upholds the principle of justice for data subjects, while fostering a culture of sustainable corporate compliance.

Suggestions for enhancing the construction of Article 70 should include several key aspects. Legislators must revise the norm by incorporating concepts of corporate fault, risk governance, and compliance obligations to make the regulation more effective and proactive. Law enforcement requires clear interpretive guidelines to assess systemic corporate misconduct, including objective indicators encompassing internal procedures, audits, and organizational culture, to minimize subjective interpretations in the litigation process. Digital corporations are required to implement a comprehensive data governance framework, encompassing risk mitigation, internal oversight, and compliance mechanisms, to prevent recurrence of violations and effectively protect data subjects' rights. Implementing these measures will strengthen corporate accountability, enhance the effectiveness of law enforcement, and ensure the protection of the public's constitutional rights against misuse of personal data.

Conflicts of Interest

The authors declare no conflict of interest.

References

Alfianda, R. R. (2024). Tindak Pidana Korupsi Dan Pertanggungjawaban Korporasi. *Wathan: Jurnal Ilmu Sosial Dan Humaniora, 1*(1), 64-75.

Ar, A. M. (2024). Peran Niat (Mens Rea) Dalam Pertanggungjawaban Pidana Di Indonesia. *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin, 1*(3), 240-252.

Elza, P. (2025). Tanggung Jawab Negara Terhadap Pelanggaran Hak Konstitusional Warga Negara Di Era Digital. *Jurnal Ilmu Hukum Indonesia, 1*(1), 10-18.

Hakim, L. (2024). Tantangan Dan Strategi Investasi Pada Perusahaan Startup Teknologi Di Indonesia. *Productivity: Journal Of Integrated Business, Management, And Accounting Research, 1*(2), 75-84.

Herawati, E. M. (2025). Analisis Yuridis Terhadap Tanggung Jawab Korporasi Dalam Tindak Pidana Kejahatan Luar Biasa Di Bidang Ekonomi. *Jurnal Sosial Teknologi, 5*(7), 2819-2831.

Hidayat, R. A. (2025). Efektivitas Manajemen Risiko Sumber Daya Manusia Dalam Menghadapi Risiko Keamanan Data Karyawan Di Sektor Teknologi. *Manajemen Kreatif Jurnal, 3*(1), 1-9.

Kinanti, P. D. (2025). Integrasi Teknologi Digital Dan Regulasi Untuk Perlindungan Konsumen Yang Efektif Dan Transparan Dalam Transaksi Elektronik. *Jurnal Media Akademik (JMA), 3*(9).

Kurniawan, K. D. (2022). Pertanggungjawaban Pidana Korporasi Menurut Vicarious Liability Theory. *Jurnal Hukum Ius Quia Iustum, 29*(2), 324-346.

Latifah, G. &. (2025). Peran Whisteblowing System, Dukungan Budaya Organisasi, Dan Efektivitas Surprise Audit Dalam Mencegah Fraud: Kajian Literatur Sistematis. *JURNAL ILMIAH EDUNOMIKA, 9*(3).

MULADI, D. (2023). *Pertanggungjawaban Pidana Korporasi (Corporate Criminal Responsibility).* Bandung: Alumni.

Nugroho, W. &. (2025). Transformasi Digital Dan Dampaknya Terhadap Kompetensi Sumber Daya Manusia Di Era Industri 5.0. *Jurnal Ilmiah Global Education, 6*(3), 1959-1974.

Pakarti, M. H. (2025). *Hukum Siber: Menyikapi Tantangan Hukum Di Era Digital.* Jambi: PT. Nawala Gama Education.

Pakina, R. &. (2024). Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan Di Indonesia: Keseimbangan Antara Keamanan Dan Hak Asasi Manusia. *Journal Of Scientech Research And Development, 6*(1), 273-286.

Rianarizkiwati, N. (2022). Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia. *Jurnal Hukum Sasana, 8*(2).

Rodliyah, R. S. (2020). Konsep Pertanggungjawaban Pidana Korporasi (Corporate Crime) Dalam Sistem Hukum Pidana Indonesia. *Jurnal Kompilasi Hukum, 5*(1), 191-206.

Sabadina, U. (2021). Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online. *Lex Renaissance, 6*(4), 799-814.

Sari, N. K. (2023). Konsep Pertanggungjawaban Pelaku Pidana Korporasi Menurut Vicarious Liability Theory. *Al Qalam: Jurnal Ilmiah Keagamaan Dan Kemasyarakatan, 17*(5), 3507-3518.

Segara, K. G. (2025). Perkembangan Teknologi Informasi Di Indonesia: Tantangan Dan Peluang. *Journal Sains Student Research, 3*(1), 21-33.

Sianturi, C. G. (2024). Peran Hukum Dalam Melindungi Data Pribadi. *Innovative: Journal Of Social Science Research, 4*(5), 2607-2624.

Yuliani, W. Y. (2025). Evaluasi Prospek Bisnis Start-Up Digital: Kajian Kualitatif Aspek Pasar, Teknis, Dan Manajemen. *Journal Of Business Economics And Management, 1*(3), 171-177.