INNOVATIVE: Journal Of Social Science Research
Volume 5 Nomor 1 Tahun 2025 Page 5053-5065
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Legal Responsibility of Companies in Cases of Personal Data Breaches

Febrian Dirgantara[1], Dharma Setiawan Negara[2], Didit Darmawan[3✉], Endra Andie Aryanto[4], Alwi Mohamad Shahab[5]
Universitas Sunan Giri Surabaya
Email: dr.dititdarmawan@gmail.com[3✉]

Abstrak

Kasus kebocoran data pribadi di Indonesia menjadi isu yang semakin mendesak dalam era digital. Penelitian ini bertujuan untuk menganalisis tanggung jawab hukum perusahaan dalam kasus kebocoran data pribadi, mengidentifikasi faktor-faktor utama yang menyebabkan insiden tersebut, dan mengevaluasi kelemahan dalam sistem regulasi serta pengawasan yang ada. Pendekatan yuridis normatif digunakan dengan mengkaji Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan regulasi terkait lainnya. Hasil penelitian menunjukkan bahwa kebocoran data disebabkan oleh lemahnya infrastruktur keamanan, rendahnya kesadaran karyawan, serta kurangnya kepatuhan terhadap standar perlindungan data. Selain itu, ketidakharmonisan regulasi dan kelemahan pengawasan menjadi hambatan utama dalam memastikan kepatuhan perusahaan terhadap kewajiban hukum. Penelitian ini merekomendasikan peningkatan keamanan data melalui teknologi canggih, harmonisasi regulasi, penguatan mekanisme pengawasan, dan edukasi masyarakat tentang hak-hak perlindungan data pribadi. Dengan demikian, kajian ini diharapkan dapat memberikan kontribusi praktis dan teoretis bagi pengembangan sistem perlindungan data pribadi yang lebih efektif di Indonesia.

Kata Kunci: *Kebocoran Data Pribadi, Tanggung Jawab Hukum, Yuridis Normatif, Regulasi, Pengawasan, Perlindungan Konsumen, Indonesia*

Abstract

Personal data leak cases in Indonesia are becoming an increasingly pressing issue in the digital era. This study aims to analyze the legal responsibility of companies in cases of personal data leaks, identify the main factors causing the incident, and evaluate weaknesses in the existing regulatory and supervisory systems. A normative legal approach is used by reviewing Law Number 27 of 2022 concerning Personal Data Protection and other related regulations. The results of the study indicate that data leaks are caused by weak security infrastructure, low employee awareness, and lack of compliance with data protection standards. Regulatory disharmony and weak supervision are major obstacles in ensuring company compliance with legal obligations. This study recommends improving data security through advanced technology, regulatory harmonization, strengthening supervisory mechanisms, and educating the public about personal data protection rights. Thus, this study is expected to provide practical and theoretical contributions to the development of a more effective personal data protection system in Indonesia.

Keywords: *Personal Data Leakage, Legal Responsibility, Normative Juridical, Regulation, Supervision, Consumer Protection, Indonesia*

INTRODUCTION

The rapidly growing digitalization era brings various conveniences and efficiencies, but also raises serious challenges, especially in the form of cybercrime. According to Aryadi et al. (2024), increased connectivity and use of information technology have created a gap for cybercriminals to exploit system weaknesses. Firmanto et al. (2024) added that this threat is aimed at every individual and even organizations and countries, often the target of attacks. Rahman et al. (2024) explained that types of cybercrime, such as online fraud and identity theft, continue to grow along with digital innovation. Issalillah and Hardyansah (2024) emphasized the importance of cybersecurity awareness and education to prevent greater losses. Negara and Darmawan (2023) noted that collaboration between the government, private sector and society is essential to create a safer digital environment. Fajar et al. (2024) and Isnaeni et al. (2023) emphasized the need for stricter regulations and more sophisticated technology to address the growing threat of cybercrime. The crime stems from leaked personal data.

In the rapidly growing era of digitalization, companies in various sectors are facing major challenges to manage the personal data entrusted to them. One of the main issues that has emerged is personal data leakage, which has become a serious problem for many companies, including large corporations with sophisticated security systems. Personal data

leaks harm the individuals who are victimized, and cause reputational and financial damage to the companies responsible for managing the data.

In an increasingly advanced digital era, cybersecurity has become one of the crucial aspects for companies to protect sensitive data and information. Threats to customers' personal data are increasing, making it important for companies to understand and address potential risks that can lead to data leakage. Data leakage cases are often caused by weak corporate cybersecurity systems. Some companies do not have adequate security protocols to protect customers' personal data from threats such as hacking, malware, or internal misuse of data. This condition is exacerbated by the lack of regular monitoring and evaluation of the implemented security system so that companies fail to detect and prevent potential threats.

Regulatory vagueness and lack of compliance with legal standards related to personal data protection are also major obstacles. Many companies do not fully understand or implement data protection regulations in accordance with applicable laws. This leads to legal uncertainty for customers whose data has been misused or disseminated without authorization (Azmi et al., 2024). The lack of awareness and education regarding customers' rights over their personal data adds to the complexity of this issue. Many individuals are unaware of the risks that can occur when their personal data is shared or collected by companies. This ignorance is often exploited by companies to avoid responsibility for managing personal data that is not up to standard.

Another challenge lies in the lack of oversight mechanisms from the competent authorities. Many cases of data leakage do not receive serious attention from regulators so that the companies involved are not adequately sanctioned. This creates a legal loophole that allows companies to ignore their legal responsibilities.

Rapid technological developments, such as artificial intelligence and big data analytics, are having a significant impact on the way data is managed and protected. While these technologies offer great potential for data collection and analysis, they also increase the risk of personal data leakage. The emergence of new technologies such as artificial intelligence and big data analytics also increases the risk of personal data leakage. These technologies enable the collection of large amounts of data at high speeds, but often without adequate protection measures in place. The imbalance between technological progress and adaptive regulation exacerbates this situation

In some cases, personal data leaks occur due to employee or third-party service provider negligence. This suggests weaknesses in internal risk management, including a

lack of training and oversight of individuals with access to sensitive data. This kind of negligence can have far-reaching impacts, especially if the leaked data includes sensitive information such as identity numbers, bank accounts or medical history.

Companies also face the challenge of dealing with the increasingly complex threat of cyberattacks. Cyber criminals are now using more sophisticated techniques to steal personal data, such as phishing, ransomware, and distributed denial-of-service (DDoS) attacks. These attacks harm customers, and disrupt the overall operations of the company. The lack of transparency from companies to disclose data leakage incidents is also a serious problem. Many companies choose to cover up such incidents to protect their image in the public eye. This results in customers not getting enough information to protect themselves from potential data misuse (Novarianti et al., 2025). The challenges of globalization also add to the complexity of managing personal data. In many cases, customer data is stored on servers located in other countries, which may have different data protection regulations. These differences create legal and operational barriers for companies to ensure optimal data protection.

This study aims to analyze the legal responsibility of companies in cases of personal data leakage from a normative juridical perspective. This study also aims to identify the main factors that lead to data leakage and evaluate the weaknesses in the existing regulatory and supervisory systems. Thus, this study is expected to serve as a foundation for the development of more responsive policies to protect people's personal data and encourage stronger legal responsibility from companies in the digital era.

RESEARCH METHOD

This research uses a normative juridical approach that aims to analyze the legal responsibility of companies in cases of personal data leakage based on applicable laws and regulations, legal doctrines, and jurisprudential principles. This approach was chosen because it is able to provide an in-depth understanding of the relevant legal framework and its application related to personal data protection.

Data collection was conducted through a literature study that included primary, secondary, and tertiary legal materials. Primary legal materials include laws, government regulations, and policies related to personal data protection, such as Law Number 27 Year 2022 on Personal Data Protection (PDP Law). Meanwhile, secondary legal materials involve scientific literature such as journals, books, and articles that discuss the legal aspects of

personal data protection. Tertiary legal materials include legal dictionaries, encyclopedias, and other supporting documents.

Data analysis was conducted qualitatively using the deductive method. The first stage in the analysis is to identify and categorize relevant regulations to determine the legal obligations of companies related to personal data management. Next, an evaluation of the application of these regulations in practice is conducted through case studies of data leaks that have occurred in Indonesia and in other countries. A comparative approach is also used to compare the legal arrangements for personal data protection in Indonesia with other countries that have more mature data protection systems, such as the European Union with its General Data Protection Regulation (GDPR).

This research also uses normative analysis methods to assess the extent to which existing regulations have reflected the principles of justice, legal certainty, and expediency. This analysis focuses on identifying legal loopholes that can be utilized by companies to avoid their legal responsibilities in cases of personal data leaks.With this approach, the research is expected to provide strategic recommendations for strengthening the legal framework governing personal data protection as well as increasing corporate accountability for maintaining customer data security.

RESULT AND DISCUSSION

Corporate Legal Responsibility in Personal Data Leak Cases from a Normative Juridical Perspective

Personal data protection is a crucial element in the digital era that increasingly relies on data processing for various business purposes. The legal responsibility of companies in cases of personal data leakage is regulated in various laws and regulations in Indonesia, particularly Law No. 27 of 2022 on Personal Data Protection (PDP Law). This law sets out the basic principles that data controllers must adhere to in order to maintain the security and confidentiality of individuals' personal data. However, in practice, violations of these obligations often occur, causing significant negative impacts for data owners.

When it comes to protecting personal data, clear and strict regulations are essential to ensure that companies take responsibility for the data they manage. Indonesia's Personal Data Protection Law (PDP Law) provides a legal framework governing data controllers' obligations to protect sensitive information. However, implementation of the regulation often faces challenges, especially in terms of interpretation and application of the necessary protection measures. Article 15 of the PDP Law requires data controllers to

implement adequate technical and organizational measures to protect personal data from threats of unauthorized access, unauthorized disclosure, and data destruction. Failure to fulfill this obligation may be grounds for asserting corporate legal liability. However, the definition of adequate technical measures is often subject to varying interpretations, creating legal loopholes that allow companies to effectively avoid liability.

From a normative juridical perspective, corporate legal liability in data breach cases includes administrative, civil and criminal liability. Administrative liability involves sanctions imposed by data protection authorities, such as administrative fines or orders to improve data security systems. Meanwhile, civil liability gives data owners the right to file a lawsuit for compensation for the losses they have suffered. Criminal liability relates to the application of legal sanctions against companies or individuals involved in serious violations of data protection provisions.

The implementation of administrative liability as stipulated in Article 57 of the PDP Law often faces technical obstacles and institutional weaknesses. One of the main issues is the lack of capacity of supervisory institutions to conduct comprehensive audits of companies that manage personal data on a large scale. As a result, many violations go undetected or are not adequately addressed.

Civil liability provides an opportunity for individuals to sue for damages for losses they have suffered due to data leaks. Article 52 of the PDP Law provides the legal basis for filing such a lawsuit. However, its implementation is still limited by people's low awareness of their legal rights. The burden of proof in data breach cases is often a significant obstacle for plaintiffs, given the technical nature of the issues at hand.

Criminal liability in cases of personal data leakage, as stipulated in Article 64 of the PDP Law, includes sanctions in the form of significant fines and/or imprisonment for individuals found guilty. However, the application of this criminal liability is often constrained by the uncertainty of proving the elements of intent or gross negligence, which are prerequisites for the imposition of criminal penalties (Watkat et al., 2024).

The normative juridical approach also identifies gaps in the harmonization of regulations related to personal data protection. Although UU PDP has provided a strong legal basis, some sectoral regulations, such as those on telecommunications and banking, are still not fully harmonized with the provisions of UU PDP. This disharmony creates legal uncertainty that can be exploited by companies to avoid their responsibilities.

The principle of accountability stipulated in Article 16 of the PDP Law requires companies to ensure that all personal data management processes are in accordance with

the established data protection principles. The application of this principle is often limited to formal documentation without being accompanied by concrete actions that reflect compliance with the principle.

Further analysis shows that although the PDP Law provides for fairly severe sanctions, the existing enforcement mechanisms are still unable to provide a significant deterrent effect. Many companies would rather pay administrative fines than make the necessary investments to improve their data security. This points to the need to strengthen oversight and enforcement mechanisms so that corporate legal responsibility can be implemented more effectively.

From a comparative perspective, the implementation of corporate legal liability in personal data leaks in Indonesia still lags behind compared to countries that have adopted stricter data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union. The GDPR sets higher fines and gives supervisory authorities greater powers to conduct inspections and enforcement.

In conclusion, corporate legal liability in cases of personal data leakage from a normative juridical perspective is a complex issue that requires a holistic approach. Although the PDP Law has provided an adequate legal framework, weak implementation and lack of regulatory harmonization are the main challenges to realizing effective personal data protection. For this reason, it is necessary to strengthen the legal framework and increase the capacity of supervisory institutions to ensure that corporate legal responsibility can be strictly enforced.

Identify Key Factors Causing Data Leakage and Weaknesses in Regulatory and Oversight Systems

The rampant cases of personal data leaks in Indonesia can be traced to various underlying factors related to technical weaknesses, organizational weaknesses, and weaknesses in regulation and supervision. One of the main causes is the weak cybersecurity infrastructure owned by the company. Many companies have not implemented an adequate data security system, making them vulnerable to cyberattacks such as hacking, phishing, or malware.

In an increasingly complex digital era, data security is a top priority for companies to protect sensitive information. However, many companies still overlook the importance of investing in security technologies, which can be fatal to the integrity of their data. To address this issue, companies need to shift their paradigm and see investment in data

security as an essential strategic need. The lack of adequate investment in security technology is a fundamental issue. Companies often consider investment in data security as an additional cost burden, rather than a strategic necessity. In fact, implementing advanced technologies such as data encryption and strong firewalls can significantly reduce the risk of data leakage. This negligence increases the opportunity for irresponsible parties to exploit existing security gaps (Annafa et al., 2024). Therefore, companies should allocate sufficient budget for security technologies and conduct regular evaluations of existing systems to ensure optimal protection of their data.

In an increasingly connected world, personal data protection is a shared responsibility within organizations. However, many companies overlook this important aspect by not providing adequate training to employees on data security. Without sufficient understanding, employees can become the weak point in a company's security system. The lack of employee training and awareness about the importance of personal data protection is one of the main causes of data leakage. Employees are often the weak point in a company's security system, either through ignorance or negligence. For example, the practice of sharing passwords or opening suspicious links from emails are common entry points for cyberattacks. To address this issue, companies should implement regular and thorough data security training programs and create a culture of security awareness among employees so that they can recognize and avoid potential threats that could compromise personal data.

Another significant factor is companies' non-compliance with regulatory data security standards. Although Law No. 27 of 2022 on Personal Data Protection (PDP Law) requires companies to adopt adequate technical and organizational measures, many companies do not fulfill this obligation. This is often due to the lack of consistent law enforcement, so there is not a strong enough incentive for companies to comply with the regulations.

Disharmony in regulations is also an important factor that worsens the situation. For example, sectoral regulations such as those in banking, telecommunications, and e-commerce are not fully aligned with the provisions of the PDP Law. This disharmony creates legal loopholes that can be exploited by companies to avoid their responsibility for data leaks.

In personal data protection efforts, effective supervision is a key element to prevent data leaks. However, many supervisory agencies face serious challenges in terms of resources and technology, resulting in an inability to conduct comprehensive audits of

companies. The absence of adequate oversight can create loopholes that are exploited by irresponsible parties. Weak oversight systems are also a major cause of failure to prevent data leakage. Responsible supervisory agencies often lack the human resources and technology to conduct thorough audits of companies that manage personal data. As a result, many violations go undetected or are not adequately sanctioned (Hutagalung et al., 2024). To address this issue, it is important for the government and relevant agencies to increase resource allocation, both in the form of staff training and investment in advanced audit technology so that supervision of companies can be conducted more effectively and violations can be followed up with strict sanctions.

The lack of transparency in data management also worsens the situation. Many companies do not provide enough information to consumers about how their data is managed and protected. This lack of transparency violates the principle of transparency stipulated in the PDP Law, and lowers consumers' trust in the company.

Another significant weakness is the lack of an efficient reporting mechanism. In many cases, data leaks are only discovered after reports from third parties or after the data is traded on the black market. Existing reporting mechanisms do not provide sufficient incentives for companies to report data leaks voluntarily, for fear of bad reputation and potential sanctions.

In terms of monitoring, the absence of uniform audit standards is a major challenge. Each industry sector tends to have a different approach to measuring compliance with data protection regulations. This inconsistency creates legal ambiguity that makes monitoring and enforcement difficult. Lack of public education about their rights to personal data is also a significant cause of data leakage (Zahwani & Nasution, 2024). Many individuals do not realize that they have the right to know how their data is being used and the right to request the deletion of data that is no longer relevant. This ignorance is exploited by companies to avoid responsibility (Samin, 2024).

An evaluation of the regulations shows that while the PDP Law has established severe sanctions, the implementation mechanism is still ineffective. Many companies prefer to pay fines rather than invest in better security systems. This shows that the existing sanctions do not provide a strong enough deterrent effect.

A comparison with international practices, such as the General Data Protection Regulation (GDPR) in the European Union, shows that the PDP Law still has many shortcomings. The GDPR, for example, requires companies to appoint a Data Protection Officer (DPO) who is fully responsible for data protection. In Indonesia, a similar obligation

has not been widely implemented and so responsibilities are often fragmented among various departments within the company.

Finally, the lack of integration between central and local governments in supervision is also a factor that affects the effectiveness of data protection. Different approaches and priorities between the central and local governments create gaps in supervision, which ultimately harms consumers as data owners. By identifying the main factors causing data leakage and evaluating weaknesses in regulation and supervision, it can be concluded that personal data protection in Indonesia needs strengthening in various aspects. Harmonizing regulations, increasing the capacity of supervisory institutions, and educating the public are important steps to improve personal data security in the future.

CONCLUSION

This study reveals that corporate legal liability in cases of personal data breaches in Indonesia still These measures are expected to create a safer legal environment and provide better protection for consumers, as well as encourage companies to be more responsible in the management of personal data.faces many challenges, both in terms of regulatory implementation and supervision. Factors such as weak security infrastructure, low employee awareness, and non-compliance with security standards are the main causes of data leaks. Regulatory disharmony and lack of transparency in data management exacerbate the situation. The ineffectiveness of supervision by authorized agencies is also one of the main obstacles leading to the weak application of sanctions for companies that violate the rules.

In normative juridical terms, personal data leaks indicate a gap in the implementation of Law No. 27 of 2022 on Personal Data Protection. Although the law has provided a fairly clear legal framework, weak law enforcement mechanisms and inconsistent supervision make this regulation unable to provide maximum protection for consumers. This shows the need for strategic steps to improve the existing personal data protection system.

Companies need to increase investment in data security systems by implementing advanced technologies such as encryption and double authentication to protect consumers' personal information. Regular training for employees on the importance of personal data protection should be an integral part of company policies. Harmonization of regulations between industry sectors and the implementation of uniform national standards should also be done immediately to reduce existing legal loopholes. The

government needs to develop more effective oversight mechanisms, including the use of digital technology for compliance audits.

Public education should be improved so that consumers are more aware of their rights regarding personal data protection. Socialization through public campaigns can help improve people's understanding of how to protect their personal data from potential misuse. In addition, it is necessary to implement efficient dispute resolution mechanisms, such as mediation and arbitration, to accelerate the resolution of data leakage cases. Supervisory institutions should also be equipped with sufficient resources to conduct periodic audits of companies that manage personal data.

These measures are expected to create a safer legal environment and provide better protection for consumers, as well as encourage companies to be more responsible in the management of personal data.

DAFTAR PUSTAKA

Ali, S., Saputra, R., Darmawan, D., & Hardyansah, R. (2024). The application of criminal law in addressing hazardous products: A case study of consumer protection in Indonesia. Legalis et Socialis Studiis, 2(3), 1–8.

Annafa, S. W., Simanjuntak, H. P. G. H., & Ayudia, M. A. (2024). Tanggung Jawab Hukum Bank dalam Kasus Kebocoran Data Nasabah. Jurnal Multidisiplin Ilmu Akademik, 1(6), 129-135.

Aryadi, D. W., R. Hardyansah, D. Darmawan, R. Saputra, A. R. Putra, D. S. Negara, A. Maulani. (2024). Prosecution on Online Gambling Based on Enforcement of Criminal Law In Indonesia, International Journal of Service Science, Management, Engineering, and Technology, 5(2),1–6.

AS, I. K., Nisa, B. K., Prayindria, D. A., & Setiawati, E. S. (2025). Perlindungan Hukum Terhadap Nasabah Perusahaan Asuransi. Causa: Jurnal Hukum dan Kewarganegaraan, 10(4), 21-30.

Azmi, M. N. A., Saifudin, H., Purba, C. T., Suryaningtyas, A., & Situmorang, U. S. (2024). Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan: Indonesia. Jurnal Multidisiplin Ilmu Akademik, 1(6), 448-458.

Darmawan, D. et al. (2021). Psychological Perspective in Society 5.0, Zahir Publishing, Jogjakarta

Fajar, I., R. Hardyansah, & D. Darmawan. (2024). Development of Cybercrime Law in Indonesia: Challenges and Prospects. Journal of Science, Technology and Society,

5(1), 1-8.

Firmanto, R., R. Hardyansah, & D. Darmawan. (2024). Responsibility of Banks in Preventing Name Abuse in Credit Applications, Bulletin of Science, Technology and Society, 3(3), 14-19.

Hutagalung, A. M. C., Marendra, N. R., & Hosnah, A. U. (2024). Perlindungan Terhadap Konsumen Dalam Kasus Kebocoran Data Bank Syariah Indonesia. Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora, 2(1), 156-165.

Isnaeni, M., D. Darmawan, S. Sutriyono, D. Sulistiono, & A. D. Octavianto. (2023). The Crime of Brand Counterfeiting In Commerce, Studi Ilmu Sosial Indonesia, 3(2), 101-118.

Issalillah, F. & R. K. Khayru. (2023). Legal Perspective on Patient Rights in Complementary and Alternative Medicine (CAM), Legalis et Socialis Studiis, 1(2), 1-13.

Issalillah, F. & R. Hardyansah. (2024). Relevance of Privacy within the Sphere of Human Rights: A Critical Analysis of Personal Data Protection, Bulletin of Science, Technology and Society, 3(1), 31-39.

Negara, D.S. & D. Darmawan. (2023). Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. Bulletin of Science, Technology and Society, 2(2), 13-19.

Novarianti, W. D., Meliala, A. P. P. S., Yusuf, N. A. S., & Melati, B. N. C. (2025). Kerahasiaan Bank vs Hak Atas Informasi: Mengurai Konflik Kepentingan dalam Perlindungan Data Pribadi. Jurnal Multidisiplin Ilmu Akademik, 2(1), 103-114.

Rahman, A., D. Darmawan, & R. Saputra. (2024). Analysis of Cross-border Payment Regulation and its Impact on Consumers in Indonesia, Bulletin of Science, Technology and Society, 3(2), 23-28.

Samin, H. H. (2024). Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif. Jurnal Ilmiah Research Student, 1(3), 1-15.

Tamaka, R. S., A. I. Wuryani, Y. N. Lethy, F. Issalillah, & R. Hardyansah. (2023). Legal Review of Patients' Rights in the Health Insurance System, Studi Ilmu Sosial Indonesia, 3(2), 69-84.

Tampil, V.C., A. Mubasyiroh, R. K. Khayru, D. Darmawan, & B. A. Prasetyo. (2023). Legal Protection for Patients in Health Services at Community Health Centers, Studi Ilmu Sosial Indonesia, 3(2), 85-100.

Watkat, F. X., Ingratubun, M. T., Ingsaputro, M. H., & Hartantyo, A. T. (2024).

Pertanggungjawaban Pidana Pengendali Data Pribadi Terhadap Kebocoran Data Pribadi Warga Negara Indonesia. Jurnal Hukum Ius Publicum, 5(2), 177-198.

Zahwani, S. T., & Nasution, M. I. P. (2024). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi Di Era Digital. Journal of Sharia Economics Scholar (JoSES), 2(2).