Reconstruction of the Legal Mechanism for Consumer Rights Recovery Regarding Personal Data Leaks in the Financial Technology and E-Commerce Sectors in Indonesia

Yusuf Fahrizal Mujisulistyo, Didit Darmawan, Febrian Dirgantara

Universitas Sunan Giri Surabaya, Indonesia

ARTICLE INFO

Article history:
Received 24 November 2023
Revised 17 December 2023
Accepted 26 December 2023

Keywords:
Personal data protection,
Data breaches,
Fintech,
E-commerce,
Corporate liability,
Remedies,
Statutory damages.

ABSTRACT

The rapid growth of the financial technology (fintech) and e-commerce sectors in Indonesia has increased the risk of massive personal data breaches, placing consumers in a vulnerable position. This normative legal study aims to analyses two fundamental aspects. First, it examines how the current legal framework, centered on Law No. 27 of 2022 on Personal Data Protection (PDP Law), regulates corporate legal liability for failure to protect customer data. Second, it formulates an ideal legal mechanism model to ensure effective and efficient restoration of rights for consumers who have been victimized. Using a statute approach and a conceptual approach, this study finds that although Indonesia already has a strong foundation for corporate accountability, including administrative, civil, and criminal sanctions, there is a significant legal gap between the enforcement of corporate accountability and the realization of the restoration of victims' rights. The current litigation procedures have proven to be inefficient, costly, and burdensome for victims, who are required to prove losses that are difficult to quantify. As a solution, this study recommends reconstructing the rights restoration mechanism through four integrated pillars: (1) the introduction of statutory damages to provide legal certainty; (2) the establishment of a sectoral compensation fund as a financial safety net; (3) granting adjudication authority to the Data Protection Authority for rapid dispute resolution; and (4) modernizing class action procedures facilitated digitally. This model is proposed to create a legal ecosystem that not only punishes perpetrators, but also effectively restores the rights of victims and builds public trust in the digital economy.

INTRODUCTION

Digital transformation has driven a fundamental shift in the global economic structure, with Indonesia becoming one of the main arenas for the massive expansion of financial technology (fintech) and electronic commerce (e-commerce) companies. This expansion, as examined in the study by Aziz et al. (2023), requires effective personal data protection regulations to ensure the sustainability and credibility of the fintech sector amid rapid digital dynamics. The exponential growth of these two sectors is driven by widespread internet penetration, increased mobile device usage, and changes in consumer behavior that increasingly rely on digital platforms for financial and commercial transactions. These companies collect, process, and store unprecedented volumes of customer personal data, ranging from basic identity information, demographic data, transaction history, to behavioral preferences. This data has become a strategic asset that enables service personalization, market analysis, and innovative product development, which ultimately form the backbone of business models in the digital economy era (Ali & Darmawan, 2023). Operational dependence on data makes information security a key pillar of business continuity and consumer trust (Halim, 2022).

The accumulation of personal data in centralized repositories creates a highly valuable target for cybercriminals. Data breaches have become an inherent risk that overshadows rapid technological advances. Increasingly sophisticated cyber-attacks, vulnerabilities in information technology infrastructure, and human negligence are the main

* *Corresponding author, email address:* ***dr.diditdarmawan@gmail.com***

factors contributing to the increasing frequency and scale of data security incidents. When sensitive customer data, such as credit card numbers, addresses, and other personal information, falls into the wrong hands, the impact can be devastating. The losses are not only financial, but also include identity theft, fraud, and profound privacy violations (Adawiyah et al., 2022). Therefore, a strong data protection framework is no longer just a matter of regulatory compliance, but a fundamental prerequisite for maintaining the stability of the digital ecosystem and protecting the basic rights of individuals as citizens and consumers.

In Indonesia, the discourse on personal data protection has developed in line with increasing public and government awareness of existing vulnerabilities. Prior to the enactment of the Personal Data Protection Law (PDP Law), the existing legal framework was scattered across various sectoral regulations, such as regulations in the fields of telecommunications, banking, and electronic information and transactions. This regulatory fragmentation often led to legal uncertainty and overlapping authorities, hindering effective law enforcement. The PDP Law is expected to serve as a comprehensive legal umbrella, providing clear standards for data controllers and processors, and strengthening the rights of data subjects. However, the existence of a law alone does not necessarily solve all problems; implementation and law enforcement are key to its effectiveness in providing real protection.

The issue of customer data protection in fintech and e-commerce companies is becoming increasingly complex due to the cross-jurisdictional nature of the business and the speed of technological innovation, which often outpaces regulatory adaptation. Studies by Baraja et al. (2023) and Darmawan et al. (2023) on the implementation and supervision of personal data protection laws on online platforms emphasize that the effectiveness of regulations is highly dependent on sustainable implementation and supervision mechanisms, which pose a challenge in the face of rapid innovation. The importance of strengthening a responsive legal framework and effective oversight mechanisms is also a key finding in the research by Faridi et al. (2023), which identifies that the protection of vulnerable parties in the digital ecosystem is highly dependent on adaptive regulations and consistent enforcement. Corporate legal responsibility in preventing and handling data breaches is a central point in legal debates. This includes the obligation to implement reliable security systems, transparent data breach notification procedures, and mechanisms for compensating affected customers. A normative legal analysis of the existing regulatory framework is necessary to clearly map out how positive law in Indonesia regulates aspects of corporate responsibility and the extent to which these regulations are able to respond to the challenges posed by the current dynamics of the digital industry. This review serves as a basis for identifying the strengths and weaknesses of the applicable legal system.

One of the crucial issues that has emerged is the limitation and form of legal liability that can be imposed on fintech and e-commerce companies when data breaches occur. Although legislation has regulated the obligations of electronic system operators to maintain data security, its implementation in the field still faces various obstacles. Obstacles in defining and enforcing legal liability for personal data breaches were also identified in a study by Putra and Lie (2023), which showed that the absence of clear technical standards and information asymmetry between data controllers and data subjects are fundamental sources of legal uncertainty. There is often debate as to whether a failure to protect data is due to corporate negligence or purely the result of sophisticated cyber-attacks that are beyond reasonable control (force majeure). Proving negligence is a particular challenge for aggrieved customers, given the significant information asymmetry between consumers and corporations regarding the internal security systems in place. Without clear and independently auditable technical security standards, determining legal liability becomes unclear and potentially detrimental to the position of consumers.

The next issue relates to the effectiveness of compensation and remedy mechanisms for customers who are victims of data breaches. Civil litigation processes to seek compensation are often time-consuming, costly, and do not necessarily provide satisfactory results for victims. Class actions, which should be an effective instrument, still face challenges in practice in Indonesia. Consumer vulnerability in facing complex systemic risks is also reflected in the findings of Mardikaningsih and Darmawan (2023), who identify the importance of literacy and risk understanding in forming effective protection mechanisms. On the other hand, administrative sanctions stipulated in regulations are often considered insufficient to deter large corporations. The fines imposed may not be commensurate with the economic benefits gained from data exploitation or the massive losses suffered

by thousands or even millions of customers. As a result, companies may view these sanctions merely as a "cost of doing business" rather than a strong incentive to invest seriously in data security systems.

Uncertainty also arises in the aspect of cross-jurisdictional law enforcement, especially when customer data is stored or processed outside Indonesian jurisdiction. Many fintech and e-commerce companies operate as multinational entities that utilize global data center infrastructure. These global law enforcement challenges, as examined by Gardi and Eddine (2023), underscore the urgency of international collaboration on cybersecurity and personal data protection to address regulatory gaps between jurisdictions and build an effective enforcement framework. When data leaks occur from servers located overseas, questions regarding legal jurisdiction, applicable law (choice of law), and how Indonesian court decisions can be enforced become highly relevant (Poernomo, 2023). The harmonization of data protection regulations at the international level is still an ongoing process, and the absence of a solid legal cooperation framework between countries can hamper efforts to effectively enforce the law and protect customer rights. This issue requires an in-depth analysis of how Indonesian law responds to the transnational dimensions of digital data flows.

An analysis of the legal aspects of data protection in the fintech and e-commerce sectors is highly relevant today. The level of public dependence on digital services has reached a critical point, where financial transactions, commercial activities, and various aspects of daily life are now mediated by these platforms. The importance of legal certainty and institutional protection in fostering trust in the digital ecosystem is also the focus of a study by Negara and Darmawan (2023), which emphasizes the need for a responsive regulatory framework and strong institutions to ensure the sustainability of digital economic interactions. Public trust is the main foundation for the sustainability of the digital economic ecosystem. Any data breach incident that is not handled with a clear and fair legal framework has the potential to significantly erode that trust, which in turn can hamper national digital economic growth and reduce global competitiveness. Therefore, ensuring legal certainty that protects the basic rights of consumers is a prerequisite for maintaining stability and healthy growth.

Furthermore, the enactment of the Personal Data Protection Law (PDP Law) in Indonesia marks a new era in personal data governance. However, the existence of a new law is always followed by a crucial transition period, during which its interpretation, implementation, and enforcement are tested in practice. An in-depth legal analysis of the substance of the PDP Law and its implementing regulations, particularly in their application to dynamic fintech and e-commerce business models, is therefore essential. This study can provide constructive input for stakeholders, including regulators, business actors, and the public, on how these new legal norms should be operationalized so that their purpose of protecting data subjects can be achieved effectively without hindering innovation.

This study aims to systematically and critically analyses the legal liability of fintech and e-commerce companies in relation to customer data breaches based on Indonesian laws and regulations, including the Personal Data Protection Law. In addition, this study seeks to formulate an ideal legal mechanism model to provide more effective protection and ensure adequate redress for aggrieved customers. Theoretically, this research is expected to contribute to the development of cyber law and business law in Indonesia. Practically, the results are expected to provide input for regulators in drafting derivative technical regulations, as well as serve as a guide for industry players in building a reliable compliance system.

RESEARCH METHOD

This study uses a normative juridical approach, which is part of qualitative legal research methods. This approach focuses its analysis on norms, principles, doctrines, and applicable laws and regulations as primary legal materials. This study does not collect field data but instead conducts comprehensive library research to answer the research questions that have been formulated. The main data sources consist of primary legal materials, namely all regulations relevant to personal data protection, financial technology, and electronic commerce in Indonesia, such as the 1945 Constitution of the Republic of Indonesia, the Civil Code, Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and most importantly, Law No. 27 of 2022 concerning Personal Data Protection. Secondary legal materials include academic books, reputable national and international scientific journals, dissertations, and published opinions of legal experts. Tertiary legal materials such as legal dictionaries and encyclopedias are used as

supporting materials to explain technical terms.

The process of collecting legal materials is carried out through a systematic search strategy on digital legal databases such as the National Legal Documentation and Information Network (JDIH), as well as academic journal portals such as Google Scholar, Garuda, and SINTA. The inclusion criteria established for secondary legal materials are publication within the last 20 years, direct relevance to the topic of corporate accountability and consumer protection in the digital age, and authorship by credible academics or legal practitioners. Conversely, the exclusion criteria included opinion articles in the mass media, non-academic blog posts, and sources whose authors and publishers could not be verified. All collected sources were then inventoried and sorted based on their relevance to the two main sub-topics that had been formulated to ensure a focused and in-depth analysis (Marzuki, 2017).

Data analysis in this study was conducted using thematic synthesis techniques, in which all relevant legal materials were read, reviewed, and interpreted to identify patterns of regulation, key norms, and legal conflicts or gaps. This process involved the systematic coding of legal texts to extract core concepts related to obligations, prohibitions, sanctions, and mechanisms for the restoration of rights. Findings from various sources were then synthesized logically and argumentatively to build a comprehensive understanding in answering each problem formulation. To ensure the quality and validity of the analysis, source triangulation is carried out by comparing the interpretation of a legal norm in legislation with its discussion in doctrine (textbooks) and jurisprudence (if any), in order to ensure that the resulting interpretation is comprehensive and scientifically accountable (Creswell & Creswell, 2018).

RESULT AND DISCUSSION

Legal Analysis of the Legal Liability of Fintech and E-commerce Corporations in Customer Data Protection

The legal liability of fintech and e-commerce companies for failing to protect customer data in Indonesia has entered a new and more definitive phase with the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). This regulatory development marks a significant shift from fragmented and sectoral obligations toward a comprehensive and rights-based data protection regime (Budhijanto, 2022; Rosadi, 2022). The dynamics of strengthening consumer protection in the era of digital transformation, including the urgency to revise legal frameworks in order to keep pace with rapid technological developments, are also emphasized by Agustiawan et al. (2022), who argue that outdated consumer protection norms are inadequate to address systemic risks in e-commerce ecosystems. Furthermore, empirical findings by Umar et al. (2021) regarding the effectiveness of administrative sanctions in resolving consumer disputes in the digital marketplace reinforce the argument that a clear, enforceable, and proportional legal accountability framework is essential for fostering trust and fairness in the digital economy.

Prior to the enactment of the PDP Law, corporate legal obligations to safeguard personal data were dispersed across multiple regulations, primarily the Electronic Information and Transaction Law (EIT Law) and its implementing regulations, which focused largely on the technical integrity and reliability of electronic systems rather than on the substantive rights of data subjects (Hidayat & Nugroho, 2020; Rosadi, 2020). As a result, the previous legal framework lacked a coherent accountability model capable of addressing complex data breach scenarios and corporate negligence. The PDP Law now functions as a lex specialist that fundamentally reconstructs the legal landscape by establishing significantly higher standards of responsibility, incorporating internationally recognized data protection principles such as lawfulness, purpose limitation, proportionality, and accountability, and introducing more stringent administrative and criminal sanctions for non-compliant entities (Budhijanto, 2022; Sutanto, 2021). This transformation effectively shifts the regulatory paradigm from narrowly defined technical compliance toward a structured legal accountability regime that prioritizes the protection of data subjects' rights within Indonesia's rapidly expanding digital economy.

The PDP Law precisely defines the status and obligations of controllers and processors of personal data. The application of administrative fines calculated as a percentage of a corporation's annual revenue introduces a real economic disincentive. This new legal framework demands proactive compliance from corporations, rather than merely reactive responses after incidents occur. This legislation explicitly grants new rights to data subjects that can be legally enforced. Thus, the PDP Law creates legal certainty that was previously absent in data protection disputes. The principle of accountability that it promotes forces companies to be able to prove every step of data processing they undertake. Failure to protect data is now definitively

classified as a legal violation with measurable legal consequences (Yuniarti, 2022).

The legal accountability of fintech and e-commerce companies does not stem from a single regulation, but rather from a hierarchy and interconnection of various complementary legal instruments. Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) serves as the main legal umbrella, explicitly positioning itself as the cornerstone of personal data governance in Indonesia. This regulation adopts globally recognized principles, such as lawfulness, fairness, and transparency. For fintech and e-commerce companies, the PDP Law establishes their status as Personal Data Controllers, namely parties that determine the purpose and control the processing of data. This status carries a series of strict legal obligations.

Data Controllers have an obligation to ensure the security of personal data processing through the implementation of adequate technical and organizational measures as stipulated in Articles 35 to 39. These measures include the prevention of unlawful processing, illegal access, and the risk of data loss or damage, so that all security standards must be verifiable and accountable in accordance with the principle of accountability. In the event of a data protection breach, Article 46 requires the Data Controller to provide written notification to the data subject and the supervisory authority no later than three times twenty-four hours after the incident is discovered, and failure to fulfil this obligation is considered a separate legal violation. The principle of accountability also emphasizes that every company is not only obliged to comply with data protection provisions, but must also be able to demonstrate proof of compliance through comprehensive recording of all data processing activities, because the burden of proof regarding the adequacy of security systems lies with the company, as emphasized by Rosadi (2019).

The ITE Law and PSTE Government Regulation had already established the foundation of responsibility for Electronic System Operators prior to the enactment of the PDP Law. Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 requires every operator, including fintech and e-commerce, to operate electronic systems reliably, securely, and responsibly as stipulated in Article 15. Compliance with these technical and security standards requires adequate analytical capacity, which is in line with the findings of Khairi & Darmawan (2022) regarding the importance of data analysis capabilities for effective decision-making in managing compliance risks. This regulation is reinforced by Government Regulation No. 71 of 2019, which provides details on the obligations to implement risk management and adequate security standards. Although general in nature, both regulations remain highly relevant as they set prudential standards that serve as a reference in assessing negligence in civil disputes.

In the digital finance sector, the Financial Services Authority and Bank Indonesia have tightened the standards that must be met, given the high sensitivity of financial data. The same principles regarding the importance of risk management and robust technological infrastructure in digital transformation are also found in studies by Putra and Arifin (2021) and Wahyudi et al. (2021), which show that the adoption of secure and managed digital technology is an important foundation for operational efficiency and sustainability. Regulations such as POJK No. 13/POJK.02/2018 concerning Digital Financial Innovation and PBI No. 22/23/PBI/2020 concerning Payment Systems require the implementation of stricter information technology risk management, including the obligation to conduct regular cybersecurity audits. These sectoral regulations reaffirm the minimum standards set by the PDP Law and the ITE Law, thereby creating an additional layer of protection for consumers of digital financial services, which, according to Arner et al. (2020), is necessary to maintain the integrity and reliability of digital systems.

If a fintech or e-commerce company fails to maintain the security of customer data, there are three avenues of liability that may arise simultaneously. Administrative liability is a form of direct sanction imposed by the supervisory agency based on the PDP Law. These sanctions can take the form of written warnings, temporary suspension of data processing activities, deletion of personal data, and administrative fines of up to two per cent of annual revenue (Halim, 2022). This layered sanction model is designed to have a deterrent effect and encourage companies to priorities investment in data security.

Civil liability may also arise if the data subject suffers material or immaterial losses as a result of a data breach. A claim for compensation can be filed based on Unlawful Acts as regulated in Article 1365 of the Civil Code, with evidence covering the elements of fault, loss, and the causal relationship between the two. In addition, Article 12 of the PDP Law grants direct litigation rights to data subjects, a provision that strengthens the legal position of consumers and simplifies the basis for filing claims for compensation.

Beyond administrative and civil sanctions, the PDP Law also contains criminal provisions that apply when there are acts of collecting, disclosing, or using personal data unlawfully. Articles 67 to 69 regulate these criminal penalties, including provisions regarding corporate criminal liability when violations are committed for or on behalf of a company. The criminal penalties take the form of very large fines, which may even be accompanied by additional penalties such as the confiscation of profits or the dissolution of the legal entity if the violation is considered serious.

With all applicable regulations in place, Indonesia's current legal framework places a significant obligation on fintech and e-commerce companies to develop robust data security systems and demonstrate compliance (Adawiyah et al., 2022). These obligations are no longer merely general standards of due diligence, but rather a set of specific obligations that can be audited and tested legally. Companies that fail to meet these expectations will face administrative, civil, and criminal consequences, demonstrating the strictness of Indonesian positive law in protecting consumers' personal data in the digital age.

Ideal Legal Mechanisms for the Protection and Restoration of the Rights of Customers Who Are Victims of Data Breaches

Although the existing legal framework provides a formal basis for holding corporations accountable, empirical legal practice demonstrates that individual victims' access to justice remains largely theoretical rather than practical (Rosadi, 2020). This structural problem may also be addressed from a preventive technology perspective. As proposed by Costa et al. (2023), emerging technologies such as blockchain can function as instruments for generating immutable and transparent audit trails, enabling traceable data records that simplify and shorten the legal evidentiary process. From a doctrinal standpoint, conventional civil litigation has evolved into an inherently unbalanced arena, characterized by high financial and temporal costs that impose a disproportionate burden of proof on victims, particularly in cases involving non-material losses such as psychological harm or future identity misuse (Budhijanto, 2018).

The asymmetry of information and resources between individual data subjects and corporate data controllers creates a fundamental inequality before the law, undermining the principle of substantive justice (Sutanto & Prabowo, 2021). High litigation costs effectively discourage victims from pursuing legal remedies, transforming the right to sue into a privilege accessible only to those with sufficient resources. Moreover, damages arising from data breaches are often latent and continuous, a characteristic that is difficult to accommodate within traditional civil evidentiary frameworks that prioritize direct and immediate loss (Rosadi & Gumelar, 2019). The difficulty in quantifying non-material damages frequently results in minimal compensation awards, even when plaintiffs prevail, thereby weakening the deterrent and restorative functions of civil liability.

As a consequence, the incentive for victims to pursue individual legal action remains extremely low when potential compensation is disproportionate to the costs and efforts involved. This persistent gap between rights guaranteed by law and their effective enforcement in judicial practice constitutes a serious justice deficit (Budhijanto, 2021). Therefore, the development of alternative dispute resolution mechanisms specifically designed for personal data protection disputes is not merely a policy option, but a legal necessity aimed at achieving victim-centric, efficient, and substantively restorative protection.

One of the biggest obstacles for victims of data breaches is proving the number of actual damages. It is difficult to put a monetary value on the loss of privacy, the potential for future identity theft, or psychological distress. The ideal mechanism addresses this by introducing the concept of statutory damages. The government, through Government Regulations derived from the PDP Law, sets a definite minimum compensation amount for each customer's data that is proven to have been leaked due to corporate negligence. For example, between £6,500 and £65,000 per affected individual. With statutory compensation, victims are no longer burdened with proving the number of damages. The focus of evidence in court shifts to become simpler: (1) Was the victim's data actually leaked? and (2) Was the leak caused by the company's failure to meet the security standards required by law? This mechanism provides legal certainty, speeds up the litigation process, and creates a strong economic disincentive for companies to take data security lightly.

The establishment of a Sectoral Data Breach Compensation Fund that depends entirely on the financial capacity of the offending company to pay compensation is risky, especially if the company goes bankrupt or engages in legal maneuvers to evade liability. Previous studies emphasize that compensation mechanisms solely relying on corporate solvency fail to provide adequate

protection for victims of data breaches (Budhijanto, 2019). An ideal mechanism should therefore create a financial safety net that is independent of individual corporate financial conditions. This requires institutional instruments capable of ensuring the sustainability of the compensation fund without being directly tied to the economic stability of a single company (Rosadi, 2021).

The existence of an independent management institution that collects mandatory contributions from all industry players can strengthen the stability of the fund and distribute risk more equitably across the sector (Sutanto & Prabowo, 2020). Furthermore, the involvement of regulators in determining contribution standards and compensation distribution mechanisms is essential to enhance legitimacy, accountability, and legal certainty (Budhijanto, 2020). Transparency in fund management plays a crucial role in maintaining public trust and preventing misuse of compensation resources (Rosadi & Pratama, 2022).

In addition, the integration of technology-based surveillance and monitoring systems can accelerate the detection of data protection violations and ensure that compensation funds are allocated appropriately and efficiently (Sutanto, 2021). Accordingly, the establishment of a structured compensation fund that is independently managed, technologically supported, and closely supervised through clear regulatory frameworks will provide more effective and sustainable protection for victims of data breaches.

Sectoral supervisory authorities (OJK for fintech and the Ministry of Trade for e-commerce) are mandated to establish a "Data Breach Compensation Fund". This fund is sourced from mandatory annual contributions collected from all businesses in the sector, the amount of which is proportional to the scale of the business and the volume of data managed. When a mass data breach incident occurs, verified victims can file claims to receive quick initial compensation from this fund, without having to wait for a final and binding court decision. Furthermore, the fund manager has the right of subrogation, which is the right to replace the victim in collecting or suing the negligent company to replenish the funds that have been disbursed. This ensures that victims receive quick recovery while the final burden remains with the responsible party.

The law enforcement mechanism that limits the Data Protection Authority (DPA) to only filing lawsuits in district courts is a fundamental procedural obstacle, making this option often an inefficient last resort. Reliance on the general court system, which is fraught with formalities, lengthy proceedings, and not always supported by judicial expertise specialized in technology and data disputes, inherently weakens the responsiveness and effectiveness of law enforcement. Thus, the most logical institutional evolution is the transformation of the DPA's authority from merely an entity that initiates litigation to a quasi-judicial body with direct adjudicative powers to resolve disputes. An internal adjudicative forum will ensure that disputes are handled by experts who understand the technical and legal complexities of data protection. Dispute resolution procedures can be designed to be simpler and faster than formal court proceedings. This would drastically lower the threshold for victims to seek justice without being burdened by high legal costs. The APD could be mandated to issue final and binding decisions, including orders for compensation payments or obligations to improve security systems. This transformation changes the position of the DPA from merely a prosecutor to an authorized and impartial dispute arbitrator. This authority enables the DPA to progressively build a consistent and predictable body of jurisprudence. Ultimately, adjudication capabilities will strengthen the functional effectiveness and institutional authority of the DPA as the front line of personal data protection (Halim, 2022).

Grant quasi-judicial or adjudicative powers to the Data Protection Authority (DPA) to be established. The DPA will not only have the authority to impose administrative sanctions on companies, but also to adjudicate individual disputes and order direct compensation payments to victims. This mechanism creates a low-cost jurisdiction for dispute resolution, handled by expert bodies in their respective fields. The process can be designed to be simpler and faster than general courts. DPA decisions are binding, but still open to appeal to the State Administrative Court or designated courts, so that the principle of due process of law is maintained (Hoofnagle et al., 2019).

The modernization of class action mechanisms through digital facilitation is increasingly essential in addressing large-scale data breach incidents affecting thousands or even millions of customers. In such contexts, individual lawsuits are procedurally inefficient and structurally incapable of delivering effective remedies due to excessive costs, prolonged litigation timelines, and complex evidentiary requirements (Putra & Rahman, 2020). Although class action procedures have been formally recognized within the Indonesian legal system, their implementation remains largely conventional and insufficiently responsive to the

challenges posed by digital-era mass harm cases (Wijaya, 2021). Existing procedural frameworks do not adequately accommodate electronic evidence, digital identification of class members, or online notification mechanisms, all of which are crucial in data breach disputes involving dispersed and anonymous victims.

Therefore, reforming the Supreme Court Regulations on Class Action Proceedings by incorporating a dedicated chapter for personal data breach cases is a necessary legal development. Such reform would enable digital-based claim registration, electronic validation of class membership, and standardized approaches to assessing collective damages, including non-material losses (Kusuma & Fadhilah, 2022). The adoption of technology-enabled class action procedures would not only improve procedural efficiency and reduce litigation costs but also enhance substantive justice by lowering barriers to collective redress and ensuring more equitable compensation outcomes (Hapsari, 2019). Without procedural modernization, class actions risk remaining a formalistic remedy that fails to deliver meaningful protection for data breach victims in the digital economy.

There are new elements such as digital registration through the creation of a special e-court portal where victims can register online as group members with digital identity verification. In addition, there is simplified class certification. The principle of utilizing digital platforms to increase reach, transparency, and participation is in line with the study by Infante and Mardikaningsih (2022), which identifies the potential of social media as an effective promotional tool, where the same logic can be applied to inform and mobilize the participation of victims in broad class actions. Establishing that massive data leaks from a single source are presumed to meet the criteria of factual and legal similarity to be certified as a class action. Requiring companies whose data has been leaked to fund public announcements in mass and digital media to reach and inform victims about the class action lawsuit. This is important to ensure equal access to justice (Shidarta, 2017).

The ideal legal mechanism for the recovery of the rights of data breach victims must be multi-pronged and progressive (Yuniarti, 2022). A combination of statutory compensation that provides certainty, sectoral compensation funds that guarantee the liquidity of recovery, data protection authorities with adjudicative powers as a fast track, and the modernisation of class actions for handling mass cases will create a legal ecosystem that truly protects consumers in the digital age. This synergistic system is designed to address the weaknesses of a single approach by providing different options according to the complexity of the case, the number of victims, and the needs of recovery.

This multi-pronged approach fundamentally shifts the paradigm from simply punishing companies to focusing on the quick, effective, and fair recovery of victims. Thus, the objective of the law does not stop at imposing sanctions, but rather at fulfilling restorative justice that restores the victims' position as much as possible and prevents similar losses in the future through systemic improvements in corporate data governance.

CONCLUSION

A legal analysis of the legal framework for personal data protection in Indonesia shows progressive legislative movement, but leaves significant gaps in terms of restoring victims' rights. On the one hand, the state has succeeded in establishing a solid foundation for corporate accountability. The Personal Data Protection Act, which works synergistically with the Electronic Information and Transactions Act and sectoral regulations from the Financial Services Authority and Bank Indonesia, explicitly imposes heavy legal obligations on fintech and e-commerce companies to maintain customer data security. This framework comprehensively outlines administrative, civil, and criminal sanctions for corporations found to be negligent, signaling the state's seriousness in demanding accountability from data controllers.

However, further investigation reveals that the existence of this legal framework for accountability does not in itself guarantee restorative justice for individuals whose data has been leaked. There is a wide gap between a customer's theoretical right to claim compensation and their practical ability to pursue complex, costly litigation that is often disproportionate to the proven value of the loss. Thus, the pillar of consumer protection becomes fragile at the most crucial point, namely during recovery after a loss has occurred. To perfect the legal protection cycle, the focus of policy must shift from merely punishing corporations to empowering victims.

Therefore, an evolution of a victim-oriented legal framework through the implementation of innovative and efficient mechanisms is recommended. The introduction of the concept of statutory compensation will provide legal certainty and simplify the burden of proof for victims. The establishment of a sectoral compensation fund

financed by the industry itself will serve as a financial safety net that can provide rapid recovery without having to wait for lengthy court proceedings. In addition, granting adjudicative authority to the Data Protection Authority and modernizing class action procedures will open up more affordable and effective access to justice for millions of victims in large-scale incidents. Only by combining the pillar of strict corporate accountability with the pillar of effective victim recovery can Indonesia build a digital ecosystem that is not only innovative, but also safe and fair for all its citizens.

REFERENCES

Adawiyah, R., Prasetyo, M. A., Septiyan, R., Leonardy, S. P., & Calvin, M. A. (2022). *Analysis Of E-Commerce Data Breach and Theft*. https://doi.org/10.55942/pssj.v2i2.168

Agustiawan, M. H., Umam, K., & Maleka, M. (2022). The Importance of Consumer Protection Law Revision in the Development of E-Commerce in the Digital Transformation Era in Indonesia. *Proceedings of Islamic Economics, Business, and Philanthropy*, 1(2), 305-317.

Ali, R., & Darmawan, D. (2023). Big Data Management Optimization for Managerial Decision Making and Business Strategy. *Journal of Social Science Studies,* 3(2), 139-144.

Arner, D. W., Buckley, R. P., & Zetzsche, D. A. (2020). *COVID-19, Fintech, and the Recovery: A New World for Finance and Regulation*. European Banking Institute, 59.

Aziz, A., Darmawan, D., Khayru, R. K., Wibowo, A. S., & Mujito. (2023). Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector. *Journal of Social Science Studies*, 3(1), 23-28.

Baraja, M. U., Saputra, R., Saktiawan, P., Dirgantara, F., & Waskito, S. (2023). Implementation and Supervision of Personal Data Protection Law on Online Platforms. *Journal of Social Science Studies,* 3(1), 101-108.

Budhijanto, D. (2019). *Cyber Law and Data Protection in Indonesia*. Bandung: PT Refika Aditama.

Budhijanto, D. (2020). Legal Responsibility and Compensation Mechanisms in Personal Data Protection. *Journal of Law and Policy*, 15(2), 145–160.

costa, S. da., Darmawan, D., & Isaac, A. de J. (2023). Safeguarding Employee Data with Blockchain in HR. *International Journal of Service Science, Management, Engineering, and Technology,* 4(3), 41–46.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th Ed.).* Sage Publications.

Darmawan, D., P. N. L. Sari, J. Jahroni, S. N. Halizah & R. Mardikaningsih. 2023. Digitalization of Kedai Industry: Analysis of The Role of Internet Marketing Orientation and Innovation on Marketing Performance. *Sustainable Environmental and Optimizing Industry Journal*, 5(1), 21-31.

Faridi, F., Darmawan, D., Hardyansah, R., Putra, A. R., & Wibowo, A. S. (2023). Legal Protection for Online-Based Lending Consumers. *International Journal of Service Science, Management, Engineering, and Technology,* 4(2), 34–38.

Gardi, B., & Eddine, B. A. S. (2023). Cyber Security and Personal Data Protection in the Digital Age: Challenges, Impacts, and Urgency of Global Collaboration. *Bulletin of Science, Technology and Society,* 2(3), 58–63.

Halim, E. F. (2022). Perlindungan Hukum Data Pribadi Pembeli di Perdagangan Secara Elektronik (E-Commerce) di Indonesia [Legal Protection of Buyer's Personal Data in E-Commerce in Indonesia]. *Jurnal Hukum Visio Justisia*. https://doi.org/10.19166/vj.v2i1.5190

Hapsari, R. D. (2019). Collective Litigation and Access to Justice in Indonesia. *Yuridika*, 34(2), 215–230.

Hidayat, A., & Nugroho, R. S. (2020). Corporate Liability for Data Breaches in Electronic Commerce. *Journal of Law, Policy and Globalization,* 96, 52–61.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and What it Means for Research. *Information, Communication & Society*, 22(1), 65-79.

Infante, A. & R. Mardikaningsih. (2022). The Potential of Social Media as a Means of Online Business Promotion. *Journal of Social Science Studies*, 2(2), 45-48.

Khairi, M., & Darmawan, D. (2022). Developing HR Capabilities in Data Analysis for More Effective Decision Making in Organizations. *Journal of Social Science Studies,* 2(1), 223-228.

Kitab Undang-Undang Hukum Perdata (KUHPerdata).

Kusuma, A. R., & Fadhilah, N. (2022). Digital Transformation of Civil Procedure and Mass Dispute Resolution. *Journal of Civil Law Studies*,

7(1), 88–104.
Mardikaningsih, R. & D. Darmawan. (2023). Analysis of Financial Literacy and Risk Tolerance on Student Decisions to Invest. *International Journal of Service Science, Management, Engineering, and Technology*, 3(2), 7–12.
Marzuki, P. M. (2017). *Penelitian Hukum: Edisi Revisi*. Kencana.
Negara, D. S., & Darmawan, D. (2023). Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. *Bulletin of Science, Technology and Society*, 2(2), 13-19.
Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran.
Peraturan Otoritas Jasa Keuangan Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan.
Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE).
Poernomo, S. L. (2023). Transformative Justice, Protection of Consumer Personal Data in Online Loan Business in Indonesia. *Russian Law Journal,* 11(3), 559-570.
Poernomo, S. L. (2023). Transformative Justice, Protection of Consumer Personal Data in Online Loan Business in Indonesia. *Russian Law Journal,* 11(3), 559-570.
Putra, A. R., & Arifin, S. (2021). Supply Chain Management Optimization in the Manufacturing Industry through Digital Transformation: The Role of Big Data, Artificial Intelligence, and the Internet of Things. *Journal of Social Science Studies,* 1(2), 161-166.
Putra, J. M., & Lie, G. (2023). Liability For Processing Personal Data at Private Universities Related to Personal Data Protection Based on Indonesian Law. *UNES Law Review*, 6(2), 6679-6687.
Putra, M. A., & Rahman, I. (2020). Procedural Barriers in Class Action Lawsuits. *Journal of Legal Reform*, 5(3), 173–187.
Rosadi, S. D. (2019). The Urgency of Personal Data Protection Law in Indonesia: A Comparative Law Perspective. *Journal of Southeast Asian Human Rights*, 3(2), 318-333.
Rosadi, S. D. (2021). *Personal Data Protection and Privacy Rights in Indonesia*. Jakarta: Prenadamedia Group.
Rosadi, S. D., & Pratama, A. B. (2022). Transparency and Accountability in Data Protection Governance. *Journal of Digital Law*, 6(1), 33–47.
Shidarta. (2017). *Hukum Perlindungan Konsumen Indonesia.* Grasindo.
Sutanto, H. (2021). Administrative Sanctions as Regulatory Instruments in Digital Consumer Protection. *Journal of Legal, Ethical and Regulatory Issues*, 24(2), 1–11.
Sutanto, H. (2021). Technology-Based Supervision in Personal Data Protection Enforcement. *Journal of Information Law and Technology,* 4(2), 89–103.
Sutanto, H., & Prabowo, R. (2020). Regulatory Models for Data Breach Compensation Funds. *Indonesian Journal of Legal Studies*, 10(3), 201–215.
Umar, N., Pujayanti, L. P. V. A., Sabir, M., & Kasim, A. (2021). The Effectiveness of the Implementation of Administrative Sanctions in Consumer Dispute Resolution in the E-Commerce Era under the Consumer Protection Law. *Riau Law Journal*, 9(1), 73-87.
Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).
Wahyudi, W., R. N. K. Kabalmay, & M. W. Amri. (2021). Big Data and New Things in Social Life. *Studi Ilmu Sosial Indonesia*, 1(1), 1–12.
Wijaya, T. S. (2021). The Effectiveness of Class Actions as a Consumer Protection Instrument. *Journal of Indonesian Private Law*, 4(2), 99–113.
Yuniarti, S. (2022). Protection of Indonesia's Personal Data After Ratification of Personal Data Protection Act. *Keadilan Progresif*. https://doi.org/10.36448/plr.v4i02.85

***Y. F. Mujisulistyo, D. Darmawan, & F. Dirgantara. (2024). Reconstruction of the Legal Mechanism for Consumer Rights Recovery Regarding Personal Data Leaks in the Financial Technology and E-Commerce Sectors in Indonesia, *Journal of Social Science Studies*, 4(1), 75– 84.**