JIHAD: Jurnal Ilmu Hukum dan Administrasi
Vol. 8 No. 1 Maret 2026
p-ISSN : 2745-9489, e-ISSNl 2746-3842
DOI: *10.36312/jihad.v8i1.10350/https://ejournal.mandalanursa.org/index.php/JIHAD/issue/archive*

Cyber Legal Responsibility for Personal Data Leaks from the Perspective of Substantive Justice in Indonesia

Hariang Dede Taufik[1], Haerul Apandi[2], Rudolf Paskaries[3], Hariyanto Aritonang[4], Andi Haruman[5] Nugraha Pranadita[6]
Universitas Langlangbuana Bandung

Article Info

Article history:
Accepted: 15 February 2026
Publish: 1 March 2026

Keywords:
Personal Data Protection;
Cyber Legal Liability;
Digital Corporations.

Abstract

Digital transformation has increased the use of personal data as a strategic asset in various sectors, but it has also given rise to the risk of data leaks that cause material and immaterial losses to society. This study aims to analyse cyber legal liability for personal data leaks in Indonesia using a substantive justice perspective. The method used is descriptive qualitative through a literature study of regulations, legal doctrines, and data protection practices to obtain a comprehensive understanding of legal responsibility in the digital ecosystem. The results of the study show that cyber legal responsibility still faces challenges of cross-border jurisdiction, weak implementation of the responsibility of digital corporations as legal subjects, and suboptimal restoration of victims' rights. A damage-based jurisdiction approach is needed to reach global digital actors, while strengthening corporate accountability is key to preventing avoidance of responsibility. From a substantive justice perspective, the legal system needs to be oriented towards the effective restoration of victims' rights through compensation, ongoing protection, and system improvements. This study emphasises that strengthening an adaptive, accountable, and victim-oriented cyber legal framework is an important prerequisite for realising fair personal data protection and increasing public trust.

Corresponding Author:
Hariang Dede Taufik
Universitas Langlangbuana
Email Coresspondent: *hadetaufik8@gmail.com*

1. INTRODUCTION

Digital transformation has brought fundamental changes to various aspects of society, including the economy, government, and public services. The use of information and communication technology enables the rapid and massive collection, processing, and distribution of personal data. In this context, personal data is no longer just individual information, but has evolved into a strategic asset with high economic, social, and political value (Westin, 1967; Solove, 2006). The development of the digital economy and the online platform ecosystem further emphasises the position of data as a major commodity that requires adequate legal protection.

However, the increasing dependence on electronic systems is also accompanied by an increased risk of personal data leaks. Various cases of data leaks in Indonesia show that cyber security systems and data governance are not yet fully capable of guaranteeing the protection of people's privacy rights. Data leaks can cause material and immaterial losses,

including identity theft, digital fraud, security threats, and psychological harm to victims (Kshetri, 2014). This phenomenon emphasises that personal data protection is not only a technical issue, but also a matter of law and justice.

Normatively, personal data protection is part of the protection of human rights, particularly the right to privacy. The right to privacy has been recognised in various international instruments, such as

Normatively, personal data protection is part of the protection of human rights, particularly the right to privacy. The right to privacy has been recognised in various international instruments, such as the Universal Declaration of Human Rights (United Nations, 1948), as well as in modern legal principles that place individuals as the main subjects of legal protection (Warren & Brandeis, 1890). In the Indonesian context, the state's commitment to personal data protection is manifested through Law No. 27 of 2022 on Personal Data Protection, which regulates the rights of data subjects, the obligations of data controllers, and the mechanisms for sanctions against violations.

However, the existence of these regulations does not fully guarantee justice for victims of personal data leaks. Law enforcement that is oriented towards formal compliance with norms is often unable to provide fair and meaningful redress for victims. Satjipto Rahardjo (2009) emphasises that the law does not only function as a set of rules, but also as a means to bring about substantive justice for society. In the context of personal data leaks, substantive justice demands accountability that is not only administrative or criminal in nature, but also includes the comprehensive restoration of victims' rights.

The substantive justice approach is relevant because the impact of personal data leaks cannot always be measured quantitatively. Victims may experience insecurity, loss of trust in digital systems, and potential discrimination due to data misuse. Rawls (1971) asserts that justice must guarantee protection for vulnerable groups and ensure the fair distribution of benefits and burdens. Therefore, cyber legal accountability needs to be examined not only in terms of compliance with laws and regulations, but also in terms of the extent to which the law is able to provide fair and effective protection for victims.

Based on this description, this study aims to analyse cyber legal accountability for personal data leaks in Indonesia using a substantive justice perspective. This research is important to assess the effectiveness of the legal system in providing real protection for victims and to formulate a more equitable approach to cyber law enforcement. Thus, it is hoped that this research can contribute theoretically to the development of cyber law and practically to policymakers in strengthening personal data protection in Indonesia.

2. METHOD

This study utilises a descriptive method with a qualitative approach to gain an in-depth and contextual understanding of the phenomenon under investigation. This approach was chosen because it is able to accurately describe the objective conditions in the field without manipulation or intervention from the researcher (Moleong Lexy, 2017) that qualitative research is naturalistic and places the researcher as the main instrument in the data collection process. The data collected is not in the form of numbers, but rather textual information obtained through in-depth interviews, direct observation, documentation, and field notes (John W. Creswell, 2014). This approach allows researchers to capture meanings, perceptions, and social dynamics that cannot be explained quantitatively. This research does not aim to test hypotheses, but rather to explore and understand variables independently based on the actual context (Nazir, 2013). The descriptive method is used to describe phenomena systematically, factually, and accurately regarding the facts that occur in the field (Sugiyono, 2019), emphasising that this method is suitable for use in social research

that aims to understand behaviour, interactions, and social structures in depth. (Denzin NK, 2009) Qualitative research is an interpretive and naturalistic approach that aims to understand the meaning of a phenomenon in its natural context. Researchers attempt to interpret the world based on the perspective of the subjects being studied.

3. RESULTS AND DISCUSSION

1. Cyber Legal Accountability in Practice and the Perspective of Cyber Jurisdiction

Findings show that personal data leaks in Indonesia are still often understood as mere technical failures, rather than legal violations that give rise to institutional responsibility. In some cases, electronic system operators tend to shift responsibility to third parties, such as technology vendors, cloud service providers, or data processing partners. This practice obscures the chain of responsibility and makes it difficult for victims to seek redress. This phenomenon reflects the lack of a strong risk-based legal responsibility paradigm in electronic system governance.

The ambiguity of responsibility becomes even more complex when data is processed or stored outside Indonesia. The cross-border nature of cyberspace raises complex jurisdictional issues, particularly in determining applicable laws and law enforcement authorities. Svantesson (2017) asserts that cyber jurisdiction can no longer be based solely on the physical location of servers or company domicile, but must also consider the impact on data subjects. An effects-based jurisdiction approach provides legitimacy for countries to hold digital actors accountable for harming their citizens, even if the perpetrators are located in another jurisdiction.

However, practice in Indonesia shows that this approach has not been fully adopted in law enforcement. Victims of data breaches often face difficulties in holding global entities accountable due to limitations in cross-border legal mechanisms, differences in regulatory standards, and obstacles to proof. The gap between the development of international legal norms and national practice highlights the need to strengthen a cyber legal framework that is adaptive to the cross-border nature of the digital space. Without such strengthening, the protection of data subjects' rights has the potential to be ineffective, especially when violations involve global digital actors.

Thus, cyber legal accountability must shift from a territorial approach to an impact-based and cross-border responsibility approach. This approach not only strengthens legal protection but also creates certainty for the public that their privacy rights remain protected amid the complexity of the global digital ecosystem.

2. Accountability of Digital Corporations as Legal Entities

Findings show that in practice, responsibility for personal data breaches is often directed at individual system operators or technical staff, while corporations as data controllers are relatively rarely held comprehensively accountable. This approach reflects a tendency to personalise blame, even though data breaches are generally the result of systemic failures, such as weak security policies, insufficient investment in cyber infrastructure, and inadequate risk management.

The legal entity theory proposed by Hans Kelsen asserts that corporations are legal subjects with their own rights and obligations, regardless of the individuals who perform functions within them (Kelsen, 1967). In the context of personal data protection, corporations as data controllers have a legal obligation to ensure system security, apply the principle of prudence, and guarantee transparency in data management. Thus, responsibility for data leaks cannot be shifted to individuals alone, because strategic decisions regarding data security are made at the corporate policy level.

The complexity of digital corporate structures, including the use of outsourcing, cloud computing, and cross-border data processing, is often used as an excuse to obscure responsibility. However, legal literature emphasises that organisational complexity actually calls for stronger accountability mechanisms, not avoidance of responsibility. Corporations still have an obligation to ensure that all partners and third parties involved in data processing meet the same protection standards.

The gap between norms and practices shows that the recognition of corporations as legal subjects in the Personal Data Protection Act has not been fully and effectively implemented. Law enforcement still tends to focus on individual errors rather than the structural responsibilities of corporations. Therefore, a more systemic and assertive law enforcement approach is needed to ensure that responsibility is attached to corporate entities as data controllers. This approach is important to create a deterrent effect, improve data security standards, and provide more effective protection for the public.

3. Substantive Justice for Victims of Personal Data Leaks

Findings show that restoring victims' rights remains the weakest aspect of Indonesia's personal data protection system. Victims of data leaks are often unaware of the available complaint mechanisms, face complicated procedures, and do not receive compensation commensurate with the losses they have suffered. This situation indicates that the legal system is still oriented towards enforcing norms rather than actually restoring victims' rights.

The progressive legal approach proposed by Satjipto Rahardjo emphasises that the law must be people-oriented and capable of delivering real justice, not just normative certainty (Rahardjo, 2009). In the context of personal data leaks, substantive justice demands the effective restoration of victims' rights, including proportional compensation, protection from further abuse, and guarantees of system improvements to prevent recurrence of violations.

International literature shows that modern data protection regimes, such as the General Data Protection Regulation (GDPR) in the European Union, grant data subjects strong rights to obtain compensation and effective legal protection. This model places victims as the main subjects of legal protection, not merely objects of regulation. In contrast, practices in Indonesia show that administrative sanctions against violators are not always followed by mechanisms for restoring victims' rights, so that substantive justice has not been fully realised.

An overly formalistic legal approach has the potential to neglect the dimension of substantive justice. When the law focuses only on procedural compliance, victims remain in a weak position in relation to digital corporations that have greater resources and structural power. Therefore, the integration of progressive legal principles in the enforcement of personal data protection laws is important to ensure that the law functions as a corrective measure against such inequalities.

Thus, substantive justice must be the main orientation in cyber legal accountability. Personal data protection is not only about sanctions for perpetrators, but also about restoring the dignity, security, and trust of the community in digital systems. This approach will strengthen the legitimacy of the law while encouraging the creation of a more just and sustainable digital ecosystem.

4. CONCLUSION

Cyber legal accountability for personal data breaches in Indonesia shows that the legal protection system still faces various structural, normative, and implementational

challenges. First, in the context of cyber jurisdiction, the cross-border nature of the digital space makes it difficult to determine legal responsibility, especially when violations involve global actors. An impact-based approach, as outlined in cyber jurisdiction theory, is essential to ensure that data subjects' rights remain protected even when violations occur outside national legal jurisdictions.

Second, the recognition of digital corporations as legal subjects has not been fully and effectively implemented. Law enforcement practices still tend to personalise the blame on individual operators, even though data leaks are generally systemic failures that are the responsibility of corporations as data controllers. Strengthening corporate accountability is key to preventing the avoidance of responsibility and improving data protection standards.

Third, from the perspective of substantive justice, Indonesia's personal data protection legal system still does not fully provide fair and meaningful redress for victims. An overly formalistic legal approach puts victims in a weak position when it comes to claiming their rights. Therefore, the integration of progressive legal principles oriented towards restoring victims' rights is important in order to realise legal protection that is not only normative but also substantive.

Thus, cyber legal accountability for personal data breaches in Indonesia needs to be directed towards strengthening cross-border jurisdiction, digital corporate accountability, and the application of substantive justice in restoring victims' rights. This approach is expected to increase the effectiveness of legal protection while building public trust in the national digital ecosystem.

5. ACKNOWLEDGMENTS

The authors gratefully acknowledge the Master of Law Program, Universitas Langlangbuana, for its institutional and financial support, which made this research possible.

6. BIBLIOGRAPHY

Brandeis, L. D., & Warren, S. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications.

Denzin, N. K., & Lincoln, Y. S. (2009). *The Sage handbook of qualitative research* (3rd ed.). Sage Publications.

Kelsen, H. (1967). *Pure theory of law*. University of California Press.

Kshetri, N. (2014). *Cybercrime and cybersecurity in the global South*. Palgrave Macmillan.

Moleong, L. J. (2017). *Metodologi penelitian kualitatif*. PT Remaja Rosdakarya.

Nazir, M. (2013). *Metode penelitian*. Ghalia Indonesia.

Rahardjo, S. (2009). *Hukum progresif: Sebuah sintesa hukum Indonesia*. Genta Publishing.

Rawls, J. (1971). *A theory of justice*. Harvard University Press.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–560.

Sugiyono. (2019). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.

Svantesson, D. J. B. (2017). *Solving the internet jurisdiction puzzle*. Oxford University Press.

United Nations. (1948). *Universal declaration of human rights*. United Nations.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.