Corporate Torts in Personal Data Breaches in Indonesia

Hani Irhamdessetya[1], Sudijono Sastroatmodjo[2], Liwingstone Filemone Ade[3], Mansur Hidayat[4]
[1,2,3,4] Master of Laws, Universitas Ngudi Waluyo, Indonesia

E-mail Corresponding Author : haniirhamdessetya@unw.ac.id

Abstract

These days companies have to handle a lot of information about people. This also means that there is a risk of this information getting out and hurting people. This study looks at the laws in Indonesia that say companies are responsible when this happens. It also tries to find ways for companies to follow the rules and keep information safe. The study uses laws and court cases to understand the problem. It finds out that if a company is not careful with information it can be held responsible for any harm caused. The Personal Data Protection Law also says that companies must keep information safe. The study suggests that companies should have a plan to manage risks be careful and be open about what they do. This can help prevent information from getting out and build trust in Indonesia.

Keywords: Acts, Personal Data, Corporate Liability, Data Protecion, Corporate Compliance.

INTRODUCTION

Data breaches involving personal information in a corporate context raise complex legal issues. The harm suffered by data subjects is not limited to material losses but also includes non-material harm, a loss of security, the risk of identity theft, and a decline in public trust in corporate digital systems (Santos et al., 2025). In such circumstances, the legal question is not merely whether an administrative violation has occurred, but also whether the corporation's actions or omissions have met the elements of a tortious act that gives rise to a liability for damages. The Personal Data Protection Act (PDP Act) itself governs the rights of data subjects and the obligations of data controllers (Yuniarti, 2022), while in the financial services sector, the strengthening of consumer protection is also emphasized in Financial Services Authority Regulation (POJK) No. 22 of 2023.

From a regulatory perspective, this issue is significant because Indonesia's personal data protection regime is shifting from an administrative approach toward a more comprehensive compliance-based approach. The Ministry of Communication and Digital Affairs (Komdigi) has emphasized the importance of collaborative enforcement of the Personal Data Protection Act and has identified personal data protection as the foundation of public trust in the digital economy (Iman, 2024). On the other hand, there remains a need to strengthen corporate internal compliance so that data governance does not stop at mere policy formalities, but also effectively prevents legal harm to data subjects.

Previous studies have addressed aspects of personal data protection from the perspectives of administrative law and public policy. However, studies that specifically analyze the concept of corporate tort liability in the context of data breaches and formulate an operational model of corporate compliance remain limited (Talesh, 2018). This research gap forms the basis for the urgency of this study.

Given these circumstances, this study aims to: (1) analyze the legal framework for corporate liability for unlawful acts in cases of personal data breaches in Indonesia; and (2) formulate an ideal corporate compliance model to prevent personal data breaches in order to strengthen legal protection for data subjects.

The phenomenon of data breaches in Indonesia has reached an alarming level, with the frequency and scale of incidents continuing to rise as the public becomes increasingly reliant on the digital ecosystem (Abdillah et al., 2024). Data from various cybersecurity reports indicate that Indonesia is often an easy target for cyberattacks, ranging from technical attacks such as hacking to manipulative tactics like social engineering. However, what is often overlooked is the issue of corporate insider negligence or systematic failures in meeting security standards which should be the responsibility of data controllers.

Globally, personal data is now regarded as "the new oil" a resource of immense economic value yet it can also become "toxic waste" if not managed properly, given the potential legal liabilities it entails. This paradigm shift requires corporations to no longer view data protection merely as a technical obligation of the IT department, but rather as a strategic legal obligation. A corporation's inability to safeguard data privacy is not merely a managerial failure, but also constitutes a fundamental violation of privacy rights.

In the context of civil law in Indonesia, the main challenge in data breach cases is proving the element of fault in a tort, as provided for in Article 1365 of the Civil Code (Johnson, 2005). Conventional tort doctrine often struggles to address the complexities of intangible digital systems. Often, corporations hide behind the argument that data breaches occur due to third-party attacks (by hackers), which are considered force majeure. However, from the perspective of modern data protection law, the occurrence of a cyberattack does not automatically exempt a corporation from liability if it can be proven that the security standards implemented were inadequate or fell below the threshold of due diligence.

The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) brings a breath of fresh air by introducing the accountability principle. Unlike the previous legal framework, which tended to be administrative in nature, the PDP Law places a clearer burden of responsibility on data controllers. Section 39 of the Personal Data Protection Act, for example, establishes the data controller's obligation to safeguard personal data. A violation of this obligation automatically strengthens the argument of "unlawfulness" in a tort claim, as it constitutes a breach of a legal duty established by law (per se illegal) (Busnelli & Koziol, 2002).

However, another challenge arises regarding the calculation of damages. Damages resulting from data breaches are often non-pecuniary in nature, such as loss of privacy, psychological trauma, or risks that may only materialize in the future (such as the misuse of data for illegal online lending) (Paat & Markham, 2021). Indonesian civil law still has limitations in standardizing compensation for such non-pecuniary damages, so court rulings often fail to provide adequate compensation to victims. Therefore, a more progressive legal framework is needed to establish corporate liability not only based on fault but also to begin incorporating the principle of strict liability in high-risk activities such as large-scale data management.

In addition to the litigation aspect, the urgency of this research also lies in the development of a compliance model. Corporations in Indonesia currently need practical guidance on how to translate the abstract norms of the Personal Data Protection Act into operational standards. An ideal compliance model must integrate the principles of Privacy by Design and Privacy by Default. The goal is to ensure that data protection is no longer a reactive response following a breach, but rather an integral part of the organization's culture. In this way, public trust in the digital economy can be maintained, and corporations can mitigate legal risks that could threaten their future business continuity.

RESEARCH METHODOLOGY

This study employs a normative legal research methodology, which involves the examination of legislation, legal principles, and legal doctrines relevant to the research problem (Taekema, 2018). The approaches used include three approaches, namely: the statutory

approach, the conceptual approach, and the case approach.

The legal approach involves analyzing all regulations relevant to personal data protection and corporate liability, namely Law No. 27 of 2022 on Personal Data Protection, the Civil Code (KUHPerdata), specifically Articles 1365–1367, Law No. 8 of 1999 on Consumer Protection, as well as sector-specific regulations in the fields of financial services and information technology.

A conceptual approach was used to examine the concept of corporate torts and legal compliance theory in order to develop a comprehensive analytical framework. A case-based approach was employed by analyzing past cases of personal data breaches in Indonesia as empirical data for the analysis.

The legal materials used consist of primary legal sources, such as relevant laws and regulations and court decisions, as well as secondary legal sources, such as legal literature, academic journals, and research findings related to the topic of study. The legal materials were collected through library research and document analysis. The analysis of legal materials was conducted qualitatively using a prescriptive approach, which involves providing normative assessments and recommendations regarding the issues under examination.

RESULTS AND DISCUSSION

THE LEGAL FRAMEWORK FOR CORPORATE LIABILITY FOR TORT IN PERSONAL DATA BREACHES

Tort under civil law is governed by Article 1365 of the Civil Code. This article states that any tortious act causing harm to another person obligates the person whose fault caused such harm to compensate for the resulting damages. In a context liability for tort does not rest solely with the individual perpetrator but may also be imposed on the corporation as a legal entity if the act was committed within the scope of the corporation`s business activities.

There are five elements of tort that must be cumulatively satisfied. These elements are: the existence of an act whether active or passive unlawfulness, fault, damage and a causal relationship between the act and the damage. Personal data breaches can be considered as a form of tort. The element of fault may consist of a corporation`s negligence in implementating data security systems.

In cases of data breaches the element of wrongdoing may consist of a corporation`s negligence in implementating adequate data security systems. Such negligence may take the form of failing to implement data encryption failing to perform regular security system updates, lacking clear data access policies or failing to respond to security incidents promptly and appropriately.

Tort (onrechtmatige daad) under Indonesian civil law is governed by Article 1365 of the Civil Code, which states that any tortious act causing harm to another person obligates the person whose fault caused such harm to compensate for the resulting damages. In a corporate context, liability for tort does not rest solely with the individual perpetrator but may also be imposed on the corporation as a legal entity if the act was committed within the scope of the corporation’s business activities.

There are five elements of tort that must be cumulatively satisfied, namely: (1) the existence of an act, whether active or passive; (2) unlawfulness, meaning a violation of another person’s rights, the perpetrator’s legal obligations, public orality, or social norms; (3) fault, in the form of intent (dolus) or negligence (culpa); (4) damage, whether material or immaterial; and (5) a causal relationship between the act and the damage (Subekti, 2003).

In cases of personal data breaches, the element of fault may consist of a corporation’s negligence in implementing adequate data security systems. Such negligence may take the form of: failing to implement standard data encryption, failing to perform regular security system updates, lacking clear data access policies, or failing to respond to security incidents promptly

and appropriately. All forms of negligence constitute acts that can be considered as grounds for tort liability.

In cases of personal data breaches, the element of wrongdoing may consist of a corporation's negligence in implementing adequate data security systems (Schwartz & Janger, 2006). Such negligence may take the form of: failing to implement standard data encryption, failing to perform regular security system updates, lacking clear data access policies, or failing to respond to security incidents promptly and appropriately. All forms of negligence constitute acts that may be considered as the basis for a tort.

An unlawful act under the Personal Data Protection Act can be identified as a violation of the mandatory obligations set forth in the Act. Article 35 of the PDP Act requires personal data controllers to ensure the security and confidentiality of personal data, while Article 46 requires data controllers to notify data subjects and the Ministry responsible for government affairs in the field of communications and information technology of any data breaches. Failure to fulfill these obligations automatically constitutes a violation of the law.

Corporate liability for data breaches generally stems from negligence, not intentional misconduct. Corporate negligence can be demonstrated by showing that due diligence standards which should have been applied but were ignored were not met. These standards include the implementation of adequate technical safeguards, organizational measures, and physical security in accordance with the principles of "privacy by design" and "privacy by default," as mandated by the Personal Data Protection Act (Jasmontaite et al., 2018).

The harm suffered by data subjects as a result of personal data breaches is complex and multifaceted. Material damages may include financial losses resulting from identity theft, while non-material damages encompass loss of privacy, a sense of insecurity, psychological distress, and potential discrimination. Case law in various countries indicates a trend among courts to recognize non-material damages in data breach cases as compensable losses.

The causal link between a corporation's negligence and the data subject's losses can be established by applying the conditio sine qua non theory (but-for test), namely that if the corporation had implemented adequate security measures, the data breach would not have occurred and the data subject would not have suffered losses. In litigation practice, proving this causality is often a critical issue that requires the support of digital forensic evidence.

Thus, the legal framework for corporate liability for personal data breaches from the perspective of tort law cannot be limited solely to Article 1365 of the Civil Code, but must be interpreted systematically in conjunction with the legal regime governing personal data protection and the operation of electronic systems. Law No. 27 of 2022 on Personal Data Protection designates personal data controllers as legal entities that bear an active obligation to protect and ensure the security of the personal data they process, while Government Regulation No. 71 of 2019 stipulates that every Electronic System Operator is required to operate electronic systems in a reliable and secure manner and to be accountable for the operation of such systems. In other words, when a corporation fails to establish adequate data security governance, that failure is not merely a technical shortcoming but has evolved into a breach of legal obligations that can form the basis for a tort claim.

Within this framework, corporate liability can be understood in two distinct categories. First, direct corporate liability, which occurs when losses result from policies, governance failures, or systemic failures within the legal entity's control such as the absence of cybersecurity standard operating procedures, weak internal oversight, or the neglect of periodic security audits. Second, liability for the acts of a corporate body or employee, provided that such acts or omissions were committed within the scope of their duties, authority, or in the interest of the corporation. In this context, a data breach does not necessarily have to be proven as an intentional act by the board of directors; it is sufficient to demonstrate that the corporation, as the data controller, failed to fulfill its objective legal obligations to prevent, detect, and

appropriately address the incident. This framework is important because, in modern digital business practices, data breaches typically arise not from a single individual action, but from systemic failures within corporations to apply the principle of technological due diligence.

From an evidentiary perspective, indicators of corporate negligence can be derived from several normative parameters. Article 35 of the Personal Data Protection Act requires data controllers to protect and ensure the security of the personal data they process, while Article 46 establishes a notification obligation in the event of a personal data breach (Protection, 2018). Furthermore, the Personal Data Protection Act also grants data subjects the right to sue and receive compensation for violations of the processing of their personal data. This indicates that the legislature does not view data protection merely as an administrative obligation, but also as the basis for civil remedies. Thus, if a corporation fails to fulfill its protection and notification obligations, the data subject's position to file a claim for damages becomes stronger, whether based on the specific regime of the Personal Data Protection Act or on the general grounds of tort under the Civil Code.

From a doctrinal perspective, this demonstrates that the Personal Data Protection Act serves as a lex specialis that clarifies the standards of corporate liability, while Article 1365 of the Civil Code remains the lex generalis that provides the basis for civil claims when such violations result in damages (Van Dunné, 1999). With this approach, judges do not need to make a rigid distinction between regulatory violations and unlawful acts, since a violation of statutory obligations can itself constitute a concrete manifestation of the element of "unlawfulness." Thus, the clearer the violation of the normative obligations under the Personal Data Protection Act and Government Regulation No. 71 of 2019, the stronger the argument that the element of an unlawful act has been satisfied.

Furthermore, personal data breaches also underscore a shift in the paradigm of corporate liability from a fault-based approach focused solely on individual errors to a compliance-based model that assesses the presence or absence of institutional compliance. In the digital economy, the extent of a corporation's liability cannot be determined solely by malicious intent, but rather by whether the corporation has established adequate compliance systems to protect personal data. Therefore, evidence such as audit trails, penetration tests, incident response plans, access classifications, encryption, employee training, and risk management documentation is relevant for assessing the presence or absence of corporate liability. The absence of these measures can be interpreted as a form of structural negligence.

In terms of remedies, corporate liability for personal data breaches should not be limited to the payment of individual compensation. More progressive remedies may include the restoration of security systems, transparent notification requirements, the temporary suspension of certain data processing activities, independent audits, and orders to improve data protection governance. This aligns with the nature of data breaches, which are not merely private in nature but also have a public dimension, as they affect public trust in the digital ecosystem. The PDP Act itself has established a framework for administrative sanctions for violations of various data controller obligations, including security obligations and the obligation to report data breaches. Therefore, corporate liability should ideally be understood as a multi-tiered system: civil damages, administrative sanctions, and, under certain circumstances, criminal penalties, depending on the nature and severity of the violation.

Ultimately, the findings of this discussion indicate that personal data breaches in corporate activities can no longer be viewed as mere technical incidents, but rather as a failure on the part of corporations to meet the legal standards for data protection mandated by law. Corporations that collect, store, and utilize personal data derive economic benefits from data processing; consequently, they must also bear the corresponding legal responsibility to ensure the security of that data. From this perspective, the legal framework for personal data breaches serves as a crucial tool for ensuring that digital transformation does not come at the expense of

data subjects' civil rights, and that corporate compliance with data protection regulations is a legal obligation, not merely an ethical choice or a business policy.

CORPORATE COMPLIANCE MODELS IN PERSONAL DATA PROTECTION

Corporate compliance in the context of personal data protection cannot be viewed merely as the fulfillment of regulatory formalities. True compliance requires an organizational culture that treats data protection as a core value, supported by effective governance systems and measurable accountability mechanisms. This approach aligns with the principle of accountability, which is one of the main pillars of the European Union's General Data Protection Regulation (GDPR) and has been incorporated into Indonesia's Personal Data Protection Law.

The ideal corporate compliance model in the context of personal data protection in Indonesia can be outlined in five key pillars. First, the Due Diligence and Risk Assessment pillar. Corporations are required to conduct data protection impact assessments (DPIAs) on a regular basis, particularly before commencing large-scale data processing or the processing of sensitive data(Georgiou & Lambrinoudakis, 2021). A DPIA enables corporations to identify potential risks and take appropriate mitigation measures before any losses occur.

Second, the pillar of Internal Data Governance. Corporations need to establish a clear data governance structure, including the appointment of a Data Protection Officer (DPO) as required by certain provisions of the Personal Data Protection Act, the development of internal data protection policies, standard operating procedures for data processing, and mechanisms for employee training and awareness. Good governance ensures that every level of the organization understands and complies with data protection obligations.

Third, the Technical and Organizational Security pillar. Corporations are required to implement technical security measures in accordance with industry standards, including data encryption, role-based access control, real-time system monitoring, periodic security testing (penetration testing), and a disaster recovery plan.

Organizational security measures include device usage policies, third-party vendor management, and data management throughout the data lifecycle.

Fourth, the Incident Management and Notification pillar. Corporations need to have robust incident response procedures in place, covering early detection, investigation, impact mitigation, and recovery. In the event of a data breach, corporations are required to fulfill their notification obligations as stipulated in Article 46 of the Personal Data Protection Act, namely by notifying data subjects and the competent authorities within the specified timeframe. The speed and transparency of the incident response are key factors in assessing corporate accountability.

Fifth, the pillar of Accountability and Continuous Monitoring. Compliance is not a one-time activity, but rather an ongoing process that requires continuous monitoring, evaluation, and adjustment. Corporations need to conduct periodic data protection audits, update policies in line with regulatory developments and evolving cyber threats, and establish internal reporting mechanisms that enable the early identification of issues.

This compliance model serves not only as a tool for mitigating legal risks but also as an instrument for building public trust. In an increasingly competitive digital ecosystem, a corporation's reputation for managing consumer personal data has become a significant differentiator. Corporations that can demonstrate a genuine commitment to data protection will gain a long-term competitive advantage while minimizing their exposure to litigation risks.

Based on these five pillars, the corporate compliance model for personal data protection should essentially be understood as a risk-based compliance model, rather than merely administrative compliance. This is in line with Law No. 27 of 2022 on Personal Data Protection, which not only establishes prohibitions but also imposes active obligations on

Personal Data Controllers to process data in a responsible and verifiable manner and to ensure data security against unauthorized access or disclosure. The Personal Data Protection Act explicitly affirms the principle that data processing must be conducted responsibly and in a manner that can be clearly demonstrated, while Personal Data Controllers are required to be accountable for the processing of personal data and to demonstrate accountability in complying with data protection principles. Therefore, corporate compliance must be established in the form of evidence-based compliance that is, compliance that can be demonstrated through documents, procedures, audits, and the organization's track record of actions.

In this context, due diligence and risk assessment serve as a critical starting point. Article 34 of the Personal Data Protection Act requires Personal Data Controllers to conduct a personal data protection impact assessment if the processing poses a high risk to data subjects, including in cases of specific data processing, large-scale processing, the use of new technologies, or processing that results in legal consequences or significant impacts. In other words, a DPIA is not merely a voluntary managerial tool, but a concrete manifestation of the legal duty of care. From the perspective of the discussion's findings, the existence of a DPIA is important not only for preventing incidents, but also for demonstrating that the corporation has identified risks from the outset, assessed potential impacts, and prepared proportionate mitigation measures. In the context of a dispute, this risk assessment document can serve as crucial evidence for determining whether the corporation acted with due care or was negligent.

Furthermore, the pillar of internal data governance demonstrates that corporate compliance requires the institutionalization of data protection functions within the organizational structure. The Personal Data Protection Act stipulates that Personal Data Controllers and Personal Data Processors are required to appoint an officer or official to carry out personal data protection functions under certain circumstances, including when processing is conducted for public services, requires regular and systematic monitoring on a large scale, or involves the processing of specific data and data related to criminal offenses on a large scale. These officials or staff members are also tasked with providing information and advice on compliance, monitoring compliance with laws and internal policies, advising on impact assessments, and serving as a point of contact for data processing issues. Thus, the role of the DPO or data protection officer should not be viewed merely as a symbolic position, but rather as a key internal accountability mechanism that ensures company policies are effectively implemented down to the operational level.

In terms of technical and organizational security, the ideal compliance model must also be interpreted in conjunction with the obligations of electronic system operators under Government Regulation No. 71 of 2019. This regulation stipulates that every electronic system operator must operate electronic systems in a reliable and secure manner and be accountable for the operation of such systems. Meanwhile, the Personal Data Protection Act requires data controllers to protect and ensure the security of personal data through technical and operational measures, maintain data confidentiality, supervise all parties involved in processing, protect data from unauthorized processing, and prevent unauthorized access by using reliable, secure, and responsible electronic systems. It is clear from this that compliance is not sufficient merely through written policies; rather, it must be implemented through concrete controls such as encryption, access restrictions, logging of processing activities, vendor management, infrastructure security, and oversight of the data processing chain from end to end (Enjam, 2021).

The pillars of incident management and notification also play a crucial role in the corporate compliance model. Article 46 of the Personal Data Protection Act requires Personal Data Controllers to provide written notification within 72 hours to data subjects and relevant authorities in the event of a personal data breach (Protection, 2018). Such notification must, at a minimum, include the personal data that was exposed, when and how the incident occurred,

as well as the mitigation and recovery efforts undertaken. This standard indicates that Indonesian law requires not only prevention but also a swift, transparent, and accountable response once an incident occurs. Therefore, it can be analytically asserted that the quality of corporate compliance is often tested in the post-breach phase: whether the company has an incident response plan, internal escalation channels, forensic documentation, crisis communication mechanisms, and concrete recovery measures for data subjects. Corporations that are slow to act, cover things up, or fail to provide adequate information may be deemed to have failed to meet substantive compliance standards.

Furthermore, the pillars of accountability and ongoing monitoring demonstrate that compliance in data protection is dynamic, not static.

The Personal Data Protection Act requires Personal Data Controllers to maintain records of all personal data processing activities, and the principles of processing also require that such processing be conducted accurately, up-to-date, responsibly, and in a manner that can be clearly demonstrated. Consequently, companies must not only establish policies at the outset of data collection, but also regularly update their risk maps, evaluate the effectiveness of controls, conduct internal audits, and adapt security standards to evolving cyber threats. In other words, a good corporate compliance model is one that incorporates mechanisms for continuous monitoring and continuous improvement, ensuring that data protection becomes an institutional process that constantly adapts to changes in technology, business models, and legal risks.

Based on this discussion, it can be concluded that an ideal corporate compliance model for personal data protection has at least three key characteristics. First, preventive that is, preventing violations through risk assessment, governance, and system security from the outset. Second, responsive that is, the ability to detect, address, and recover from incidents quickly and transparently. Third, demonstrative meaning that the entire compliance process can be objectively demonstrated and verified. This demonstrative aspect is important because, in data breach disputes, what is assessed is not merely whether a corporation ever established a policy, but whether that policy was actually implemented, monitored, and documented. This is where the principle of accountability finds its practical significance under Indonesia's Personal Data Protection Act. Corporations that build substantive compliance will reap two benefits at once: protection against legal risks and increased public trust. Conversely, corporations that treat data protection merely as an administrative formality open themselves up to civil liability, administrative sanctions, reputational damage, and, in certain circumstances, criminal implications. Thus, the ideal compliance model is not merely one that adheres to the letter of the law, but one that is capable of embedding data protection as part of the organization's legal culture.

CONCLUSION

Based on the results of the analysis conducted, this study concludes two main points. First, a personal data breach caused by a corporation's negligence in implementing data security systems may be construed as a tort under Article 1365 of the Civil Code if it satisfies all five elements: an act, unlawfulness, fault, damage, and causation. Law No. 27 of 2022 on Personal Data Protection reinforces this framework of liability by establishing mandatory obligations for data controllers, the failure to comply with which automatically constitutes a violation of the law.

Second, the ideal corporate compliance model for preventing personal data breaches is built on five pillars: due diligence and risk assessment, internal data governance, technical and organizational security, incident management and notification, and accountability and continuous monitoring. This model serves not only as a mechanism for mitigating legal risks but also as the foundation for building public trust in Indonesia's digital ecosystem.

This study recommends that: (1) corporations operating in Indonesia immediately align

their data governance systems with the provisions of the Personal Data Protection Act and establish comprehensive data compliance programs; (2) the government, through the data protection authority to be established, should issue practical technical compliance guidelines for corporations of all sizes; and (3) further research is needed to analyze the development of case law on personal data protection in data breach cases following the full implementation of the Personal Data Protection Act.

BIBLIOGRAPHY

Abdillah, A., Widianingsih, I., Buchari, R. A., & Nurasa, H. (2024). Big data security & individual (psychological) resilience: A review of social media risks and lessons learned from Indonesia. *Array*, *21*, 100336.

Busnelli, F. D., & Koziol, H. (2002). *Unification of tort law: wrongfulness*.

Enjam, G. R. (2021). Data Privacy & Encryption Practices in Cloud-Based Guidewire Deployments. *International Journal of AI, BigData, Computational and Management Studies*, *2*(3), 64–73.

Georgiou, D., & Lambrinoudakis, C. (2021). Data protection impact assessment (DPIA) for cloud-based health organizations. *Future Internet*, *13*(3), 66.

Iman, N. (2024). The fight for our personal data: analyzing the economics of data and privacy on digital platforms. *International Journal of Law and Management*, *66*(6), 774–791.

Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., & Leucci, S. (2018). Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *Eur. Data Prot. L. Rev.*, *4*, 168.

Johnson, V. R. (2005). Cybersecurity, Identity Theft, and the Limits of Tort Liability. *ScL REv.*, *57*, 255.

Paat, Y.-F., & Markham, C. (2021). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health*, *19*(1), 18–40.

Protection, D. (2018). General data protection regulation. *Intersoft Consulting, Accessed in October*, *24*(1).

Santos, C., Morozovaite, V., & De Conca, S. (2025). No harm no foul: how harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. *Information & Communications Technology Law*, *34*(3), 329–375.

Schwartz, P. M., & Janger, E. J. (2006). Notification of data security breaches. *Mich. L. Rev.*, *105*, 913.

Taekema, S. (2018). Theoretical and normative frameworks for legal research: Putting theory into practice. *Law and Method*, *2018*.

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry*, *43*(2), 417–440.

Van Dunné, J. M. (1999). Liability for Pure Economic Loss: Rule or Exception? A Comparatist's View of the Civil Law-Common Law Split on Compensation of Non-physical Damage in Tort Law. *European Review of Private Law*, *7*(4).

Yuniarti, S. (2022). Protection Of Indonesia's Personal Data After Ratification Of Personal Data Protection Act. *Progressive Law Review*, *4*(02), 54–68.