Model of Regulation for Personal Data Protection of Online Loan Consumers Based on Maqasid Syariah and Personal Data Protection Law No. 27 of 2022

Rahmat Setiyadi[1*], Ilham Abdi Prawira [2], Cici Sundari[3], Herri Novealdi[4]

rahmadsetiyadi2@gmail.com, ilhamabdiprawira@uinjambi.ac.id, cicisundari@uinjambi.ac.id, herrinovealdi@uinjambi.ac.id

[1234]Sultan Thaha Saifuddin State Islamic University of Jambi, Indonesia

Article Info

Received: 2022-11-20
Revised: 2023-01-20
Accepted: 2023-03-22

Keywords:
Personal Data, Online Loans, Consumer Protection, Maqasid Syariah, PDP Law.

Abstract

This study aims to analyze the Model of Regulation for the Protection of Personal Data of Online Loan Consumers Based on Maqasid Syariah and the No. 27 Of 2022 Personal Data Protection Law. This research employs a qualitative method with a normative juridical approach, utilizing primary data in the form of the PDP Law, as well as secondary data from social media and relevant journals. The analysis was carried out using NVivo 12 Plus to systematically process qualitative data through word, frequency, and attribute analysis. The study's results demonstrate that the PDP Law provides a robust legal framework for protecting the rights of data subjects, including the right to privacy, security, and control over their personal data. This law emphasizes that online loan providers are required to obtain the user's explicit consent before processing their data (Articles 15–20) and provide consumers with the right to access, correct, or delete their personal data (Article 16). The PDP Law also provides for administrative and criminal sanctions for violations, including hefty fines and imprisonment (Articles 57–63), to ensure transparent, fair, and accountable data management. From the perspective of Maqasid Sharia, the protection of personal data aligns with the principles of hifz al-nafs (protection of life), hifz al-'aql (protection of reason), and, in particular, hifz al-'irdh (protection of honor). Violations of personal data are viewed as a violation of human honor and dignity, which is contrary to the values of Justice and benefit in Sharia. Thus, the protection of personal data of borrowed consumers reflects the synergy between positive law and Islamic ethical principles.

I. Introduction

The development of digital technology in the modern era has changed almost all aspects of human life. Digitalization not only affects the patterns of social interaction and communication but also has a significant impact on the global financial sector. One of the most prominent innovations is the presence of *financial technology* (*Fintech*) that combines financial services with digital technology to create a faster, more efficient, and more inclusive financial system. This phenomenon then spread to various countries, including Indonesia, which has witnessed the rapid growth of application-based loan services, also known as online loans (pinjol) (Diana et al., 2024). Online loans are proliferating because they provide people with easy and fast access to financing. Through internet-based applications, people can obtain funds without the need for physical guarantees or the complicated procedures typically encountered in conventional financial institutions. This advantage makes Pinjol a sought-after alternative financing option, particularly for those who lack access to formal banking services. The high number of loan users in Indonesia demonstrates how this service has become a practical financial solution considered by most people (Scott et al., 2025).

However, behind the convenience offered, the practice of online lending presents various serious problems that cannot be ignored. One of the most prominent issues is the misuse of consumers' personal data. Personal data that should be protected is often misused by loan operators, especially when customers experience delays or defaults. It is not uncommon for customer personal data to be disseminated to third parties or even published to the public space as a form of pressure and intimidation. This kind of practice is clearly contrary to the principles of legal, ethical, and human rights protection (Syaiful & Sugiyono, 2024). The misuse of personal data not only has a legal impact but also causes social and psychological harm. Many victims of loans experience stress, mental distress, and loss of reputation in the family and community environment due to the dissemination of their personal data. In some instances, the dissemination of personal data can result in significant financial loss. This situation highlights that consumers are in a vulnerable position in the face of unethical practices by some loan providers, particularly those offering illegal loans without an official license from the Financial Services Authority (OJK) (Yulianto, 2024).

To address these issues, the Indonesian government subsequently enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The presence of this regulation is expected to provide a strong legal basis for protecting the personal data of all citizens, including loan consumers. The PDP Law clearly regulates the rights of data subjects, the obligations of data controllers, and imposes strict sanctions for violators. In the context of online lending, this law should provide legal certainty and

prevent the practice of misuse of personal data by the organizer (Hal et al., 2025). However, the implementation of the PDP Law in the field still faces various obstacles. There are still many illegal loans that operate without a permit, so they are not subject to the applicable official regulations.

On the other hand, the digital literacy of the Indonesian people remains relatively low, particularly in terms of understanding personal data protection rights. This low level of legal awareness often leads consumers to give consent to the use of their data without fully understanding the risks that may arise. In addition, the law enforcement mechanism against personal data violations still faces obstacles in terms of technical, resource, and inter-agency coordination. This condition results in consumer protection in practice not being fully optimal, despite a clear legal basis (Nadiah et al., 2025).

Meanwhile, the notable case in Indonesia is the 2020 Tokopedia data leak. Tokopedia, one of the largest e-commerce platforms in Indonesia, announced that it has experienced a data leak involving its users' personal information. The affected data includes name, email address, phone number, and shipping address. This incident highlights the importance of personal data protection in Indonesia. It highlights the importance of data security in the e-commerce industry, as exemplified by the 2022 personal data leak case carried out by hacker Bjorka, who leaked the data of government officials to the internet media (Hal et al., 2025). Several studies have identified potential problems that may arise from personal data leakage, based on previous research and data. Some of the issues that often arise are identity and data theft, financial impact, psychological impact, reputational loss, and violation of individual privacy and freedom (Neltje et al., 2023).

A report by various national media, quoted in several legal and digital policy journals, highlights the case of the dissemination of personal data of online loan customers in Manado by unauthorized online lenders as an example of a serious violation of consumer privacy rights in Indonesia. Based on the results of the investigation by the Metro Jaya Police, two perpetrators who operated four illegal loan applications were found to have misused customers' personal data, including ID cards and contact lists, to intimidate and threaten them (Politik et al., 2025). These actions not only harm victims materially but also cause significant psychological and social impacts due to the dissemination of personal data to the public and the surrounding environment. This case is often cited as a reference in academic research as evidence of the weak personal data protection system prior to the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The implementation of the PDP Law is expected to provide a firm and comprehensive legal umbrella to prevent similar practices, while strengthening the accountability of online loan providers in maintaining the confidentiality, security, and integrity of consumers'

personal data (Jering, 2025).

This condition underscores the need to investigate the protection of personal data for online loan consumers in greater detail. This problem is not only about legal certainty, but also about social Justice, ethics, and moral responsibility. The study of this issue is important not only to strengthen the effectiveness of implementing the PDP Law, but also to affirm the urgency of incorporating Islamic values, such as trust, Justice, and the prohibition of tyranny, into the practice of digital financial services. Thus, the protection of consumer loans is ultimately not only a matter of formal regulation, but also an effort to maintain dignity, honor, and human rights in accordance with universal values and Islamic teachings (Kennedy et al., 2025).

The concept of Maqasid Syariah has strong relevance to personal data protection efforts in online loan services (pinjol) because both are oriented towards creating benefits and preventing harm to humans. From the perspective of Maqasid Syariah, which includes five main principles, namely *Hifz ad-Din* (Keeping Up With the Times), *Hifz an-Nafs* (Preserving the soul), *Hifz al-'Aql* (keeping your mind), *Hifz an-Nasl* (take care of offspring), and *Hifz al-Mal* (safeguarding property), the protection of personal data can be understood as part of the moral and spiritual responsibility in maintaining the honor, security, and rights of individuals (Hafidzah, 2024). In the context of online lending, the application of these principles is reflected in the need for fintech operators to maintain honesty and trust in managing user data (*Hifz ad-Din*), protect consumers from threats, data dissemination or intimidation in the event of default (*Hifz an-Nafs*), provide education about the rights and risks of using digital data (*Hifz al-'Aql*), prevent misuse of information that could harm family or social reputation (*Hifz an-Nasl*), as well as ensuring the security of users' financial data so that they are not misused for commercial purposes (*Hifz al-Mal*). Thus, Maqasid Syariah expands the meaning of personal data protection beyond mere compliance with positive laws, as stipulated in Law Number 27 of 2022 concerning Personal Data Protection, to encompass an ethical and spiritual commitment to creating Justice, security, and benefits in the digital financial ecosystem (Wahjono, 2025).

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) has a vital role in regulating and protecting people's personal data in the practice of online loans (pinjol), both legal and illegal. In this context, the PDP Law serves as the primary legal basis to ensure that every online loan provider is obligated to respect, maintain, and secure customers' personal data in accordance with the principles of prudence and transparency. Based on Articles 3 and 4 of the PDP Law, every individual has the right to get protection for their personal data, including financial data, identity, and other digital information collected by lending platforms. Then, Articles 15 to 20 affirm the obligation for data controllers, in this case, loan companies, to use data only according to the purposes approved by the data owner, as well as to protect data from

unauthorized access, collection, and dissemination (Research, 2023). This is especially relevant considering the numerous cases where loan customer data is misused for intimidation, threats, and the dissemination of personal disgrace on social media. The PDP Law also provides new rights for loan users, such as the right to access, correct, delay, and even delete their personal data from the loan system as stipulated in Article 16. In addition, Articles 57 to 63 provide strict administrative and criminal sanctions for loan operators who violate these provisions, including fines of up to billions of rupiah and the threat of imprisonment. With the PDP Law, online lending practices are expected to be more ethical, transparent, and secure, thereby increasing public trust in digital financial services. Philosophically, the application of the PDP Law is also in line with the principles of Justice and protection of human rights, and can be integrated with the values of Maqasid Syariah, which emphasize the importance of safeguarding property (*Hifz al-Mal*) and soul (*Hifz an-Nafs*) from all forms of abuse in the digital era (Ulil, 2024).

Previous research that has discussed the same theme of personal data protection is that of Manalu et al. (2025). This discusses how to protect customers' personal information in the context of online loan services, which are increasingly growing in Indonesia. A second study was also conducted by Maria Theresia et al. (2025), which discusses the importance of Personal Data Protection on online lending digital platforms, as reviewed in Law Number 27 of 2022 concerning Personal Data Protection (Case Study in Kupang City, NTT). Moreover, the latest research conducted by Fitriani et al. (2021), which discusses the problem of misuse of personal data in online loan services, especially illegal ones, continues to increase in line with the consumptive behavior of the digital society and low consumer awareness of personal data protection rights (Naswa Fiolla Anggraini et al., 2025).

Based on previous research, the topic of the Model of Regulation for the Protection of Personal Data of Online Loan Consumers, grounded in Maqasid Syariah and the Personal Data Protection Law Number 27 of 2022, is considered a new and interesting research subject. This study focuses on the Protection of Personal Data of online loan consumers from the Perspective of Maqasid Syariah. For this reason, the author chooses to focus more on the topic, which aims to analyze the Personal Data Protection of Online Loan Consumers from the Perspective of Maqasid Sharia. Using a careful methodological approach and accurate analysis, the author chooses to focus more on the topic for this reason. With a better understanding of this, this research can provide valuable insights for governments and law enforcement in the legal protection of personal data. As an additional innovation, this study utilizes NVivo 12 analysis tools to support more systematic data processing and analysis (Sapitri et al., 2024).

2. Research Method

The method used in this study is a qualitative research approach, which involves describing findings through online media. The method in this study aims to systematically describe the data obtained, providing factual and accurate information about the facts contained in a media text, such as news (Pratama et al., 2022). To facilitate research, social media data is processed using NVivo 12 Plus analysis software to display the data, which the researcher then narrates. The focus of this study is to analyze the Model of Personal Data Protection for Online Loan Consumers, based on Maqasid Syariah and the 2022 Personal Data Protection Law.

Furthermore, in this study, the researcher also utilized secondary data, including online media, social media, and journals related to the research, to examine the handling of gambling practices. The analysis technique utilizes NVivo 12 Plus, a data processing application for qualitative document analysis, which leverages computer assistance. Their equipment is easy to use and can process words, exploring word frequencies, attributes, and cases from large datasets. They also generate categories of factors or sub-factors in journalistic and research applications related to research topics (Sundari et al., 2022).

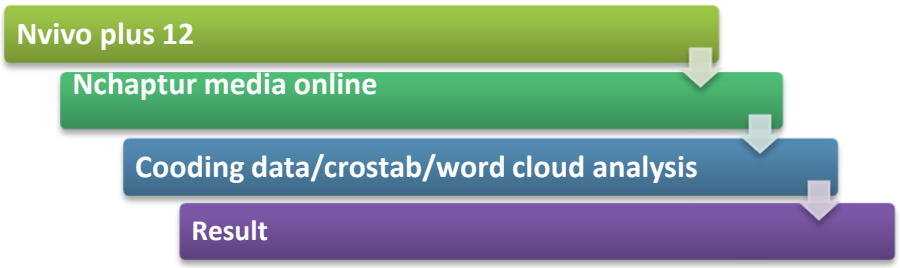


Figure 1. Data analysis stage
Source: Modified with NVivo 12 Plus

3. Results and Discussion

Description In the contemporary digital era, information has become a crucial factor that determines the dynamics of the country's economy, both developing and developed. While governments and the private sector have traditionally managed individual information, the emergence of digital technologies has presented a more complex and systematic threat to personal privacy. The explosive growth of personal data stored and transmitted through computers and mobile devices has created new vulnerabilities. Technological advances not only open up opportunities for innovation but also pose significant risks to the security and integrity of individual information, with the potential for substantial losses due to data leaks or misuse. Digital technology has transformed the way personal information is stored, distributed, and utilized, making individuals increasingly vulnerable to potential privacy breaches and irresponsible data exploitation (Antoine, 2025).

Cases of personal data misuse also occur during the process of online loans, which involve the use of data belonging to others, including the copying of data and ATM information (skimming), as well as the dissemination of personal information to the public. This type of activity involves violations of privacy rights that occur in the digital world. Currently, legal regulations that offend related to the privacy rights of digital data owners are contained in Article 26 paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) which states "Unless otherwise specified by Laws and Regulations, the use, of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned (Kharisma Arrasuli et al., 2023).

Some of the legal cases related to personal data protection that have occurred in Indonesia include:

1. The issue of data leaks resurfaced in June 2023. This time, Bjorka, who is often involved in similar incidents in Indonesia, is again the perpetrator. The hacker, who claims to be from Poland, published the data on the dark forum Breach Forums, having managed to access 35 million My IndiHome user records and offer them for US$5,000, or approximately Rp77 million. My Indihome rejects this news.
2. Bjorka is back in the spotlight after allegedly leaking passport data of 34.9 million Indonesian citizens (WNI) on July 5, 2023. The data containing personal information related to passports was sold on the dark web for US$10,000, or approximately Rp154 million.
3. On July 16, 2023, a data leak incident occurred, affecting approximately 337 million data points at the Directorate General of Population and Civil Registration (Dukcapil) of the Ministry of Home Affairs. This leaked data contains complete personal information, including NIK to birth or marriage certificate numbers. However, the Dukcapil rejected this news (Wijaya et al., 2024).

Islam has prohibited buying and selling gharar because it can harm or benefit one party. Meanwhile, buying and selling must contain benefits to both sellers and buyers. Gharar here is in accordance with the opinion of Bassyariah, who explains that gharar is characterized as an act that raises doubts or ambiguity in one or all of the pillars of the transaction.25 The prohibition of gharar is conveyed in a hadith which reads: From Abu Hurairah ra, he said, "The Messenger of Allah (PBUH) has prevented (us) from (doing) buying and selling gharar." (HR. Muslim III/1153). Muchtar explained that gharar involves buying and selling that contains elements of uncertainty, betting, or gambling. Giving rise to uncertain outcomes for rights and obligations in a transaction (Dewi, 2023).

The emergence of the PDP Law should be followed by increasing digital literacy education in the public about the importance of protecting personal data. The level of digital literacy among the Indonesian people remains very low. The government must engage with citizens to encourage them to protect their data, prevent various leaks of personal data held by public bodies in recent years, and promote public bodies as stakeholders to increase their awareness of data protection (Wijaya et al., 2024).

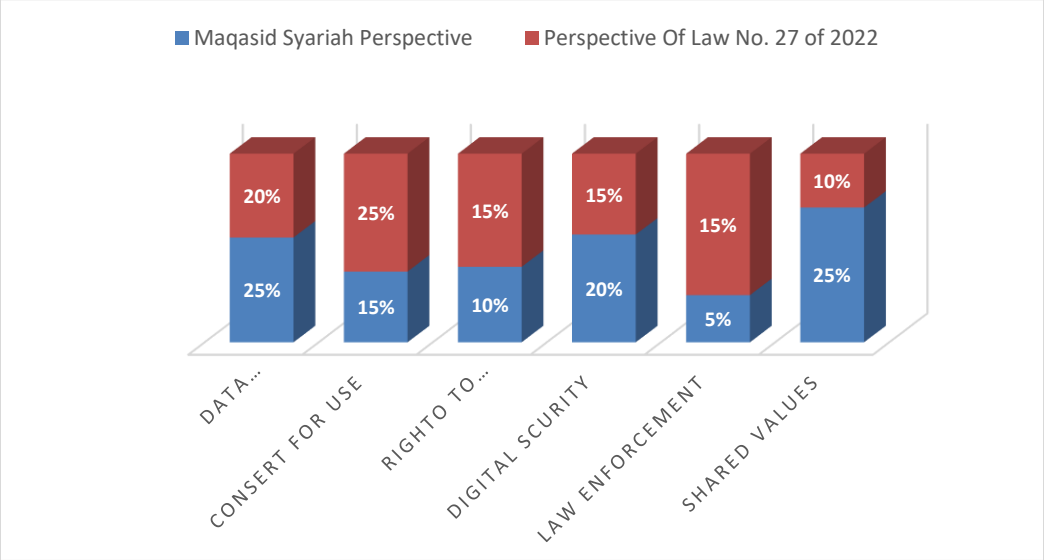


Figure 2. Personal Data Protection of Online Loan Consumers
Source: Modified with Nvivo12 Plus

Figure 2. The above comparison illustrates the Personal Data Protection of Online Loan Consumers from two perspectives: Maqasid Syariah and Law Number 27 of 2022 on Personal Data Protection. From the Maqasid Syariah side, the value of personal data protection emphasizes the principle of safeguarding benefits and avoiding harm, which is reflected in the high proportion of data confidentiality (25%) and shared values (25%). This demonstrates that, from a sharia perspective, data protection is not only a formal legal aspect but also part of efforts to protect *hifz al-nafs* (the protection of life) and *hifz al-'ird* (the protection of honor). Meanwhile, from the perspective of Law No. 27 of 2022, the primary focus lies on the aspects of consent to the use of data (25%) and access rights and digital security (15% each), which reflect a legal and formal approach to protecting personal data. This law emphasizes the importance of legal certainty and the responsibility of electronic system operators in protecting consumer data. Overall, this diagram illustrates that the two perspectives share a common goal in safeguarding individual rights and security, but differ in their basic orientation: Maqasid Syariah emphasizes moral and spiritual values, whereas Law No. 27 of 2022 focuses on legal aspects and their enforcement (Sulistiawati et al., 2025).

No	Type of Personal Data	Method of Collection	Potential Misuse Risks
1	Personal identity (ID card, NIK, photo)	Uploaded by users	Identity fraud
2	Phone contacts & friend list	Automatic app access	Unauthorized disclosure
3	Location data (GPS)	Through app permissions	Unethical tracking
4	Financial data (bank account, payslip)	Entered by users	Financial data breach
5	Digital activity	System analytics	Profiling & discrimination

Table 1. Types of Personal Data Collected by Pinjol Applications

Table 1. Showing the various types of personal data of online loan consumers, how they are collected, and the potential risk of misuse that can occur. Each type of data has a different level of sensitivity and risk. For example, personal identity data such as ID cards, NIKs, and photos are collected through user uploads. They are vulnerable to identity forgery, which can be used for illicit activities such as opening fictitious accounts or committing fraud. Phone contacts and friend lists that are automatically accessed by apps can also be potentially misused for unauthorized data dissemination, especially in cases involving intimidating billing practices (Syafi et al., 2022).

Additionally, location data (GPS) collected through app permissions can be leveraged for unethical tracking, posing a threat to user privacy and security. Financial data, such as accounts and payslips, that users input is at high risk of financial leakage if the app's security system is weak or compromised. Meanwhile, digital activities obtained through system analytics can lead to profiling and discrimination, for example, in determining a person's creditworthiness or consumption behavior. Overall, this table confirms the importance of personal data protection mechanisms, such as explicit consent, transparency in data use, and robust law enforcement, in preventing the misuse of online loan consumer data (Azizah et al., 2024).

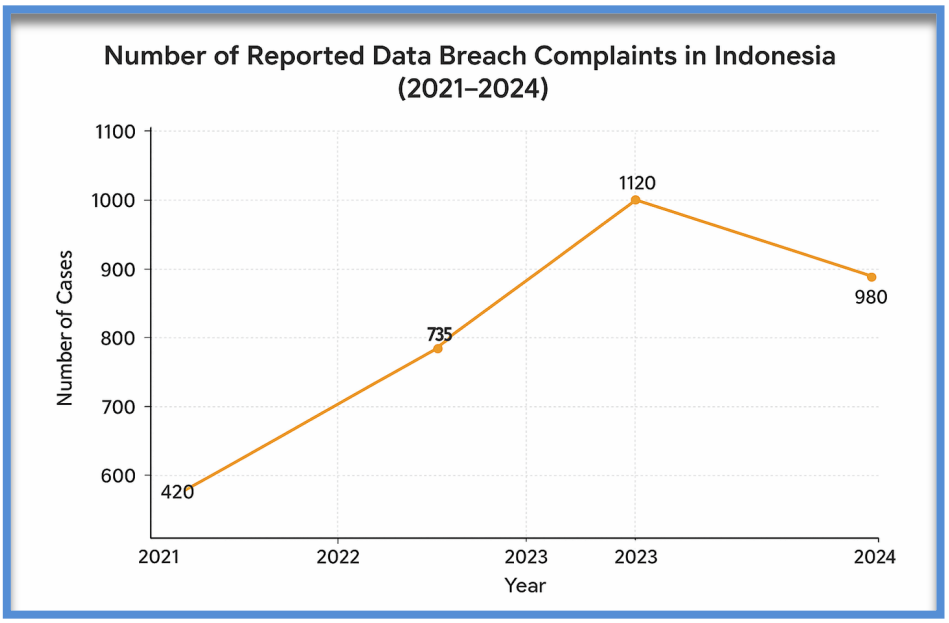


Figure 3. Number of Data Leak Complaints in Indonesia (2021-2024)

Figure 3. The graph illustrates the dynamics of data leak complaints in Indonesia during the 2021–2024 period, showing an up-and-down pattern with a general trend of continued increase compared to the 2021 starting point. The year 2021 became the baseline, with 420 complaints, indicating that data protection issues already existed but may not have received significant attention from the public or regulators. This figure also suggests that during that period, there was no structured reporting channel or sufficient public awareness to report data leak incidents. The sharp increase in 2022, reaching 735 complaints, reveals two interrelated phenomena. First, the increasing penetration of digital services, particularly fintech, e-commerce, and social application platforms, is driving more personal data exchange and storage activities. Second, there are increasing incidents of data leaks due to weak cybersecurity systems and inadequate data management practices in many companies and government agencies. During this phase, the public became increasingly critical of privacy violations as cases of large-scale data breaches were reported. 2023 was a tipping point with 1120 complaints, the highest number in four years. This drastic increase could indicate the presence of *a cumulative risk effect*, where an increasing number of digital platforms are under attack, including data leaks from large agencies that attract public attention.

Additionally, this surge can also signal an improvement in access and reporting mechanisms, making it easier for people to identify and report incidents when they experience indications of leaks. In the context of regulations, 2023 marks a transitional phase towards the stronger implementation of the Personal Data Protection Law (PDP Law), resulting in increased public oversight of data protection issues. In 2024, the chart shows a slight decrease to 980 complaints; however, this figure remains very high and is almost at the same level as the previous year's peak.

The decline could be an early sign of improvements in data security management, particularly following regulatory and public pressure that encourages companies and government agencies to enhance their security systems (Soleh et al., 2024). However, the number of complaints remaining close to a thousand indicates that the improvement is not significant enough to reduce incidents drastically. This confirms that the challenge of data leakage remains a structural issue that requires long-term strategies and cross-sector coordination.

When viewed from a cybersecurity perspective, the graph pattern reveals that the threat of data leakage is not merely a technical incident, but a multidimensional phenomenon encompassing technological factors, digital culture, data governance, and public literacy. The sharp increase from 2021 to 2023 may reflect the increasingly complex nature of Indonesia's digital ecosystem, with many systems fragmented and yet to adopt global security standards. On the other hand, the high numbers in 2024 suggest that cyber threats continue to evolve faster than the ability of many institutions to mitigate them. Additionally, from a public policy perspective, this graph serves as a crucial indicator for the government in evaluating the effectiveness of regulations, particularly the PDP Law. Although regulatory implementation is underway, data trends indicate that education for controllers and data processors remains essential. Companies must understand that data protection is not just a formal obligation, but an integral part of building customer trust. Failure to safeguard data can have greater reputational, economic, and legal consequences in the digital age (Aji, 2022). Ultimately, this graph highlights the importance of enhancing digital security literacy in society. Many cases of data leaks occur not only due to external attacks, but also due to user negligence, such as sharing OTPs, clicking on phishing links, or using easy-to-guess passwords. Therefore, the data leak handling strategy focuses not only on service providers, but also on systematic and continuous public education. By understanding the pattern of data leaks over the past four years, stakeholders can design more targeted policies and interventions to mitigate similar risks in the future.

HES Principle	Meaning	Ideal Practice	Current Condition in Online Lending (Pinjol)
Amanah	Upholding religious trust	Data is stored and processed with proper consent	Data breaches still frequently occur
Justice (‘Adl)	Not harming or exploiting others	Transparent information	Many apps do not clearly explain their privacy policies

		regarding data usage	
Maslahah	Promoting benefit and preventing harm	Data is used for lawful and ethical economic purposes	Some illegal lenders misuse data for intimidation
Hifz al-'Ird (protecting dignity)	Safeguarding users' honor and dignity	No dissemination of personal data	Cases of data exposure of borrowers in arrears still occur

Table 2. Regarding the HES principle in the context of personal data protection in online loan services in Indonesia.

Table 2. Describe the application of HES (Human Ethical and Shariah Principles) principles in the context of personal data protection in online loan services in Indonesia. Conceptually, the principles *of amnah*, *Justice ('adl), maslahah*, and *hifz al-'ird* should be ethical and religious guidelines in managing user data in accordance with the values of Maqasid Sharia. However, the current conditions reveal a significant gap between ideal practice and reality on the ground. From the aspect of *amnah*, which means maintaining trust, ideally, the user's personal data should only be stored and processed with explicit permission and used responsibly. However, in reality, there are still frequent leaks of loan user data. This suggests that the principle of trust has not been adequately maintained, as many loan providers lack adequate security systems and fail to prioritize consumer data protection.

In the principle *of Justice ('adl),* which requires that no party is wronged, the ideal practice is openness and transparency in the use of personal data. Every user has the right to know how their data is collected and used. However, many loan applications do not clearly explain their privacy policies, and some do not display them at all. This situation creates an information imbalance between users and service providers, resulting in injustice for consumers. Furthermore, *the principle of maslahah*, which is oriented towards bringing benefits and preventing harm, has also not been fully implemented. Ideally, data should be used for halal economic purposes, such as supporting productive and beneficial financing activities. However, in fact, some illegal loans actually use personal data to intimidate delinquent customers, causing psychological and social losses that are contrary to the purpose of Sharia to create benefits.

Meanwhile, the principle *of hifz al-'ird* or maintaining honor emphasizes the importance of protecting human dignity by not disseminating personal data without permission. This ideal practice should be the primary basis for protecting user privacy. However, in reality, there are still frequent cases of the dissemination of outdated customer personal data, both through social media and private messages. Such actions clearly violate the individual's honor and are contrary to the principles of Islamic ethics. Overall, the table indicates that personal data protection practices in the online lending sector in Indonesia are not fully aligned with HES values. Weaknesses in maintaining trust, a lack of transparency, the misuse of data, and the violation of user privacy are evidence that ethical and Sharia principles are still not fully internalized in the lending system. Increased supervision, strict law enforcement, and digital ethics education are necessary to ensure the lending industry operates in accordance with the values of Maqasid Syariah and Law Number 27 of 2022 concerning Personal Data Protection.

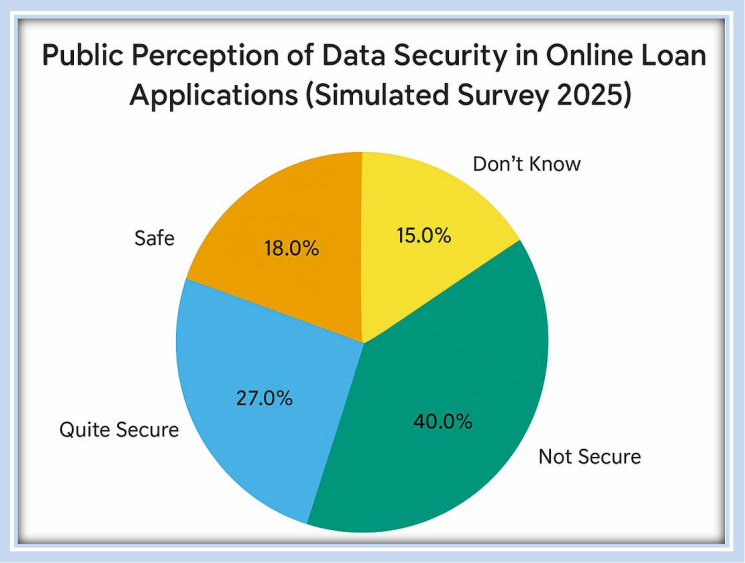


Figure 4. Based on public perception

Figure 4. Describe public perception of data security in online loan applications (Pinjol) based on a simulated survey in 2025. According to the survey results, the majority of people still feel uncertain or insecure about the protection of their personal data. As many as 40% of respondents stated that they were unsafe, 27% felt relatively safe, 18% rated it safe, and 15% did not know. This percentage indicates that 67% of the public (encompassing the combined categories of "not secure" and "quite secure") lack complete confidence in the security of data on lending platforms. This finding indicates that public trust in loan operators remains very low, particularly in the area of personal data management. This insecurity can be caused by various factors, including numerous data leaks, data misuse by individuals, a lack

of transparency in privacy policies, and the rise of illegal loan applications that lack official permission from financial authorities. This condition reinforces the view that most loan providers lack a robust data protection system and have not fully implemented the principle of prudence in managing sensitive user information.

From the perspective of Sharia Economic Law (HES), the results of the graph illustrate the non-optimal implementation of several basic principles that become ethical guidelines in digital economy transactions, namely *amanah*, *Justice ('adl), maslahah*, and *hifz al-'ird*. The principle *of trust* requires loan operators to maintain user trust by protecting their data from leakage, misuse, or unauthorized use. However, in reality, many users still feel that their data is vulnerable and insecure, indicating the weak implementation of trust values in lending business practices.

Furthermore, the principle *Justice ('ADL)* About transparency and the balance of rights between users and service providers. Ideally, users have the right to know how their personal data is collected, stored, and used. However, the low perception of security indicates that many loan providers still fail to clearly explain their privacy policies or use language that is difficult for users to understand. This information imbalance creates injustice and harms consumers, mainly when personal data is used without explicit consent. The principle *of maslahah*, which emphasizes efforts to bring benefits and prevent harm, has also not been fully realized (M. Iffah et al., 2025). Personal data should be used for productive and halal purposes, such as accurate credit analysis and community economic empowerment. However, in practice, many lenders still use user data unethically, for example, by disseminating delinquent data or intimidating customers who pay late. Such actions clearly cause moral and social harm that is contrary to the principle of welfare (Indonesia & Compiler, 2021).

Meanwhile, the principle of *hifz al-'ird*, or maintaining one's honor, demands that the user's privacy be protected as part of human dignity. The fact that most people feel insecure shows that this principle has not been properly practiced either. The case of disseminating customer personal data, which still often occurs on social media or in personal messages, constitutes a form of violation of individual honor and is contrary to Sharia values. Thus, this perception graph not only illustrates the level of public trust in data security but also becomes a moral and ethical indicator for the lending industry. To align with the principles of Sharia Economic Law and Law Number 27 of 2022 regarding Personal Data Protection, loan operators must enhance digital security systems, ensure transparency in their privacy policies, and instill the values of trust and social responsibility in every aspect of their operations.

Additionally, the government and financial authorities should tighten their supervision and educate the public about the importance of digital literacy and personal data protection. Overall, the graph suggests that protecting personal data in the online lending sector remains a significant challenge in Indonesia. Improvement

efforts must be made not only from the technological aspect, but also from the ethical and spiritual aspects of business. Only by consistently applying the principles of *amanah*, *Justice*, *maslahah*, and *hifz al-'ird* can the Pinjol ecosystem develop into a digital financial system that is not only efficient and innovative but also fair and in accordance with Sharia values (Rani et al., 2024).

No	Violation	Article	Criminal Sanctions
1	Collecting/obtaining another person's personal data without authorization	Article 65 paragraph (1)	Imprisonment up to 5 years and/or a fine up to IDR 5 billion
2	Disclosing/leaking personal data without authorization	Article 65 paragraph (2)	Imprisonment up to 4 years and/or a fine up to IDR 4 billion
3	Using another person's personal data without consent	Article 65 paragraph (3)	Imprisonment up to 5 years and/or a fine up to IDR 5 billion
4	Falsifying or creating fake personal data	Article 66	Imprisonment up to 6 years and/or a fine up to IDR 6 billion
5	Violations committed by corporations	Article 70	Fines up to 10 times the amount for individuals, plus additional sanctions (business suspension, license revocation, dissolution, compensation, etc.)

Table 3. Violations and Criminal Sanctions of the Personal Data Protection Law of 2022

Table 3. Explains that there are five main categories of violations that can be subject to criminal sanctions under the PDP Law 2022, with different ranges of penalties based on the level of threat to personal data security. In the first and third violations, namely the collection and use of personal data without the right or permission of the data owner, the criminal threat in the form of a maximum prison sentence of five years and a fine of up to five billion rupiah reflects that the state provides strong protection for the control rights of data subjects. This demonstrates

that unauthorized data control is not only an administrative violation but also a serious criminal offense. The second offense, namely the act of disclosing or leaking personal data, carries a threat of four years in prison and a maximum fine of four billion rupiah. This sanction is slightly lower than those in the first and third categories. However, it remains significant because the dissemination of data can trigger further impacts, such as digital fraud, identity theft, and financial losses for victims. This confirms that the condition of data leakage is not only an ethical issue, but also a real legal threat.

The fourth offense, falsifying or providing false personal data, carries the highest criminal penalty, including a prison term of up to six years and a fine of six billion rupiah. The high level of sanctions is in line with the level of danger that data falsification can lead to, such as unauthorized access to financial services or the misuse of identities to obtain loans. Thus, the state considers data falsification a form of digital crime with severe implications. The fifth point emphasizes that the PDP Law targets not only individuals but also business entities or corporations as legal subjects. When corporations commit violations, fines can be up to ten times the individual sanctions. They can be accompanied by additional penalties such as business freezes, revocation of licenses, or dissolution of legal entities. This provision is of significant importance because cases of data breaches in the digital ecosystem often occur within large institutions, such as technology companies, fintechs, and online loan providers.



Figure 5. WordCloud of the concept of Personal Data Protection in Fintech and Sharia Perspective in Indonesia

Source: Modified with Nvivo 12 Plus

The *word cloud* image illustrates the main concepts and themes related to personal data protection, especially in the context of fintech (financial technology)

and the perspective of sharia law and maqasid in Indonesia. The most dominant words were *"data"*, *"personal"*, *"privacy"*, *"protection"*, and *"law"*, indicating the research focus on the issues of security, privacy, and the regulation of consumers' personal data, especially in digital transactions and technology-based financial services. The emergence of words such as *"fintech"*, *"digital"*, *"online"*, and *"technology"* confirms that the discussion is centered on the challenges of data protection in the digital era, where online *lending services* and financial applications are becoming increasingly popular. Meanwhile, the terms *"Islamic"*, *"maqasid"*, and *"sharia"* indicate the existence of an ethical and legal approach to assessing the protection of personal data, which is oriented towards maintaining the honor, security, and rights of consumers in accordance with the principles *of maqasid Sharia*.

In addition, words such as *"regulation"*, *"law"*, *"law"*, and *"law"* indicate the important role of the national legal framework, especially Law Number 27 of 2022 concerning Personal Data Protection, in creating a fair and transparent protection system. The emergence of the words *"transparency"* and *"consumer"* underscores the importance of accountability for fintech operators to their users. Thus, this *word cloud* visually illustrates the relationship between personal data protection, legal regulations, digital technology, and Sharia values in the development of a safe, transparent, and ethical financial system in Indonesia. In addition, the existence of terms such as *customers*, *consumers*, and *users* underscores that the issue of data protection is inextricably linked to the dynamics of consumer behavior. This is important in academic studies because user behavior, including the level of digital literacy and awareness of privacy risks, is a key variable in understanding the level of vulnerability of personal data. This word cloud shows that users are not only regulatory objects, but also important actors in maintaining data security through safer and more responsible technology use practices.

4. Conclusion

The phenomenon of personal data leakage in Indonesia illustrates that digital transformation not only presents economic opportunities but also poses significant risks to individuals' privacy and security. Various major cases, such as the leak of MyIndiHome data, Indonesian passports, and Dukcapil data, confirm the weak cybersecurity system, low digital literacy, and lack of institutional discipline in implementing data protection standards. Although Law Number 27 of 2022 concerning Personal Data Protection has established a new legal framework, its implementation still faces significant challenges because many data controllers remain unfamiliar with the legal and ethical obligations that must be met. Data on the increase in complaints throughout 2021–2024 shows that cyber threats are evolving faster than the mitigation capabilities of many institutions. Hence, data protection is now a multidimensional issue that concerns technology, governance, and public

behavior.

The 2022 PDP Law establishes five main categories of violations with different criminal sanctions according to the level of threat to personal data security. The collection, use, and dissemination of data without permission is considered a serious crime because it has the potential to cause significant losses to the data owner. Falsification of personal data has the harshest penalties because it can trigger a chain of digital crimes. In addition to individuals, corporations can also be subject to much greater sanctions, along with additional penalties, given that many data breaches occur through technology and digital services companies. Overall, this regulation shows the state's commitment to providing strong protection for personal data in the digital era.

In the context of online lending, this problem is increasingly complex due to the many invasive data collection practices, misuse of personal information, and intimidation of customers. Analysis through the perspective of Sharia Maqasid and Sharia Economic Law (HES) shows that the loan industry is still far from the principles of trust, Justice ('adl), maslahah, and hifz al-'ird. Both diagrams and risk tables, as well as public perceptions, illustrate the loss of public trust in loan providers due to a lack of transparency and weak data protection. The Sharia approach and the national legal framework share the same goal of protecting the dignity, rights, and security of individuals; however, the reality of practice on the ground still reveals significant gaps. Thus, personal data protection in Indonesia requires systemic strengthening through strict regulations, increasing digital security capacity in both public and private institutions, more intensive digital literacy among the community, and integrating ethical and spiritual values into data management. Collaboration among the government, the technology industry, lenders, and the community is key to building a safe, fair, and trusted digital ecosystem. Only with such a comprehensive approach can Indonesia ensure that digital innovation does not compromise the privacy and dignity of its users, in accordance with positive legal principles and Sharia values.

References

Aji, M. P. (2022). *Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective*. https://doi.org/10.22212/jp.v13i2.3299.

Antoine, R. A. (2025). *Abuse of Personal Data in Digital Transaction Technology in the Digital Banking Industry (Case Study of PT. Bank Syariah Indonesia)*. *2*(1), 316–327.

Azizah, S., Ula, Z. N., Mutiara, D., Prameswari, M. P., Economy, F., Islam, U., Abdurrahman, N. K. H., & Pekalongan, W. (2024). *Cybersecurity as the*

foundation of mobile finance application development: A literature study on cybercrime and its mitigation, mobile financial applications have become one of the leading innovations that businesses utilize to access and manage finances more efficiently. With various life activities, the availability of this technology also brings a negative impact on the emergence of financial technology business forms, as newcomers take advantage of opportunities from technological process innovation, products, business models, and changes. *17*(April), 221–237.

Dewi, P. (2023). *Prohibition of MAGHRIB (Maysir, Gharar, Riba) in Buying and Selling Transactions of Islamic Economic Studies*. *1*:23–33. https://doi.org/10.32923/ejesh.v1i1.3265.

Diana, B. A., & Sari, J. A. (2024). *The Impact of Digitalization Transformation on Changing Behavior of Rural Communities*. *9*(2), 88–96.

Reviewed, O., Number, D. U., Protection, T., Personal, D., Case, S., Kupang, K., Kim, M. T., Jacob, Y. M. Y., & Bire, C. M. D. (2025). *Artemis Law Journal*. 511–526.

Fitriani, S. D., Satriana M, M. R., Retnosari, T., & Rohmawati, N. (2021). Digitalization of Sharia Economics: The Application of Islamic Laws in Online Buying and Selling. *Journal of Sharia Economics*, *6*(1), 51–59. https://doi.org/10.37058/jes.v6i1.2542.

Fitriyadi Ningsih, A., Sulistiono, B., Anawati, N., & Tri Setiyoko, D. (2025). Indonesian Research Journal on Education: The Influence of Technological Innovation on the Dynamics of Social Life: Literature Review. *Indonesian Research Journal on Education*, *5*, 134–144. https://irje.org/index.php/irje.

Hafidzah, Y. Al. (2024). *Legal Protection of Consumers in Online Loan Transactions on the Indodana Application: A Review of Law Number 8 of 1999 Concerning Consumer Protection and Sharia Economic Law*. pp. 1043–1061.

Hal, V. N. J., Satria, A., & Ahyar, S. (2025). *Legal Responsibility of E-Commerce Platforms for Personal Data Leakage from the Perspective of Law No. 27 of 2022*. *2*(2), 1089–1096. https://doi.org/10.58344/jws.v3i3.584.6

Indonesia, A. F., & Penyususun, T. (2021). *No Title*. *2*(2), 55–72.

Jering, P. (2025). *Online Security in Social Media: The Importance of Personal Data Protection in the Digital Era (Case Study of the National Service Journal (JPN) Indonesia*. *6*(1), 38–52.

Jurnal, E., Hukum, I., Iffah, M., Raib, E., Rosadi, S. D., & Cahyadini, A. (2025). *Comparison of the Application of the Principle of Transparency Between Indonesia and Ireland in the Event of Failure to Protect Personal Data, Faculty of Law, Padjadjaran University, Indonesia, and the World, Including Indonesia. According to the data obtained from the survey results, as shown in Figure 1, the number of Internet Users in 2023 and their daily lives in Indonesia. This is supported by data indicating that the internet penetration rate in Indonesia reached 79.5%* in 2024. *Sec. 3*.

Kennedy, A. (2025). Challenges of Implementation and Development of Telematics Law in Indonesia. *Ethics and Law Journal: Business and Notary*, *3*(2), 1–9. https://doi.org/10.61292/eljbn.262.

Kharisma Arrasuli, B., & Fahmi, K. (2023). Unes Journal Of Swara Justisia Indonesia's Positive Legal Protection Against The Crime Of Misuse Of Personal Data. *Sound of Justice*, *7*(2), 370. https://creativecommons.org/licenses/by/4.0/https://swarajustisia.unespadang.ac.id/index.php/UJSJ/indexDOI:https://doi.org/10.31933/ujsj.v7i2.

Manalu, N., Handayani, P., & Abra, E. H. (2025). *Contract Law in the Integration of Artificial Intelligence and Data Protection in the Era of Digital Business*. *8*(2), 978–990.

Nadiah, F., & Wiraguna, S. A. (2025). Legal Review of Personal Data Protection in Electronic Transactions in Indonesia. *Journal of Educational Multidisciplinary Research*, *2*(6), 270–278. https://journal.hasbaedukasi.co.id/index.php/jurmie.

Naswa Fiolla Anggraini, & Sidi Ahyar Wiraguna. (2025). Legal Responsibility of Online Lending Platforms for the Illegal Misuse and Dissemination of Consumer Personal Data. *RISOMA: Journal of Social Research in Humanities and Education*, *3*(3), 144–167. https://doi.org/10.62383/risoma.v3i3.767.

Neltje, J., Lubna, S., & Sulthanah, T. (2023). *Protection of Personal Data in Doxing Actions Based on Law Number 27 of 2022*. *7*(2), 1708–1713.

Penelitian, J. (2023). *All Fields of Science J-LAS*. *3*(2), 17–24.

Politics, A. J., Humanities, H., Jl, A., North, A., & Jeruk, K. (2025). *Legal Responsibility of Online Loans for the Illicit Dissemination of Customer Data by Online Loan Providers, Including Both Licensed and Unlicensed Protection of Personal Data in Indonesia. Digital technology also affects the effectiveness of protecting people's personal data. 3*(April).

Pratama, I., Purnomo, E. P., Mutiaran, D., Adrian, M. M., & Sundari, C. (2022). Creating a Peatland Restoration Policy to Support Indonesia's Economic Development in a Sustainable Way. *IOP Conference Series: Earth and Environmental Science*, *1111*(1). https://doi.org/10.1088/1755-1315/1111/1/012004.

Rani, A. M., Purnomo, B. S., & Purnamasari, I. (2024). *Navigating the Landscape of Islamic FinTech : A Comprehensive Literature Review*. *02*(02), 118–125. https://doi.org/10.58812/esmb.v2i02.

Sapitri, D., & Widana, O. (2024). Motivation of Ethical Sharia Property Investment for The Millennial and Generation Z. *JIEI: Jurnal Ilmiah Ekonomi Islam*, *10*(02), 1905–1924.

Soleh, M., Tjenreng, Z., Pacasarjana, S., & Applicator, M. (2024). *Public Service Data Leakage Prevention Strategy*. *11*(1), 1–10.

Sulistiawati, A., & Hastuty, A. (2025). *Integration of Sharia Principles in Fintech*

Development: Challenges and Opportunities. *Consider using this technology as a tool to help you better understand your child*'s needs.

Sundari, C., Purnomo, E. P., & Fathani, A. T. (2022). Civil Society Participation Model: Forest and Land Fire Prevention Policy in Jambi Province. *Journal of Natural Resources and Environmental Management*, *12*(4), 669–678. https://doi.org/10.29244/jpsl.12.4.669-678.

Syafi, U. I. A.-, Syafi, U. I. A.-, & Syafi, U. I. A.-. (2022). *As-Syafi'iyah Islamic University, Indonesia*. *Sec. 4*(2).

Syaiful, R. D., & Sugiyono, H. (2024). *Misuse of Consumer Personal Data Through Illegal Fintech Peer-to-Peer Lending*. *10*(1), 189–201.

Ulil, S. (2024). *Legal Protection of Personal Data of Customers of Non-Bank Loan Service Providers Online English Title: Legal Protection of Personal Data of Customers of Non-Bank Loan Service Providers Online*. *2*(1), 176–182.

Wahjono, S. I. (2025). *UNIVERSITY OF MUHAMMADIYAH SURABAYA JUNE 2025*. *5*(2).

Wijaya, J., Titin, A., Nursanthy, R., & Thamrin, M. A. (2024). *Protection Of Personal Data In Surfing In Cyberspace*. *VIII*(2), 638–644.

Yulianto, D. (2024). Economic Crime Analysis in Online Lending Practices: Impact on Society and Countermeasures Strategies. *Journal of Syntax Admiration*, *5*(12), 5641–5657. https://doi.org/10.46799/jsa.v5i12.1888.