E-ISSN : 2963-4946
Vol. 2 No. April 07, 2024
Asian Journal of Social and Humanities
https://ajosh.org/

Legal Protection of Consumer Personal Data In Online Loan Transactions

Redi Rahadian Bagaskara
Universitas Pancasila, Indonesia
E-mail: redirahadianbagas27@gmail.com

***Correspondence:** redirahadianbagas27@gmail.com

KEYWORDS
finance, online loans, protection

ABSTRACT
The financial sector, especially through online loan applications, has seen new opportunities thanks to technological advances, especially in the field of communications. Although online loans are easy to use, they also present risks regarding personal data security and unsafe lending practices. Along with the popularity of online loans, crimes in the digital world, such as data theft and misuse of information, are increasing. Although vulnerable to detrimental lending practices, especially illegal loans that have not been registered with the Financial Services Authority (OJK), people with low incomes see online loans as an attractive option. The aim of this research is to study how the protection of consumer personal data in online loan transactions is protected by law, especially considering the phenomenon of violations and unprofitable lending practices. This research examines how Law no. 27 of 2022 concerning Personal Data Protection (UU PDP) protects personal data and how it impacts borrowers socially and psychologically. This research shows regulatory and practical innovation in dealing with the problem of personal data leakage which is detrimental to consumers when borrowing money via the internet. Through regulatory analysis and case studies, this research is expected to provide insight into how effective personal data protection is in online loan transactions. Therefore, this research helps build better regulations and efforts that protect customers in the ever-growing era of online lending.

Introduction

The protection of consumers' personal data in online loan transactions must be strictly regulated in accordance with the Personal Data Protection Law. Consumers have the right to privacy and security of their personal data collected by online lending companies (Abdul-Rahman & Habib, 2019). Companies must ensure that consumers' personal data is stored securely and not misused. Violation of the privacy of consumers' personal data may result in legal sanctions for the company concerned. So, it is important

for online loan companies to comply with regulations related to consumer personal data protection (Ali, 2018).

The presence of peer to peer lending system in Indonesia has a positive impact on the community, especially for those who live in remote areas (Asikin, 2012). Some of the positive impacts of this system include:

Facilitate Financial Access: People in remote areas can easily access loan services through online loan applications without having to go to a physical bank office.

Increased Ability to Operate: With easier access to loans, residents in remote areas can start businesses or expand existing businesses.

Improving Financial Inclusion: Peer to peer lending helps increase financial inclusion in remote areas by providing access to financial services that were previously difficult to reach (Miru et al., 2020).

Local Economic Development: With more accessible loans, it is expected to help strengthen the local economy in remote areas (Nasution, 2015).

Increased Employment Opportunities: With funding easier to obtain, people in remote areas can open up new job opportunities so as to reduce unemployment in the area (Gozali & Usman, 2022).

Thus, the peer to peer lending system contributes positively to economic development and financial inclusion in Indonesia, especially for people in remote areas (Islami, 2021).

Information Technology Security Challenges in Personal Data Protection Cannot Be Denied The advancement of information technology has brought new challenges related to personal data security (Nurmantari & Martana, 2019). Some examples of identified crimes related to information technology include:

1. Carding (credit card fraud)
2. ATM/EDC skimming
3. Hacking
4. Cracking
5. Phishing (internet banking fraud)
6. Malware (viruses/worms/trojans/bots)
7. Cybersquatting
8. Pornography
9. Online gambling
10. Transnational crime (drug trafficking, mafia, terrorism, money laundering, human trafficking, underground economy)

The potential for crime also increases in the data and information management sector, especially in the management of personal data that requires protection (Mahmud Marzuki, 2018). Privacy boundaries are getting thinner as personal data becomes more easily dispersed (Turkington & Allen, 2022).

To overcome these challenges, it is important to implement strict data security measures, such as data encryption, the use of strong firewalls, multi-factor security systems, as well as training for employees on information security (Dewi, 2019). In addition, clear and strict regulations related to personal data protection are also needed to protect consumers from misuse of their data (Nurmantari & Martana, 2019). With the right measures, it is expected to reduce the risk of crimes related to information technology and personal data protection. People with low incomes tend to use online loans because of their fast access and easy conditions. However, online loans are vulnerable to predatory lending practices, especially on illegal loans that are not registered

with the OJK (Mahmud Marzuki, 2018). The issue of personal data theft is increasing along with the increase in the use of mobile phones and the internet. Although banks and non-bank lending institutions are an option, people often choose online loans even though the interest charged is higher (Poerwadarminta, 2016). Problems arise regarding aggressive billing methods and contract transfer. Consumer personal data protection is still low because lenders can access mobile phone transactions and consumer photos. It is important to address these issues so that consumers get adequate legal protection in online loan transactions. Harmful practices in online loan services can have a negative social and psychological impact on borrowers (Chatfield, 2021). The dissemination of personal and sensitive information can cause shame and suffering, especially if known by the surrounding environment. The relationship between online loan service providers and borrowers is a civil relationship that must be properly regulated to protect the rights and privacy of borrowers (Soekanto & Mamudji, 2013). It is important to implement strong personal data protection in the online lending industry to prevent negative impacts that can harm borrowers. The online loan agreement must be clear in determining the promised performance and how to implement it so as not to harm both parties. Many online loan application services are not legally registered with the Financial Services Authority, which can result in harmful practices for debtors (Rosadi, 2015). For example, misuse of the debtor's personal data for unethical collection, such as through WhatsApp by leaking the debtor's personal information to other parties. Debtors often feel embarrassed and annoyed by this way of inappropriate collection, which can ultimately cost them money. It is important to protect debtors from unethical and harmful collection practices in online loan transactions.

The protection of personal and consumer data in online loans according to Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) aims to protect the types of personal data which are divided into general data and special data. Personal data includes information such as full name, gender, nationality, religion, and data used to identify an individual. Personal data subjects have the rights stipulated by the PDP Law in Articles 5 to 15 (Nugraha, 2012).

Online loans are increasingly becoming public attention because cases of violations by online lending institutions continue to appear in the mass media. Violations committed by online loans can be in the form of intimidative collection, dissemination of personal data, fraud, to sexual harassment through electronic media. Some cases even lead to customer suicide tragedies due to pressure from loan collection (Mahfuz, 2021).

Legal problems related to online loans are still minimally resolved, so similar cases continue to arise. Online borrowers, who are also consumers and owners of data, need to have their legal interests protected in every transaction so as not to fall victim to harmful practices in the online lending industry. It is important to implement strict regulations and strong law enforcement to protect personal data and consumer rights in online loan transactions.

In this study, the author will focus on legal protection of consumer personal data in online loan transactions, which are often misused by online loan service providers. This research will also compare changes in the Law from the oldest to the latest, referring to Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems, Consumer Protection Law No. 8 of 1999, Law No. 19 of 2016 concerning Electronic Information and Transactions, and Law No. 27 of 2022 concerning Personal Data Protection.

The research method used is normative law with a statute approach and a conceptual approach, especially to overlapping regulations. The purpose of this study is to identify the main problems related to problems between online loan application service providers and consumers / users of these services.

This study aims to provide deeper insight into the right to protection of consumer personal data in the context of online loan transactions, as well as see the impact of changes in legislation on consumer personal data protection. It is expected that this research can make a positive contribution in dealing with problems related to online loans and protecting consumer interests in online loan transactions.

Research Methods

This writing uses normative juridical methodology research methods, normative juridical methodology is used to approach the problem under study from a normative legal point of view. The normative approach involves legal principles, comparative laws, as well as historical reviews that outline norms, articles of legislation related to the topic under investigation.

The statute approach is used to examine laws and regulations that still have shortcomings or may foster deviant practices, both in technical aspects and their implementation in the field. This approach involves an analysis of all laws and regulations related to the legal issue being studied.

With this approach, researchers will examine consistency and compatibility between various related laws, regulations, and Constitutions. Law is viewed as a closed system with the following properties:

1. Comprehensive, meaning that legal norms are logically interrelated.
2. All-inclusive, so that these legal norms are able to solve all legal problems without flaws.
3. Systematic, because legal norms are arranged systematically and coordinated.

The conceptual legal approach is a type of approach in legal research that analyzes the resolution of this problem from the point of view of the legal concepts behind it. This approach may also involve an assessment of the values contained in legal regulations related to the concepts used. This approach is based on the views and doctrines that exist in legal science. The selection of approaches in conceptual legal research is carried out to find answers to available legal issues. The compatibility between the chosen approach and the legal issues studied is the main consideration in determining the approach to be used. In addition to conceptual legal approaches, there are also other approaches that are often used in normative legal research.

Results and Discussions

Research on the Protection of Borrowers' Personal Data in Online Loan Application Services

First Research:

Title: Legal Protection of Personal Data of Borrowers in Online Loan Application Services

Author: Ni Nyoman Ari Diah Nurmantari

Method: Normative law with statutory approach and fact approach

Problem Statement:

What is the legal protection of borrowers' personal data in online loan application services?

What are the penalties for personal data breaches?

Legal References: Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions, and POJK No. 77/POJK.01/2016 concerning Information Technology-Based Money Lending and Borrowing Services

Second Study:

Title: The Urgency of Legal Protection of Borrowers' Personal Data in Online Loan Application Services

Author: Oktaria Wim Kusuma

Method: Statute approach with normative analysis techniques using deductive methods

Discussion:

Legal Protection of Borrowers' Personal Data in Online Loan Application Services

Legal Protection Efforts Against Misuse of Borrower's Personal Data in Online Loan Application Services

Both studies contribute to analyzing the protection of borrowers' personal data in online loan application services as well as providing insight into the urgency of legal protection of personal data in the context of online loan transactions.

CONSUMER PROTECTION THEORY IN PERSONAL DATA PROTECTION

Consumer protection theory in personal data protection emphasizes the importance of privacy policies governing the collection, storage, processing, and protection of consumer personal data. Consumers should have control over their personal information, including the right to access, correct, and delete such data. In this context, the positions of consumers and producers should be on an equal footing, where consumers have the right to resist the arbitrary actions of producers.

Consumer protection also requires the role of the government in enforcing laws related to actions that harm consumers. The government has an important role to play in policing the actions of producers who are dishonest with consumers.

Privacy policies should also govern companies' use of consumers' personal data, ensuring data is only used for approved purposes and is not misused or sold to third parties without permission. Security measures should also be implemented to protect data from unauthorized access or leakage.

In a legal context, privacy policies must comply with applicable data protection regulations and laws. In Indonesia, there are several regulations governing the protection of consumer personal data, such as Law No. 19 of 2016, Government Regulation No. 71 of 2019, and Regulation of the Minister of Communication and Information of the Republic of Indonesia No. 20 of 2016.

With a clear privacy policy and in accordance with applicable regulations, it is expected that consumers can feel safe and confident when transacting online, while companies can maintain their trust and reputation in the protection of consumers' personal data. Consumer protection theory is used to provide legal protection for individuals or consumers in a variety of contexts, ensuring that the rights and interests of individuals are protected fairly and securely.

THEORY OF LEGAL REASONING IN PERSONAL DATA PROTECTION

Legal reasoning theory is an important method in ensuring legal compliance, protection of individual rights, and continuity of the process of processing personal data in accordance with applicable rules. The starting point of MacCormick's theory of legal reasoning is to identify the role of reasoning in the process of applying law, with the aim of providing an objective explanation of the judge's actions and justifying decisions.

Legal reasoning in the context of personal data protection is important to ensure that the continuity of the data processing process is carried out correctly and in accordance with applicable regulations. In Indonesia, the theory of legal reasoning in personal data protection can be related to consumer protection, which aims to provide protection to individuals from potentially harmful practices in online transactions, such as online loans.

In the legal realm, personal data protection in Indonesia can be strengthened by referring to the principles of legal reasoning underlying privacy and data protection rights. Thus, the implementation of this practice is not only limited to compliance with regulations, but also about respect for individual rights, as well as having a positive impact on overall social and economic development.

FORMS OF CONSUMER PERSONAL DATA PROTECTION FROM THE RISK OF PERSONAL DATA LEAKAGE

1. **Clear Privacy Policy**: Implement a transparent and clear privacy policy regarding the collection, storage, processing, and use of consumers' personal data.
2. Access Control and Authorization: Ensure that only authorized parties can access consumers' personal data and apply appropriate levels of authorization.
3. **Data Encryption**: Uses encryption technology to protect consumers' personal data as it is stored, processed, and transmitted.
4. **Security Monitoring**: Conduct continuous security monitoring to detect security threats and suspicious actions against personal data.
5. **Employee Training**: Provide training to employees on the importance of keeping consumers' personal data secure and the steps to follow to protect that data.
6. **Data Destruction Policy**: Establish a data destruction policy that is no longer necessary or relevant to prevent misuse of consumers' personal data.
7. **Data Security Audits**: Conduct periodic audits to ensure compliance with data security policies and identify potential vulnerabilities that need to be fixed.
8. **Data Recovery**: Develop a data recovery plan in case of personal data leakage to minimize the negative impact on consumers.
9. **Cooperation with Supervisory Authorities**: Collaborate with data supervisory authorities to report data leaks and follow established procedures for handling data security incidents.
10. **Increased Consumer Awareness**: Educating consumers about the importance of personal data protection, how to protect their personal information, and actions to take in dealing with data leakage risks.

FORM OF RESOLVING CONSUMER PERSONAL DATA LEAKAGE FROM THE RISK OF PERSONAL DATA LEAKAGE

1. **Notice to Consumers**: Provide notice to consumers regarding leakage of personal data that occurs so that they can take the necessary protective measures.
2. **Internal Investigation**: Conduct an internal investigation to determine the cause of the personal data leak and determine the corrective steps to be taken.
3. **Report to the Relevant Authority**: Report leakage of personal data to the competent data supervisory authority in accordance with applicable regulations.
4. **Data Recovery**: Take steps to recover data affected by personal data leakage and ensure no further damage.
5. Law Enforcement: If necessary, engage law enforcement to crack down on perpetrators of personal data leakage and ensure justice for affected consumers.
6. **Enhanced Data Security**: Improves data security systems to prevent future leakage of personal data by identifying and addressing existing vulnerabilities.

7. **Compensation to Consumers**: Provide compensation to consumers affected by leakage of personal data as a form of fair compensation for the losses they have suffered.
8. **Transparency and Accountability**: Maintain transparency in resolving personal data leaks, including providing information to the public about the measures taken and ensuring accountability in handling such incidents.
9. **Reputation Restoration**: Make efforts to restore the company's reputation after a personal data leak by providing assurance to consumers that steps have been taken to prevent similar things from happening in the future.
10. **Supervision and Evaluation**: Conduct regular supervision and evaluation of the data security system to ensure the effectiveness of measures to resolve personal data leakage and prevent the recurrence of similar incidents.

Legal Protection for Consumers in Online Loan Services: Article 1313 K of Law No. 8 of 1999 concerning Consumer Protection states that consumers have the right to security in using goods and/or services produced and/or traded.

Legal Relationship in Agreement: Article 1313 K of Law No. 8 of 1999 also affirms that the legal relationship between consumers and service providers must be based on a valid and fair agreement for both parties.

Conclusion

The research on "Legal Protection of Consumer Personal Data in Online Loan Transactions" by Redi Rahadian Bagaskara from Universitas Pancasila, Indonesia, presents an in-depth analysis of the issues surrounding personal data security and unsafe lending practices in the online loan industry. The conclusion of this study highlights the urgency of implementing strict regulations and enforcing strong law enforcement to protect consumer personal data in online loan transactions. In addressing the threats of information security and the risks of cybercrimes, the research emphasizes the need for stringent data security measures and clear regulations. Additionally, it underscores the negative social and psychological impacts of detrimental lending practices in online loan services and emphasizes the importance of protecting consumer personal data to mitigate these effects. By adopting normative legal methodology and a conceptual approach, the research provides a comprehensive understanding of the legal framework governing online loan transactions and the associated challenges and risks. Identifying legal issues and providing recommendations to enhance regulatory frameworks and consumer protection, this research offers valuable contributions to the understanding and further development in this field.

References

Abdul-Rahman, A. A., & Habib, S. A. (2019). Allelopathic effect of alfalfa (Medicago sativa) on bladygrass (Imperata cylindrica). *Journal of Chemical Ecology*, *15*, 2289–2300.

Ali, A. (2018). *Menjelajahi kajian empiris terhadap hukum*. Yarsif Watampone.

Asikin, Z. (2012). Pengantar Tata Hukum Indonesia. *Jakarta: PT Raja Grafindo Persada*.

Chatfield, T. (2021). How to Think: Your Essential Guide to Clear, Critical Thought. *How to Think*, 1–100.

Dewi, S. (2019). Cyberlaw Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional. *Bandung: Widya Padjajaran*.

Gozali, D. S., & Usman, R. (2022). Hukum perbankan. *(No Title)*.

Islami, M. J. (2021). Implementasi Satu Data Indonesia: Tantangan dan Critical Success Factors (CSFs). *Jurnal Komunika: Jurnal Komunikasi, Media Dan Informatika*, *10*(1), 13–23.

Mahfuz, A. L. (2021). Analisis Resiko Hukum Eksistensi Bisnis Pinjaman Online di Indonesia. *Doctrinal*, *6*(2), 110–122.

Mahmud Marzuki, P. (2018). Pengantar Ilmu Hukum. *Kencana, Jakarta*.

Miru, A., Pati, S., Anshori, A. G., Asshiddiqie, J., Safa'at, M. A., & Badrulzaman, M. D. (2020). *DAFTAR PUSTAKA BUKU*.

Nasution, A. Z. (2015). *Konsumen dan hukum: tinjauan sosial ekonomi dan hukum perlindungan konsumen Indonesia*.

Nugraha, R. A. (2012). *Analisis yuridis mengenai perlindungan data pribadi dalam cloud computing system ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik= Juridical analysis concerning the personal data protection in the cloud computing system from the Law of Infor*.

Nurmantari, N., & Martana, N. A. (2019). Legal Protection of Borrower's Personal Data in Online Loan Application Services. *Kertha Wicara: Journal of Legal Studies*, *8*, 1–14.

Poerwadarminta, W. J. S. (2016). Kamus Umum Bahasa Indonesia, edisi III, cet. 3. *Jakarta: Balai Pustaka*.

Rosadi, S. D. (2015). Cyber Law-Aspects of Data Privacy According to International, Regional and National Law. *Refika Aditama*.

Soekanto, S., & Mamudji, S. (2013). Penelitian Hukum Normatif Suatu Tinjauan. *Singkat, Jakarta: CV. Rajawali*.

Turkington, R. C., & Allen, A. L. (2022). Privacy law: Cases and materials. *(No Title)*.