Effectiveness of Legal Protection Against Misuse of Personal Data in Peer-To-Peer Lending Fintech Services Based on Law Number 27 Of 2022 on Personal Data Protection

Uly Alfinda Salsabila[1*], Dona Budi Kharisma[2]

[1] Faculty Of Law, Sebelas Maret University
[2] Faculty Of Law, Sebelas Maret University
*Corresponding Author:
Email: ulyalfind04@gmail.com

Abstract.

This study analyzes the effectiveness of legal protection against the misuse of consumers' personal data in the digital financial services sector. The research is motivated by the increasing incidents of data breaches and misuse of personal data that harm consumers, while also examining the capability of existing regulations to provide adequate protection. This study evaluates the effectiveness of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The research employs a normative legal research method with a statutory and conceptual approach. Primary data is derived from Law Number 27 of 2022 on Personal Data Protection (PDP Law), while secondary data comes from relevant legal literature. This research is important due to the growing problem of personal data misuse in fintech P2P lending services, which is rapidly expanding, thus necessitating more specific regulatory updates to keep up with technological developments in fintech in general. The purpose of this study is to analyze the effectiveness of the implementation of Law No. 27 of 2022 in regulating personal data protection and the sanctions imposed on parties involved in the misuse of personal data. This indicates that although legal instruments for data protection are available, their implementation still faces obstacles, particularly in terms of oversight and law enforcement, which remain weak. Therefore, this study concludes that regulatory harmonization, strengthening the role of supervisory institutions, and raising legal awareness are necessary.

Keywords: *Personal Data Protection; Fintech P2P Lending and Legal Effectiveness.*

I. INTRODUCTION

Globalization has had a very significantly impacted the development of information and communication technology. These changes have not only affected people's lifestyles but have also driven transformations in various aspects of life, ranging from culture, society, and security to law and the economy (Andhika et al., 2024). The development of information technology has also driven the emergence of a new economic system, shifting from a traditional manufacturing-based model to a digital economy that prioritizes technology, creativity, and knowledge. This phenomenon has given rise to the concept of a creative economy, which has become a hallmark of modern civilization.However, these advances in information technology present both challenges and opportunities for the field. On one hand, technology brings convenience and efficiency to various aspects of life, but on the other hand, it creates new problems, including in the digital economy. One of the most affected sectors is information technology-based financial services. As society’s needs grow increasingly complex, fintech has emerged as an alternative solution, providing fast, practical, and easily accessible financial services, especially for groups that have difficulty accessing conventional banking services (Pasaribu et al., 2024).One of the rapidly growing innovations in fintech is Peer to Peer Lending (P2P Lending) online loan service One of the rapidly growing innovations in fintech is peer-to-peer (P2P) lending online loan services (Agustin et al., 2023).

Through this mechanism, the public can obtain funds quickly without having to go through lengthy procedures as in banking institutions do. Online lending fintech also directly brings creditors and debtors together through digital platforms without requiring collateral. This has made online lending services increasingly popular, especially among those in urgent financial situations (Septiani et al., 2024).However, online lending innovations are inevitably accompanied by crucial legal issues, particularly regarding the protection of consumers' personal data. Various cases of personal data misuse have emerged, including the use of all personal contacts for debt collection, spam text messages, threats, and even defamation (Satrio Ulil Albab, 2024). These practices not only cause material losses but can also lead to severe psychological impacts, including extreme cases such as depression and suicide. This phenomenon highlights the gap between ideal legal norms (das sollen) and the realities of data protection implementation in the field (das sein).Cases involving digital-based lending services are a tangible manifestation of the widespread misuse of consumers' personal data in online lending activities.

Although normatively, personal data protection has been regulated in various laws, such as Law Number 11 of 2008 on Electronic Information and Transactions as amended by Law No. 19 of 2016 (UU ITE), Law Number 27 of 2022 on Personal Data Protection (UU PDP), and the Financial Services Authority Regulation Number 77/POJK.01/2016 concerning Information Technology-Based Lending and Borrowing Services, in reality, the implementation of these regulations still faces major challenges (Ramadhani, 2022). This study differs from previous studies in that it specifically focuses on analyzing the effectiveness of legal protection against the misuse of consumer personal data in online lending services. This study discusses the normative aspects of personal data protection and analyzes the legal consequences of agreements involving personal data breaches and the legal sanctions that may be imposed on service providers. Accordingly, this research is expected to provide academic contributions and practical input for improving regulations and the implementation of consumer personal data protection in Indonesia. Therefore, this study aims to answer the following research question: To what extent is the effectiveness of legal protection against the misuse of consumers' personal data in P2P lending services based on Law No. 27 of 2022 on Personal Data Protection, and what are the legal ramifications arising from online loan agreements involving personal data breaches, as well as the applicable legal sanctions for service providers violating these provisions.

II. METODS

This research uses a normative juridical method, with a primary focus on literature studies. This approach was chosen to analyze and examine the effectiveness of legal protection against the misuse of personal data in digital financial services (Markuat, 2022). This study employs a normative juridical approach that is both prescriptive and descriptive. This is based on the analysis of legal concepts, regulations, and other legal materials. The study also comprehensively identifies legal principles, including legal protection and its application in Law Number 27 of 2022 on Personal Data Protection, as well as legal remedies for personal data misuse in the context of fintech services that have developed in society. The selection of normative legal research methods is highly relevant to this study, as it enables a systematic and critical review of the norms, principles, and prevailing legal regulations (statute approach) concerning the social issues of personal data misuse in fintech. This method is crucial for assessing das sollen (what ought to be), as stipulated in legal texts, in comparison with das sein (what actually happens) in practice, thus allowing for an evaluation of the legal framework's effectiveness. The analytical approach is conducted by dissecting the provisions of the Personal Data Protection Law, the Electronic Information and Transactions Law, and the Financial Services Authority Regulations to understand their scope, limitations, and interrelations, and then synthesizing these legal materials to build a comprehensive argument regarding legal protection and sanctions.

Legal material analysis specifically includes the interpretation of lawmakers' intentions when they draft regulations. Additionally, the analysis covers the identification of possible multiple interpretations or differing meanings of the same rule (i.e., multiple interpretations). Furthermore, an evaluation is conducted to ensure that these rules are consistent and not contradictory (coherent) with each other to provide strong and effective data protection. The legal sources used in this analysis are primary legal materials, namely, officially applicable laws, such as Law Number 27 of 2022. This primary legal material serves as the main basis for understanding the rules and provisions that govern data protection. Secondary legal materials include books, journals, academic articles, and official reports from government agencies, whereas tertiary legal materials include legal dictionaries and encyclopedias. This methodology also involves a literature review and normative juridical perspective to provide a critical evaluation of the effectiveness and implementation of Law No. 27 of 2022 in the context of personal data protection in the digital era and the legal consequences imposed on Fintech service providers for the misuse of personal data.

III. RESULT AND DISCUSSION

3.1 Legal Protection of Consumers' Personal Data in Digital Financial Services

This study focuses on the effectiveness of legal protection of consumer personal data in digital financial services. The legal protection of consumer personal data in the digital financial services ecosystem can be fundamentally conceptualized into two complementary dimensions: general and specific legal protection. General legal protection is rooted in the universal constitutional guarantee inherent to every individual as a citizen. Article 28G, paragraph (1) of the 1945 Constitution of the Republic of Indonesia is the main foundation, explicitly guaranteeing every individual's right to be protected from threats to personal security, dignity, and the right to privacy. This right affirms that each individual possesses authority over their personal information, a principle of significant importance in the contemporary digital era (Kurniawan et al., 2025).Specific legal protection refers to a sectoral regulatory framework designed to address the complexities and specific risks of personal data processing in digital services (Gea et al., 2025). Specific legal protection in Indonesia's fintech sector can be divided into several layers of regulation. The General Sectoral Law, namely, Law Number 11 of 2008 concerning Electronic Information and Transactions (EIT Law) and its amendments, regulates the principle of data owners consent in Article 26 as the basis for the utilization of electronic data.Implementing Government Regulations such as Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, which defines Personal Data in more detail and regulates the obligations of electronic system providers.

The Ministry of Communication and Information Technology Technical Regulations, such as Regulation Number 20 of 2016 concerning Personal Data Protection in Electronic Systems, sets technical standards and procedures. Special Financial Sector Regulations: Financial Services Authority Regulation (OJK Regulation) Number 77/POJK.01/2016 provides stricter legal foundations for fintech providers, requiring the application of confidentiality, integrity, and data availability principles.This framework includes a series of more detailed legal instruments, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which regulates the use of personal data via electronic media. Article 26 of the EIT Law explicitly requires the consent of data owners as a primary prerequisite before data can be utilized. Although Article 26 of the EIT Law clearly requires data owner consent, in practice, this consent is often obtained through complex and non-transparent standard clauses, as frequently seen in online loan applications. This situation reveals the disparity between the principle of consent, which should be informative and voluntary (das sollen), and the reality in which consumers often feel compelled to agree without adequate understanding (das sein).Regulations regarding personal data can also be found in various legislative regulations, such as in the financial services sector, there is the Financial Services Authority Regulation (OJK Regulation) Number 77/POJK.01/2016, which provides stricter legal foundations, requiring fintech providers to apply principles of confidentiality, integrity, and data availability to prevent misuse (Rifa & Hidayati, 2024).

Although this normative framework has been established, its implementation frequently poses substantial challenges. These include the rapid pace of technological advancement, which introduces new avenues for misuse, as well as the transnational nature of data flows, which are challenging for a single jurisdiction to regulate.There is also organic regulation of personal data, as stipulated in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. The general provisions state that "Personal Data is any data about an individual that is identified and/or can be identified either separately or combined with other information, both directly or indirectly through Electronic and/or non-electronic Systems." Further regulation is found in the Ministry of Communication and Information Technology Regulation Number 20 of 2016 concerning Personal Data Protection in Electronic Systems. Regulations regarding personal data are also found separately in various legislative regulations, such as the Ministry of Communication and Information Technology Regulation Number 11 of 2016 concerning Electronic Interactive Game Classification, Law Number 43 of 2009 concerning Archiving, Ministry of Communication and Information Technology Regulation Number 4 of 2016 concerning Information Security Management Systems, Ministry of Communication and Information Technology Regulation Number 36 of 2014 concerning Procedures for Registration of Electronic System Providers, and many others related to personal data in the context of positive Indonesian law (Ramadhani, 2022).

There are case studies of large-scale data breaches, such as the Facebook data leak case involving Cambridge Analytica, where 87 million user data were misused, including from Indonesia, showing the vulnerability of personal data even on the largest global platforms. Domestically, the Tokopedia data leak incident in 2020, which involved 91 million user data, highlights the limitations of law enforcement against business actors, especially when standard clauses and court decisions favor business actors (Ramadhani, 2022). Indicators of implementation challenges drawn from statistical data and institutional reports include data collected by the Legal Aid Institute in Jakarta, which shows that 36.07% of reports originate from DKI Jakarta and are spread across 25 provinces in Indonesia. This indicates that the misuse of personal data, particularly in online loan applications, is a systemic problem in the country. This is reinforced by a report from the Directorate of Special Crime Investigation at the North Sulawesi Regional Police, which revealed a data theft scheme used for debt collection, confirming that illegal practices have been integrated into the operations of some online lending services (Giffari, 2025). This situation leads e-commerce business actors to often neglect the security of consumers' personal data, risking abuse such as fraud and consumer losses. Developments in information technology have enabled promotions and buying and selling transactions to occur easily and without temporal or geographical limitations.

Personal data protection is part of the right to privacy, which includes the right to confidentiality, the right to communicate free from surveillance, and the right to control access to one's data. Article 26 of the Ministry of Communication and Informatics Regulation No. 20 of 2016 regulates the rights of personal data owners, such as lodging complaints, accessing, correcting, and destroying data, as well as the obligations of data users to maintain confidentiality, use the data as needed, and bear responsibility for its misuses. In e-commerce, contracts occur digitally (paperless) through consent via clicks or checkboxes, creating a legal bond between the seller and buyer (N. Hidayat et al., 2025).Indonesia has faced significant challenges regarding personal data protection due to the absence of comprehensive regulations specifically governing this issue. Previously, data protection was only partially covered by the Electronic Information and Transactions Law (UU ITE) and several related regulations, which were deemed inadequate to address the complexity and risks associated with personal data management. This regulatory gap has contributed to several incidents of data misuse, causing public concern and highlighting the urgent need for a clearer and stronger legal framework to protect privacy and personal information in the metaverse. In response to these challenges, the Indonesian government has initiated the drafting of a new law specifically aimed at protecting personal data. This new regulation seeks to establish comprehensive standards and mechanisms for the collection, processing, storage, and sharing of personal data to ensure that individuals' rights are adequately protected in the digital era.

By addressing previous legal limitations and providing clearer guidelines for both the public and private sectors, this regulation aims to prevent data misuse, increase accountability, and build greater trust in digital services and technology. The regulation of personal data protection in fintech transactions in Indonesia is governed by a series of laws and regulations promulgated by the pertinent authorities. The Personal Data Protection Law (UU PDP) constitutes the primary legal framework for safeguarding personal data in Indonesia, including the fintech sector. This legislation delineates the responsibilities of fintech service providers in managing and protecting consumer data in accordance with the principles of transparency, accountability, and security. Within the Indonesian legal framework, Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) stipulates the rights and obligations of entities involved in managing personal data. This regulation underscores the necessity of obtaining consent from data owners when handling personal information of individuals. The UU PDP is a legislative measure that incorporates elements of the General Data Protection Regulation (GDPR), which was previously enacted in the European Union (EU). The following are several principles shared by both the UU PDP and the GDPR.(Febrian et al., 2025).The enactment of Law No. 27 of 2022 concerning Personal Data Protection primarily seeks to enhance public awareness and adherence to the principles of safeguarding personal information and security in Indonesia. This legislation is anticipated to improve the protection of individuals' personal data and mitigate the occurrence of information breaches that could potentially harm citizens.

The regulation encompasses various dimensions, including fundamental principles, categories of personal information, the rights of data owners, and the obligations of data managers and processors, as well as administrative and criminal penalties for violations of personal data protection.(Kurniawan et al., 2025) In this context, the OJK promulgated OJK Regulation Number 10/POJK.05/2022 concerning Information Technology-Based Funding Services, which governs the access to and utilization of personal data, data retention durations, data deletion, and administrative sanctions. In 2023, the OJK issued OJK Circular Letter Number 19/SEOJK.05/2023 on the Implementation of Information Technology-Based Funding Services as a continuation of POJK Number 10/POJK.05/2022. This OJK Circular Letter represents a tangible implementation of the 2023–2029 fintech lending development and strengthening roadmap within the pillars of regulation, supervision, and licensing. Concurrently, in 2022, the Republic of Indonesia enacted Law Number 27 of 2022 on Personal Data Protection, which, among other provisions, regulates institutions, specifically the Personal Data Protection Authority (PDP). The PDP Law is responsible for overseeing the management of personal data by electronic system providers, both governmental and private, to ensure adherence to the criteria set forth in the PDP Law, which mandates its independence. (Nurul Insi Syahruddin & Eva Achjani Zulfa, 2024). As outlined in Article 1, Point 12 of Law Number 27 of 2022 on Personal Data Protection (PDP Law), the automated processing of personal data encompasses the collection, analysis, and evaluation of such data without direct human involvement in the final decision-making process.

Profiling is characterized as a type of automated processing used to assess an individual's personal attributes, including preferences, behavior, and economic status. In the realm of finance, personal data handled by financial technology (fintech) platforms comprise basic details, such as name, address, and identification number, alongside sensitive information, such as transaction history, routine expenditures, and geographic location. According to Article 4, paragraph (2) of the PDP Law, financial data are classified as sensitive personal data, necessitating explicit consent from the data subject for its processing, along with additional protective measures. The legal obligations of fintech companies include ensuring data accuracy, providing transparent information, guaranteeing system security, and facilitating mechanisms for data subjects to access, amend, or delete their data. In instances of non-compliance, fintech companies may incur administrative or criminal penalties, as outlined in Articles 57–60 of the PDP Law (Cristine et al., 2025).The Personal Data Protection Law (PDP Law) delineates the legal responsibilities of all entities engaged in the processing of personal data. Within this framework, two primary roles are identified: the Data Controller, who is accountable for determining the purposes and means of data processing, and the Data Processor, who processes data on behalf of the Controller. Entities involved in this process include government agencies, private companies—particularly those in the digital, e-commerce, and fintech sectors—and non-governmental organizations.

A significant number of these agencies and companies have yet to fully comprehend the obligations mandated by the Personal Data Protection Law (PDP Law). Key aspects requiring attention include the necessity to obtain valid consent from data subjects, provide rights of access, correction, and deletion of data, and ensure data protection through adequate security systems. The PDP Law further underscores that every individual possesses rights as a personal data owner; however, for these rights to be effectively upheld, public awareness of the existence and significance of personal data protection is essential.Many Indonesians lack a comprehensive understanding of personal data. A significant number are unaware of their right to withhold their data and are not cognizant of their ability to file complaints in the event of data misuse. For example, it is common for people to provide their ID number, national identification number, or bank account number to applications without first checking the applicable privacy policy. The socialization of the Personal Data Protection Act (UU PDP) is still very limited, with efforts focused only on certain circles, particularly among digital industry players. Unfortunately, the general public has not received adequate attention in this field (Simanjuntak, 2024).In practice, consumers often find themselves compelled to accept all the terms set by loan applications to access funds.

The consent they provide is frequently not based on a comprehensive understanding but is instead given unilaterally, buried within a complex and technical agreement. This undermines the principles of contractual fairness and consumer protection. From a law enforcement perspective, structural weaknesses remain significant. The absence of an independent personal data supervisory authority, as required by Article 58 of the UU PDP, creates ambiguity in oversight and complaint procedures. Law enforcement officials still face limitations in handling cases of digital data misuse, leading to slow legal processes for offenders or cases that never reach the court. This issue is compounded by the low levels of digital literacy among the public. Many users are unaware of their rights as data subjects, including the right to refuse irrelevant data access, withdraw their consent, and seek compensation. Consequently, data misuse persists and is seldom officially reported, as victims often feel confused, fearful, or pessimistic about the outcomes of reporting (Kurniawan et al., 2025).Data leak cases remained high in 2023, indicating that challenges in implementing these regulations remain significant. However, over the past year, the number of reported data breach cases tripled from 35 in 2023 to 111 in 2024. According to global reports released by multiple independent institutions, Indonesia ranks among the top 10 countries with the most data breaches worldwide. The Ministry of Communication and Digital (Komdigi) notes that a high level of risk can erode consumer trust in the national digital ecosystem, especially in fintech services (TribunBisnis, 2025).

Reports from the Financial Services Authority (OJK) documented 1,081 new complaints related to "pindar" from January to March 2025. Most of these reports originated from illegal online loan services that lacked official licenses from the OJK. Throughout 2024, the OJK Task Force for the Eradication of Illegal Financial Activities received 16,231 complaints, of which 15,162 pertained to illegal online lending activities. The reported issues include exorbitant interest rates and fines, unlawful collection practices, misuse of personal data, and lack of legal protection for consumers. A significant number of individuals, particularly in rural areas, lack an understanding of the distinction between legal and illegal online loans, often resulting in their victimization (BPHN, 2025).The implementation of personal information protection in Indonesia encounters several challenges that impede the efficacy of existing regulations despite the enactment of Law No. 27 of 2022. A primary obstacle is the insufficient knowledge and awareness among consumers and business entities regarding the rights associated with personal data and the obligations outlined in the UU PDP. Many consumers remain unaware of their rights to access, correct, or delete personal data on digital platforms. Conversely, business entities often lack a comprehensive understanding of their obligations to manage consumer personal data securely and transparently, which may lead to regulatory infractions and penalties.

Furthermore, technical challenges related to personal data protection are equally important. Although the UU PDP mandates that business entities implement adequate data security systems, numerous companies lack the robust technological infrastructure to safeguard personal data from hacking or data breaches. Personal data security frequently becomes a secondary priority in business development, adversely affecting the quality of data management and protection. Many digital platforms, particularly in the e-commerce and fintech sectors, exhibit vulnerabilities in their security systems, rendering data breaches possible and impacting consumers (R. S. Hidayat, 2025). This situation not only causes financial and non-financial losses for individuals who become victims but also reduces public trust in the national digital ecosystem, especially fintech services, and can hamper the overall growth of Indonesia's digital economy. One of the main challenges is the absence of an independent authority specifically tasked with overseeing companies' compliance with the UU PDP. In Indonesia, supervision still relies on government institutions that do not fully focus on personal data protection. This leads to less-than-optimal enforcement of regulations and makes personal data violations difficult to manage. This condition requires further attention to increase the effectiveness of data protection in Indonesia (Hukom et al., 2025).One of the main challenges is the absence of an independent authority specifically tasked with overseeing companies' compliance with the UU PDP.

In Indonesia, supervision still relies on government institutions that do not fully focus on personal data protection. This leads to less-than-optimal enforcement of regulations and makes personal data violations difficult to manage. This condition requires further attention to increase the effectiveness of data protection in Indonesia (Hukom et al., 2025). Although Law No. 27 of 2022 has been enacted, law enforcement remains weak due to the lack of an independent supervisory authority. Law enforcement officers still lack the adequate capacity to handle data crimes, while inter-agency coordination remains weak. The absence of compensation procedures for victims and allegations of selective law enforcement worsens public trust. Many data breach cases are not fully addressed, creating the impression that privacy violations are not serious criminal offenses. This weakens the deterrent effect and makes digital service providers reluctant to make improvements, while simultaneously undermining the state's legitimacy in protecting citizens' digital rights(Sitorus et al., 2025).

3.2 Sanctions for Violations of Personal Data Protection

Sanctions against parties involved in violations of personal data protection, particularly in the fintech sector, are crucial given the high number of personal data misuse cases. These sanctions play an important role in ensuring compliance by fintech operators and in creating a strong deterrent effect for violators. The imposition of sanctions demonstrates that the existing regulatory framework is effective in providing adequate protection and oversight within the fintech sector. Sanctions for violations of personal data protection in this sector function not only as instruments of law enforcement but also as mechanisms to encourage compliance by service providers. With the threat of administrative and criminal sanctions, fintech operators are expected to exercise greater caution and responsibility in managing consumers' personal data. Administrative sanctions—such as warnings, restrictions on data processing activities, revocation of licenses, and administrative fines—provide corrective and preventive measures that can be implemented swiftly. Meanwhile, criminal sanctions in the form of imprisonment and substantial fines create a stronger deterrent effect for perpetrators who deliberately misuse personal data. Any violation of consumers' personal data protection rights in digital financial services will result in sanction-related consequences enforced by the competent authorities. Under the criminal law framework, Articles 32 and 35 of the Electronic Information and Transactions Law (ITE Law), which are frequently used to prosecute perpetrators of data misuse, stipulate severe penalties in the form of imprisonment of up to six years and/or fines of up to one billion rupiah.

These sanctions are intended to produce a strong deterrent effect on offenders.(Situmeang, 2021).Since a new and more specific regulation concerning the misuse of personal data—particularly in the fintech sector—has now been enacted, namely Law Number 27 of 2022 on Personal Data Protection, any individual who experiences personal data leakage or hacking may rely on this new regulation as a legal basis. Law enforcement in cases of data security violations constitutes the Indonesian government's efforts to uphold the law against organizations or individuals that violate the provisions of the Personal Data Protection Law (PDP Law). Administrative sanctions are instruments of public law authority that may be exercised by the government as a response to non-compliance with obligations stipulated in the norms of State Administrative Law. Based on this definition, four elements of administrative sanctions can be identified, namely: instruments of authority (machtmiddelen), their public law character, their application by the government, and their function as a response to non-compliance. Types of administrative sanctions may be classified according to their objectives as follows: (1) reparatory sanctions, which are imposed as a response to violations of legal norms and are intended to restore conditions to their original state prior to the violation, such as bestuursdwang and dwangsom; (2) punitive sanctions, which are aimed at imposing punishment on an individual, for example in the form of administrative fines; and (3) regressive sanctions, which are imposed as a response to non-compliance with provisions contained in an issued administrative decision. (H.R., 2006).

Administrative sanctions related to violations of personal data protection are clearly regulated under Law Number 27 of 2022 on Personal Data Protection, along with its implementing regulations. These administrative sanctions include: (1) the issuance of warnings, whether verbal or written, to personal data controllers who have committed violations; (2) the temporary suspension of personal data processing activities that do not comply with the applicable regulations; (3) the deletion or destruction of personal data that has been processed unlawfully; and (4) administrative fines that may amount to a maximum of 2% of the annual revenue of the relevant personal data controller, depending on the nature of the violation committed. These administrative sanctions are intended to create a deterrent effect and to ensure that personal data controllers carry out their responsibilities with due care and seriousness in managing personal data. Administrative sanctions serve two essential functions: prevention and punishment. The preventive function seeks to encourage data controllers to comply with personal data protection regulations from the outset, while the punitive function aims to impose a deterrent effect so that violations do not recur.

Through the implementation of these administrative sanctions, it is expected that personal data management will be conducted in a safer and more trustworthy manner, thereby ensuring that the public feels protected in all digital activities.(Shafa Salsabila & Sidi Ahyar Wiraguna, 2025). According to Articles 57 through 60 of the Personal Data Protection Law (PDP Law), administrative sanctions constitute non-criminal legal instruments intended to enforce compliance and to promote improvements in data governance by personal data processing entities. The imposition of administrative sanctions is carried out by an institution designated by the President, with the procedures for their application further regulated through a Government Regulation as stipulated in Article 57 paragraphs (4) and (5). This institution is responsible for conducting supervision, enforcing administrative law, and imposing administrative sanctions for personal data violations as provided under Articles 58, 59, and 60 of the PDP Law. The mechanism for imposing administrative sanctions under Law Number 27 of 2022 on Personal Data Protection is implemented by an institution appointed by the President. This institution is vested with the authority to impose administrative sanctions in the form of written warnings, temporary suspension of personal data processing activities, deletion or destruction of personal data, and/or administrative fines of up to a maximum of 2% of the relevant annual revenue or income, in relation to the violations referred to in Article 57 paragraphs (2)–(4).

(Undang-Undang (UU) Nomor 27 Tahun 2022).In addition to administrative sanctions, the Personal Data Protection Law (PDP Law) also regulates legal measures through criminal proceedings as a form of stronger and more stringent protection against violations in the management of personal data. These criminal penalties are imposed on individuals or legal entities that intentionally access, disclose, or use another person’s personal data without lawful authorization or valid consent. Article 67 of the Personal Data Protection Law stipulates that offenders may be subject to imprisonment for up to five years and/or fines of up to five billion rupiah. This provision demonstrates the government’s serious commitment to creating a strong deterrent effect against personal data violations. Where the violation is committed by a corporation or business entity, the PDP Law allows for the imposition of criminal fines amounting to up to ten times the maximum fine applicable to individuals, indicating that corporations as legal entities are also required to bear full responsibility for negligence or intentional misconduct in safeguarding personal data. (Agustina & Wiraguna, 2025).

Verifiable evidence of government involvement in enforcing data security violations can be seen in law enforcement actions taken against organizations or individuals that violate the provisions of the Personal Data Protection Law (PDP Law). This reflects the government’s commitment to imposing firm sanctions and consequences for data security breaches. Under the PDP Law, both administrative and criminal sanctions are предусмотред for personal data controllers who violate its provisions (Article 67 paragraph (2) of the PDP Law). Individuals who intentionally and unlawfully misuse another person’s personal information may be subject to a maximum penalty of five years’ imprisonment and/or a fine of up to five billion rupiah (Article 67 paragraph (3) of the PDP Law). Administrative sanctions may take the form of warnings, reprimands, restrictions on personal data processing activities, revocation of licenses, and/or administrative fines. Meanwhile, criminal penalties for data-related offenses include fines and/or imprisonment. Through the enforcement of laws against data security violations, it is expected that awareness and compliance among personal data controllers will increase, leading to the consistent application of personal data security standards across all sectors. (Mahameru et al., 2023).

IV. CONCLUSION

This study analyzes the effectiveness of legal protection against the misuse of consumers’ personal data in digital financial services, particularly in online lending fintech platforms. Although regulations such as Law No. 27 of 2022 on Personal Data Protection (PDP Law), the Electronic Information and Transactions Law (ITE Law), and regulations issued by the Financial Services Authority (OJK) are already in place, their implementation continues to face significant challenges, especially with regard to weak supervision and law enforcement.The background of this research is driven by the increasing number of incidents involving personal data breaches and misuse, which have caused substantial losses to consumers, while simultaneously testing the capacity of existing regulations to provide adequate and responsive protection amid rapid technological developments. This study employs a normative legal research method using statutory and conceptual approaches, relying on qualitative analysis of primary, secondary, and tertiary legal materials. Primary data include Law No. 27 of 2022 on Personal Data Protection (PDP Law), while secondary data are derived from relevant legal literature. The analysis aims to describe the current state of regulatory implementation and to identify obstacles that hinder effective law enforcement. Therefore, the urgency to strengthen legal instruments is unavoidable.

This can be achieved through the harmonization of existing regulations, ideally by enforcing a personal data protection law that functions as lex specialis. In addition, the role of supervisory institutions such as the Financial Services Authority (OJK) and the Ministry of Communication and Informatics (Kominfo) must be strengthened, not only in terms of oversight functions but also in the consistent and firm enforcement of sanctions. Equally important, this study emphasizes that effective protection can only be achieved through synergy between integrated regulations, consistent law enforcement, and active consumer participation through increased awareness and legal literacy.Cases of data breaches in Indonesia have increased sharply, with the number of incidents tripling over the past year, placing Indonesia among the top ten countries worldwide with the highest number of data breach incidents. This condition threatens consumer trust in the national digital ecosystem, particularly in fintech services, and demands serious attention from the government and relevant stakeholders. Sanctions for violations of personal data protection include imprisonment of up to six years and fines of up to one billion rupiah under the ITE Law, as well as administrative sanctions ranging from warnings and fines to the revocation of operational licenses imposed by the government and the OJK. With the enactment of the PDP Law, these sanctions have been further strengthened, including maximum penalties of five years' imprisonment and fines of up to five billion rupiah for perpetrators of personal data misuse. Firm law enforcement is expected to enhance awareness and compliance among personal data controllers in applying consistent security standards across all sectors.

REFERENCES

[1] Agustin, N. N., Syapsan, S., & Mayes, A. (2023). Analysis of Factors Affecting Funding Decisions at Fintech Peer-to-Peer Lending in Indonesia. ***International Journal of Economics Development Research***, *4*(3), 2023–2876.

[2] Agustina, W., & Wiraguna, S. A. (2025). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Media Hukum Indonesia (MHI)*, *2*(6), 23–31. https://doi.org/10.52005/rechten.v4i2.98

[3] Andhika, I., Hasan, D., & M. Rafif, A. (2024). Pengaruh Globalisasi Terhadap Kemajuan Teknologi Di Indonesia. ***JI-Tech***, *20*(1), 32–35. https://doi.org/https://doi.org/10.55864/jitech.v20i1.274

[4] Cristine, M. A., Mario, F., Risakota, A., & Celine, S. R. (2025). Perlindungan Data Pribadi dalam Sistem Skoring Kredit Otomatis oleh Fintech di Indonesia : Analisis Yuridis Normatif Berdasarkan Undang- Undang Nomor 27 Tahun 2022. ***Jurnal Studi Hukum Modern***, *07*(3), 1–15.

[5] Febrian, F., Saputra, I. Y., & Napitupulu, D. R. W. (2025). Implikasi Hukum terhadap Perlindungan Data Pribadi dalam Transaksi Fintech. ***Rechtsnormen Jurnal Komunikasi Dan Informasi Hukum***, *4*(1), 21–30. https://doi.org/10.56211/rechtsnormen.v4i1.1153

[6] Gea, G. V. V., Wijaya, J. G., Clarissa, O., & Witanto, A. K. C. (2025). Personal Data Protection on International Digital Trade: Harmonizing State Regulations Through a Common Standard. Veritas et Justitia, *11*(1), 198–225. https://doi.org/https://doi.org/10.25123/zbea9p38

[7] Giffari, R. O. (2025). Perlindungan Terhadap Data Pribadi Yang Digunakan Pihak Lain Pada Pinjaman Online Gagal Baya. ***Jurnal Ilmiah Wahana Pendidikan***, *11*(9), 156–166.

[8] Hidayat, N., Subekti, Astutik, S., & Widodo, E. (2025). Penegakan Hukum Terhadap Penyalahgunaan Data Pribadi Pengguna E-Commerce Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. ***JIRK : Journal of Innovation Research and Knowledge***, *5*(2), 1221–1230.

[9] Hidayat, R. S. (2025). Transformasi hukum bisnis di ekosistem digital: Studi atas perlindungan data pribadi konsumen. ***Journal of Asrtificial Intelligence and Digital Business (RIGGS),*** *3*(4), 46–52.

[10] Hukom, S., Humi, N., & Lukman, I. (2025). The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era. ***Hakim: Jurnal Ilmu Hukum Dan Sosial,*** *3*(1), 974–992. https://doi.org/10.51903/hakim.v3i1.2291

[11] Khodijah, Kamila, M., & Siddiq, M. R. (2022). The Impact of Digital Economics on Economic Growth in Indonesia. Fara'id and Wealth Management, *2*(1), 27–35. https://doi.org/https://doi.org/10.58968/fwm.v2i1.185

[12] Kurniawan, M. F., Eftria, E. R., Prastiwi, D. E., Studi, P., Hukum, I., Hukum, F., Pamulang, U., Selatan, K. T., Digital, P., & Siber, K. (2025). Menjaga Privasi Di Era Digital Perlindungan Hukum Terhadap Data Pribadi Di Indonesia. ***Causa : Jurnal Hukum Dan Kewarganegaraan***, *14*(10). https://doi.org/10.8734/CAUSA.v1i2.365

[13] Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal Badjeber, M., & Rahmadia, M. H. (2023). Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas di Indonesia. ***Jurnal Esensi Hukum,*** *5*(2), 115–131.

[14] Markuat. (2022). Dampak Penetapan Lockdown Bagi Sebuah Negara Dalam Pemenuhan Kebutuhan Berdasarkan Asas Keadilan. ***JPeHI (Jurnal Penelitian Hukum Indonesia),*** *3*(1), 80. https://doi.org/10.61689/jpehi.v3i1.336

[15] Nurul Insi Syahruddin, & Eva Achjani Zulfa. (2024). Personal Data Protection Violations By Fintech Lending in Indonesia. ***Journal of Law, Politic and Humanities***, *4*(4), 999–1006. https://doi.org/10.38035/jlph.v4i4.414

[16] Pasaribu, D., Judijanto, L., Vandika, A. Y., Bilondato, N Sudarmanto, E., & Basri, T. S. (2024). The Role of Fintech Innovation in Financial Inclusion: A Literature Review of Emerging Tren and Challenges. ***Innovative: Journal Of Social Science Research***, *4*(2), 3784–3792.

[17] Ramadhani, S. A. (2022). Komparasi Perlindungan Data Pribadi di Indonesia dan Uni Eropa. ***Jurnal Hukum Lex Generalis***, *3*(1), 73–84. https://doi.org/10.56370/jhlg.v3i1.173

[18] Rifa, F., & Hidayati, M. N. (2024). Kebijakan Penal dalam Perlindungan Data Pribadi Nasabah Fintech Lending di Indonesia. Binamulia Hukum, *13*(2), 461–481. https://doi.org/10.37893/jbh.v13i2.964

[19] Satrio Ulil Albab. (2024). Perlindungan Hukum Terhadap Data Pribadi Nasabah Penyedia Jasa Pinjaman Bukan Bank Secara Online. ***Ethics and Law Journal: Business and Notary***, *2*(1), 176–182. https://doi.org/https://doi.org/10.61292/eljbn.112

[20] Septiani, S., Lalita, S. F., & Zahra, D. R. (2024). Pengaruh Financial Technology Peer to Peer Lending dan Uang Elektronik (E-Money) terhadap Pertumbuhan Ekonomi di Indonesia (Tahun 2021-2023). ***Jurnal Keuangan Dan Perbankan,*** *21*(1), 69–78. https://doi.org/https:doi.org/10.35384/jkp.v21i1.591

[21] Shafa Salsabila, & Sidi Ahyar Wiraguna. (2025). Pertanggungjawaban Hukum atas Pelanggaran Data Pribadi dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. ***Konsensus : Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi,*** *2*(2), 145–157. https://doi.org/10.62383/konsensus.v2i2.736

[22] Simanjuntak, P. H. (2024). Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR). ***Jurnal Esensi Hukum,*** *6*(2), 105–124.

[23] Sitorus, R., Felix, Z., & Banke, R. (2025). Kendala Pelaksanaan Perlindungan Data Pribadi. ***Locus: Jurnal Konsep Ilmu Hukum,*** *5*(1), 53–60.

[24] Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. ***Jurnal SASI,*** *27*(1), 38–52.