 ISSN 2828-9463

Legal Protection of Personal Data in Combating Cybercrime in Indonesia

Rizal Abidin[1], Nur Kumala Dewi[2], Dwi Agung Santoso[3], Taufan Dwiyogo S[4], Nanang Sumargo[5], Cahya Citra Carolene[6], Triana Asih Wulandari[7], Muthi'ah Dwita Fathinah[8]

Informatics Engineering Study Program, Muhammadiyah University of Science and Technology, Jakarta, Indonesia

The development of online lending services as part of financial technology has transformed public access to financial services in Indonesia. This convenience has been accompanied by an increasing volume of personal data processing, which raises new concerns regarding information security and privacy protection. Various data breach incidents indicate that personal data protection is no longer limited to administrative issues but is closely related to cybercrime risks within the digital ecosystem. This study aims to analyze the legal liability of online lending providers for personal data violations and to evaluate the effectiveness of data protection regulations in addressing cybercrime. The research employs a normative juridical approach through the analysis of legislation, scholarly literature, and case studies involving the misuse of personal data in online lending services. The findings show that online lending providers, as personal data controllers, bear administrative, civil, and criminal liability in cases of negligence in safeguarding user data. The main challenges in personal data protection include weaknesses in regulatory supervision, complexities in digital evidence procedures, and the low level of public digital literacy.

Keywords: Personal Data Protection, Online Lending, Cybercrime, Legal Liability.

Corresponding Author:
Rizal Abidin
Informatics Engineering Study Program, Muhammadiyah University of Science and Technology, Jakarta, Indonesia
abidinrizal032@gmail.com

1. Introduction

The development of digital technology has also encouraged changes in the pattern of public interaction with information-based systems, so the use of digital services requires users to be prepared to understand aspects of data security and responsible use of technology (Nur Kumala Dewi, 2021).

Digital transformation has driven significant changes in the financial services sector through the development of financial technology (fintech), particularly online lending services. The ease of access and fast processes have made these services widely used by the public, but at the same time have increased the risk of violations of users' personal data (Hidayat et al., 2025).

Online lending providers collect various sensitive data such as personal identities, phone contacts, and users' financial information. The large-scale use of such data increases the potential for data breaches and misuse, which can lead to economic losses as well as psychological pressure on victims (Anggraini & Wiraguna, 2025).

The development of cybercrime has become increasingly complex due to its anonymous and cross-jurisdictional nature, making the legal proof process more difficult compared to conventional crimes (Aini & Lubis, 2024). Globally, personal data protection has become an important element in digital economic governance, emphasizing the active responsibility of electronic system providers from the system design stage (Albrecht, 2022). Unlike previous studies, this research positions personal data protection as a preventive approach in combating cybercrime within online lending services.

 ISSN 2828-9463

2. Methods

This study uses a normative juridical research method, which is a legal research approach that places law as norms or rules applicable within the system of statutory regulations. This approach is used to analyze the legal responsibility of online lending providers in protecting personal data and its relevance to combating cybercrime in Indonesia. The main focus of this research is directed at examining legal norms, principles of personal data protection, and their implementation in digital service practices.

Research Approach

This research employs several approaches as follows:

a. Statutory Approach
This approach is conducted by examining various regulations related to personal data protection and electronic systems in Indonesia, particularly the Personal Data Protection Law and the Electronic Information and Transactions Law along with its amendments. The analysis is carried out to determine the legal position of online lending providers and the forms of legal liability that can be imposed in cases of data misuse.

b. Conceptual Approach
The conceptual approach is used to examine legal doctrines and concepts developed in academic literature, such as the concepts of legal liability, privacy protection, cybersecurity, and principles of personal data control. This approach helps provide a theoretical framework for understanding the relationship between the development of digital technology and changes in the concept of legal protection.

c. Case Approach
The case approach is used through the analysis of the phenomenon of personal data misuse in online lending services in Indonesia. Case studies are conducted to examine the conformity between applicable legal norms and practices occurring in society, thereby enabling the effectiveness of legal protection to be analyzed in a real context.

Types and Sources of Data

The type of data used in this research is secondary data, obtained through literature study. The secondary data consist of:

1. Primary Legal Materials, including:
   a. Law Number 27 of 2022 concerning Personal Data Protection,
   b. Law Number 11 of 2008 concerning Electronic Information and Transactions along with its amendments through Law Number 1 of 2024
   c. Regulations and policies related to cybersecurity and fintech services.
2. Secondary Legal Materials, including:
   a. national and international scientific journals,
   b. previous research findings,
   c. academic literature discussing personal data protection, fintech, and cybercrime.
3. Tertiary Legal Materials, including:
   a. legal reference books,
   b. legal dictionaries,
   c. and other supporting sources that help in understanding the research concepts.

Data Collection Technique

Data collection is conducted through library research by identifying, reading, and reviewing various legal documents and scientific literature relevant to the research topic. This process is carried out systematically to obtain a comprehensive understanding of regulations and the development of personal data protection concepts.

Data Analysis Technique

Data analysis is conducted qualitatively using the legal interpretation method. The stages of analysis include:

a. Identifying legal norms governing personal data protection.
b. Interpreting legal provisions related to the responsibility of electronic system providers.
c. Comparing legal norms with the practice of data misuse in online lending services.
d. Drawing deductive conclusions based on the relationship between legal theories and the analyzed facts.

This analytical approach aims to produce a comprehensive understanding of the effectiveness of legal protection for personal data in addressing the development of cybercrime.

3. Result and Discussion

Legal Position of Online Lending Providers as Personal Data Controllers

The development of online lending services reflects a paradigm shift in financing activities, where personal data has become a primary component in digital business processes. Unlike conventional financial institutions that rely on physical documents, application-based services depend on electronic data processing as the basis for credit decision-making. This condition places personal data in a strategic position while simultaneously making it vulnerable to misuse.

From the perspective of personal data protection law, online lending providers can be positioned as personal data controllers because they have the authority to determine the purposes and methods of processing users' data. This position creates legal consequences in the form of obligations to maintain the security, confidentiality, and use of data in accordance with the initial purpose of its collection.

The legal responsibility of providers does not only arise when a data breach occurs, but also when the system used is not designed to prevent the risk of misuse from the outset. In other words, negligence in building an adequate security system can be considered a violation of legal obligations. This principle indicates that personal data protection is preventive in nature, not merely repressive.

In practice, the relationship between users and digital service providers is often unequal. Users are typically in a position where they must accept terms of use without having the ability to negotiate the data access requested by applications. As a result, consent to data usage often becomes an administrative formality rather than consent truly based on full understanding. This phenomenon shows that personal data protection does not depend solely on regulation, but also on technology system design and the transparency of digital service providers.

Misuse of Personal Data as a Form of Cybercrime

The misuse of personal data in online lending services reflects the characteristics of modern cybercrime that utilizes electronic systems as its primary means. Unlike conventional crimes, data violations often occur without physical contact between perpetrators and victims, so the impact is usually felt only after personal information has been disseminated or used unlawfully.

Data breaches within the digital ecosystem can occur through various mechanisms, including excessive application access, weak system security, or the use of data beyond its original processing purpose. In the context of online lending, data initially used for identity verification is often utilized as a tool of pressure during the debt collection process.

From a cyber law perspective, the dissemination of personal information without authorization constitutes the use of electronic systems in violation of individual rights. The complexity of this crime lies in the nature of digital evidence, which can easily be altered and is difficult to trace, making the evidentiary process require both technical and legal approaches simultaneously (Aini & Lubis, 2024).

In addition, technological developments show that security threats do not always originate from external attacks. Many data violations actually occur due to weaknesses in internal governance, such as unrestricted data access management or insufficient supervision of how internal parties use user information. This condition demonstrates that data security cannot be understood solely as a technological issue, but also as a matter of organizational governance.

Challenges in Law Enforcement for Personal Data Protection

Although the regulatory framework already exists, the implementation of personal data protection in practice still faces various challenges. One of the main obstacles is the gap between the rapid development of digital technology and the readiness of law enforcement authorities in handling electronic evidence.

The characteristics of digital data, which can easily be transferred and stored on servers across different countries, often create jurisdictional issues in law enforcement processes. Perpetrators of violations may be located in different legal jurisdictions from the victims, requiring coordination among institutions and cross-border cooperation.

Apart from technical aspects, the low level of digital literacy in society also increases the risk of data violations. Many users do not fully understand the consequences of granting application access permissions to their personal data, thereby unintentionally opening opportunities for information misuse. Law enforcement approaches that are purely repressive are often insufficient to address this issue. Preventive efforts through digital security education and limiting access to relevant data are important steps to reduce potential violations from the outset.

Analysis of Legal Liability Based on Indonesian Case Studies

Case studies of data misuse in online lending services in Indonesia show that data violations often occur through the use of users' contact lists as a means of pressure during the debt collection process. This practice demonstrates the use of data beyond its original processing purpose.

Within the framework of personal data protection law, such actions can be categorized as violations of the principles of purpose limitation and data confidentiality. Data controllers have an obligation to ensure that user information is not used for other purposes without legitimate consent.

In addition to administrative responsibility, such violations may also give rise to civil lawsuits in the form of compensation for damages suffered by victims. If the dissemination of data is intentionally carried out through electronic systems, the act may also be analyzed as a cybercrime offense as regulated in electronic information and transaction regulations (Republic of Indonesia, 2024). This analysis shows that the legal responsibility of online lending service providers is multi-layered, encompassing administrative, civil, and criminal liability simultaneously.

Theoretical Implications for Personal Data Protection in the Fintech Ecosystem

The results of the discussion indicate that personal data protection in online lending services can no longer be understood solely as an issue of protecting individual privacy, but rather as part of the development of legal theory in responding to digital transformation. Changes in technology-based social and economic interactions have caused personal data to shift from merely representing individual identity to becoming a core element of the digital economic system.

Theoretically, this condition expands the concept of legal responsibility from a traditional approach oriented toward unlawful acts to a risk-based regulation approach. In digital services, legal responsibility arises not only after losses occur but also includes preventive obligations through secure system design from the beginning of operations.

Another implication is the change in legal relationships between business actors and digital service users. In classical contractual concepts, parties are considered equal; however, in the digital ecosystem there is significant information asymmetry. Users often do not fully understand the mechanisms of data processing conducted by electronic systems. This indicates that consumer protection theory in the digital realm needs to evolve toward a user vulnerability approach.

Furthermore, this study shows that personal data protection is closely related to modern cybersecurity theory, which places security as part of system governance rather than merely an additional technical safeguard. This concept shifts the legal paradigm from a reactive approach to a preventive one, where law functions as an instrument for managing technological risks.

From the perspective of technology law theory, the phenomenon of online lending shows that regulation is no longer sufficient to regulate only human behavior but must also guide the design of the technology itself. Thus, law functions as both a mechanism of social control and a governance framework for digital innovation. These theoretical implications emphasize that personal data protection in the digital economy requires integration between law, technology, and organizational governance, making a multidisciplinary approach essential for ensuring that regulations can keep pace with technological development without hindering innovation.

Practical Implications and Policy Recommendations

The research findings show that problems in personal data protection within online lending services are not only caused by regulatory weaknesses but also by suboptimal implementation of electronic system governance. Therefore, practical measures are required to bridge legal norms with operational practices in digital services. From the regulator's perspective, supervision should not only focus on licensing aspects but also on the implementation of data protection standards in application systems, including limiting access to user information to prevent misuse from the operational stage.

For fintech providers, data protection should become part of risk management through technological design that applies the principle of data minimization and transparent privacy policies so that users clearly understand the purpose of data processing. From a law enforcement perspective, improving the capacity of authorities in digital forensics is crucial considering the complexity of proving data violations in electronic systems. Additionally, increasing public digital literacy is necessary as a preventive measure to reduce the risk of personal data exploitation. Based on the research findings, policy recommendations include:

1. Strengthening data security standards in online lending services.
2. Limiting access to irrelevant data.
3. Increasing supervision of illegal applications.
4. Strengthening the digital forensic competence of law enforcement officers.

5. Developing digital literacy programs related to personal data security.

A collaborative approach involving regulators, industry, law enforcement, and society is essential to ensure effective personal data protection in practice.

Overall Discussion

Based on the overall discussion, it can be understood that the issue of personal data protection in online lending services is not merely related to individual legal violations but reflects changes in the structure of legal relationships within the digital ecosystem. The use of data as the operational basis of technology-based financial services places electronic system providers in a position of broader legal responsibility compared to conventional business models.

Case studies in Indonesia show that weaknesses in data protection often arise from a combination of technology design, operational practices, and users' limited understanding of digital risks. Therefore, personal data protection must be understood as a preventive digital risk governance mechanism, not merely as a law enforcement instrument applied after violations occur. This understanding forms the basis for the research conclusions regarding the importance of strengthening regulation, supervision, and digital literacy as integral parts of combating cybercrime.

Case Study

The development of online lending services in Indonesia has not only provided easier access to financing but has also generated various cases of personal data misuse by illegal online lending providers. One phenomenon widely reported by the public occurred during the 2019–2023 period, when several online lending applications used excessive access to users' device data and utilized it as a means of pressure during debt collection.

Based on public complaint reports submitted to the Financial Services Authority (OJK) and the Investment Alert Task Force, many victims experienced the dissemination of personal data such as contact lists, identity photos, and loan information to other parties without consent. This practice usually occurred when users experienced payment delays, where debt collectors contacted or even spread debt information to colleagues, family members, or other contacts stored on the user's device.

One widely highlighted example involved illegal online lending applications requesting access to phone contacts and device storage during the installation stage. Users in urgent need of funds tended to approve all access requests without understanding the implications of such data usage. Once the loan was active, the collected data was used to conduct digital intimidation through mass messages or calls to third parties.

From a legal perspective, these actions demonstrate violations of personal data protection principles, particularly the principles of purpose limitation and valid consent. Data initially collected for credit verification purposes was used beyond its original objective, thereby violating the privacy rights of individuals as data subjects. This practice may also be categorized as a form of cybercrime, as it utilizes electronic systems to cause harm to victims.

The impacts include not only financial losses but also psychological pressure, social reputation damage, and a loss of trust in digital services. Some victims reported experiencing stress, social intimidation, and even workplace disruptions due to the widespread dissemination of debt information.

This phenomenon indicates that the primary issue lies not only in the existence of regulations but also in weak supervision of illegal applications and the low level of digital literacy among the public. Many users do not fully understand the consequences of granting data access permissions to digital applications, making them vulnerable to personal data exploitation. Based on this case study analysis, personal data protection in online lending services requires a multidimensional approach, including:

a. Strengthening supervision of illegal fintech applications.
b. Limiting data access to information relevant to service purposes.
c. Implementing the privacy by design principle in digital application development.
d. Providing public digital literacy education on personal data security.
e. Increasing law enforcement capacity in investigating cybercrime.

This case study in Indonesia shows that personal data protection is not only a matter of legal compliance but also closely related to technology governance and user awareness within the digital economic ecosystem.

4. Conclusion

Based on the research findings, it can be concluded that the development of online lending services as part of the financial technology ecosystem has resulted in an increased risk of personal data breaches, potentially leading to cybercrime. Online lending providers are legally obligated to ensure the security, confidentiality, and use of data in accordance with legitimate processing purposes. Violations of these obligations can result in administrative, civil, and criminal legal liability.

The discussion shows that issues with personal data protection are not solely caused by regulatory weaknesses but also by implementation factors, such as system design that is not yet oriented toward data security, weak oversight of illegal applications, and low digital literacy among the public. The complexity of proving evidence in cybercrime also poses a challenge to law enforcement, particularly due to the cross-jurisdictional nature and ease of manipulation of digital evidence.

Case studies in Indonesia demonstrate that misuse of personal data in online lending services often occurs through excessive data access and the use of user information beyond the original processing purposes, particularly in collection practices. This situation demonstrates that personal data protection needs to be understood as a digital risk prevention mechanism, not simply a law enforcement tool after a violation occurs.

Therefore, it is necessary to strengthen regulatory oversight, implement data protection principles from the system design stage (privacy by design), increase the capacity of law enforcement officers in digital forensics, and develop public digital literacy. Synergy between regulators, service providers, law enforcement officers, and the public is key to achieving effective personal data protection while supporting the development of a safe and equitable digital economy ecosystem in Indonesia.

5. References

Aini, N., & Lubis, F. (2024). Tantangan pembuktian dalam kasus kejahatan siber di Indonesia. *Jurnal Hukum Teknologi Informasi*, 6(1), 45–58.

Albrecht, J. P. (2022). Data protection and accountability in the digital economy. *International Data Privacy Law*, 12(3), 189–201. https://doi.org/10.1093/idpl/ipac012

Anggraini, N. F., & Wiraguna, S. A. (2025). Tanggung jawab hukum platform pinjaman online terhadap penyalahgunaan data pribadi. *Jurnal Hukum dan Pembangunan*, 55(1), 112–128.

Borgesius, F. Z. (2021). Privacy protection in the age of digital platforms. *Computer Law & Security Review*, 41, 105–118. https://doi.org/10.1016/j.clsr.2021.105566

Hidayat, E. R., Prasetyo, A., & Kurniawan, D. (2025). Perlindungan hukum bagi korban pinjaman online ilegal di Indonesia. *Jurnal Legislasi Indonesia*, 22(1), 67–82.

Kshetri, N. (2023). Cybercrime and cybersecurity challenges in fintech ecosystems. *Journal of Cyber Policy*, 8(2), 214–230. https://doi.org/10.1080/23738871.2023.2172456

Martin, K., & Shilton, K. (2022). Why experience matters to privacy: Context-based privacy expectations and regulation. *Journal of Business Ethics*, 175(3), 599–612. https://doi.org/10.1007/s10551-020-04636-4

Nisa, R., Rahmawati, L., & Putra, H. (2025). Literasi digital dan perlindungan data pribadi masyarakat Indonesia. *Jurnal Komunikasi Digital*, 9(1), 25–39.

Dewi, N. K. (2021). Review of vehicle surveillance using IoT in the smart transportation concept. *International Journal of Engineering and Manufacturing*, 11(1), 1–10.

OECD. (2023). *Enhancing access to and sharing of data: Reconciling risks and benefits for data reuse across societies*. Paris: OECD Publishing.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Jakarta: Sekretariat Negara.

Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan atas Undang-Undang Informasi dan Transaksi Elektronik*. Jakarta: Sekretariat Negara.

UNCTAD. (2024). *Data protection and privacy legislation worldwide*. Geneva: United Nations Conference on Trade and Development.

World Bank. (2022). *Digital financial services and consumer protection in emerging economies*. Washington, DC: World Bank Group.