

# TRANSFORMATIVE JUSTICE, PROTECTION OF CONSUMER PERSONAL DATA IN ONLINE LOAN BUSINESS IN INDONESIA

**SRI LESTARI POERNOMO**

Faculty of Law - Indonesian Muslim of University - Indonesia

Corresponding email: sri.lestari@umi.ac.id<sup>1</sup>

**Abstract** - Lately there have been many online loan cases that have had various impacts, starting from problematic billing times to misuse of customer personal data. Online loan application services, many people have complained about problems regarding the distribution of personal data carried out by online loan providers without notification and without permission from the owner. Legal protection and sanctions for violations of personal data have been regulated in UURI No. 27 of 2022 and its amendments concerning Electronic Information and Transactions. Of course there are several indicators that can cause conflict in the aspect of personal data protection, especially in the case of online loans, including prohibitions: (a) prohibition of obtaining or collecting personal data that is not theirs, with the intention of benefiting oneself or others, which may result in the loss of the subject's personal data; (b) prohibition of disclosing personal data that does not belong to him with the intention of benefiting himself or another person which could result in the loss of the personal data subject; (c) prohibition of using personal data that does not belong to him, with the intention of benefiting himself or another person which can result in the loss of the personal data subject; (d) prohibition of making false personal data or falsifying personal data with the intention of benefiting oneself or another person which may result in harm to another person. The research used in this research process uses a type of normative legal research. The determination of this study puts forward the dignified aspect of justice in the process of resolving online loan conflicts against all forms of protection of consumers' personal data, so that consumers feel transformative justice in an electronic trading system. Apart from that, it also maintains the principles of privacy rights in order to protect and provide legal certainty against all forms of abuse of consumer personal data.

**Keywords:** *consument, justice, personal data protection*

## Table of Contents

### INTRODUCTION

1. Problem
2. Research Method
3. Result and Discussion

### CONCLUSION

### ACKNOWLEDGEMENT

## INTRODUCTION

Indonesia is a country that has a population that continues to follow the flow of technology and business which is very high. This is evidenced by the consumptive Indonesian millennial generation who utilize online business with technology. Nearly 270 million people in Indonesia can be said to know and explore business through technology. These things encourage the creation of an increasingly fast online business climate in Indonesia. In addition to online business through Electronic Trading Systems (PMSE) has become a factor and indication of the rise of online loans which are used by most millennial youth in Indonesia as a form of business investment, however these online loans are often misused in order to damage consumer personal data for the benefit of just for a second.

Lately there have been many online loan cases that have had various impacts, starting from problematic billing times to misuse of customer personal data (Darmiwati & Syahfitri, 2021). Online loan application services, many people have complained about problems regarding the dissemination of personal data carried out by online loan providers without notification and without the permission of the owner. Legal protection and sanctions for personal data violations have been regulated in UURI No. 27 of 2022 and its amendments concerning Electronic Information and Transactions.

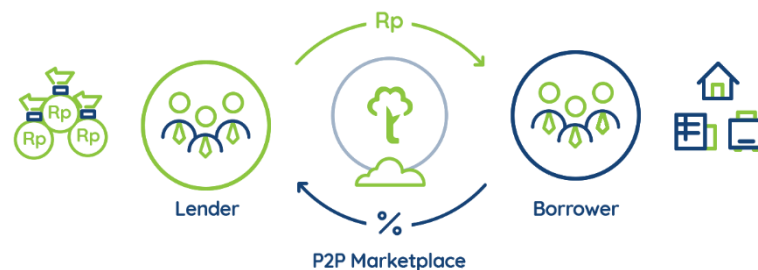
Specifically regarding legal protection and sanctions for breach of personal data in online loan services, it has been stated in Financial Services Authority Regulation No.77/POJK.01/2016 concerning Information Technology-Based Borrowing and Borrowing Services, which is emphasized in Article 26 that the organizer is responsible for maintaining the confidentiality, integrity and availability of users' personal data and in utilizing it must obtain approval from the owner of personal data unless otherwise specified by the provisions legislation. Sanctions for violations of personal data refer to Article 70 paragraph (4) UURI No. 27 of 2022 jo Article 57 UURI No. 27 of 2022, namely administrative sanctions in the form of written warnings, fines, obligation to pay a certain amount of money, restrictions on business activities, and revocation of licenses (Nurmantari & Martana, 2019).

The presence of technology has supported the creation of financial services that are more efficient and in accordance with the needs of society based on information technology (peer to peer). Through this peer to peer lending, people who need funds in micro amounts can easily and quickly get loans without the need to apply for credit to the bank with certain requirements. Peer to peer lending services can be accessed by the public through applications quickly anytime and anywhere. This is certainly different from credit facilities in banking services, where prospective customers must apply for credit to a certain bank, then a credit agreement is made between the bank and the customer by bringing collateral. The presence of innovation in the financial sector will have two sides, on the one hand it will provide benefits or a side that has the potential to disrupt traditional financial services. Disruptive effects that will occur can lead to financial sector instability and unhealthy competition. Besides that, the presence of innovation has made it easy for people to get loans quickly without collateral (Erna Priliyasi, 2019).

Currently, the growth of online loans in Indonesia is currently very fast. Unexpectedly, in a short time, not even two years, thousands of Fintech companies have sprung up that offer online loans. Data from the Financial Services Authority shows the number of registered fintech is currently 127, while the number of illegal fintech is around 1230. Online loans offer many features that benefit consumers compared to banking. As a result, in the past two years, online loan fintech has grown very fast. With the existence of fintech, now someone who wants to apply for a loan can simply download an application or access the loan service provider's website, fill in the data and upload the required documents and in a relatively short time the loan is directly looking for the borrower's account. (W. Wahyuni, 2021).

Negative impacts have emerged such as the spread of the borrower's personal data, because in the online loan verification process it is done online and will ask for approval from the loan recipient to access all data. This is a very high risk of misusing the personal data of the loan recipient. Requests for consumer personal data are actually needed by companies to conduct an assessment of prospective borrowers and to ensure that the borrower is really the person whose name is listed in the application, but in some cases, contact access is used to make billing. (Dewi, 2009).

Information Technology-Based Borrowing and Borrowing Services or known as peer to peer lending (A. Basha et al., 2021) (P2P Lending) is one of the fintech that attracts the attention of the public. The presence of P2P lending provides convenience facilities to the public who need credit quickly. This P2P Lending brings together the owner of the funds (lender) or what is commonly called the creditor with the borrower or debtor (borrower) through an electronic application (without meeting face to face). Illustratively the P2P Lending flow is described as follows:



Peer to peer lending is a description of the online market, where lenders who are also known as lenders can lend to individuals or small businesses (borrowers). Peer to peer lending companies also offer a competitive advantage for bringing together lenders. These advantages include a very low interest margin, due to low administrative costs, the ability to offer loans to multiple borrowers. that banks (unbankabel) may reject, and their innovative use of technology to provide greater transparency, flexibility, fast and more convenient service to lenders or borrowers.

The workings of peer to peer lending are as follows:

- Process for Borrowers. After registration, the borrower will submit a lending proposal. The peer to peer lending provider will then analyze the credit score, borrowing history, total income of the borrower, to determine the loan interest rate, and the borrower's score.
- Process for lenders. The lender will provide personally identifiable information to the peer to peer lending provider such as name, ID card number, account number, mobile phone number or cell phone and so on. After the registration process, the lender can view the profile of the loan recipient and decide to whom the loan will be given.
- Process for implementing peer to peer lending. Providers of peer to peer lending as business entities in Indonesia will manage personal data from lenders and manage funds from lenders and concurrently personal data from lenders. The organizer also performs a credit analysis on the borrower.

The method used by P2P Lending has eliminated the intermediation function that has been carried out by banks so far. P2P Lending creates an online platform to provide facilities known as Providers (platforms) for fund owners to provide loans directly to borrowers with higher returns, while borrowers can apply for loans directly to fund owners through online organizers with relatively easier conditions, and process faster. Another advantage is that it is easy to compare with conventional financial institutions. When compared to conventional banks, the credit application process can take 7-14 days, while online loan services between 3-5 days the funds are liquid.

The practice of P2P Lending makes the community more and more choices in determining assistance regarding financial matters. Banks, which are usually the choice of alternative funding assistance, are now starting to be replaced with P2P Lending. The process for peer lending loans usually follows the following process (Saiedi et al., 2022):

1. The borrower enters the website,
2. Register and fill out the application form.
3. The platform then verifies and analyzes the qualifications of the loan.
4. Loans that have passed are posted on the website where the lender can provide a commitment of funds for the loan

Online loans can be accessed by downloading on the PlayStore for Android/IOS users and can be accessed via the website. These online loans offer easy conditions with fast disbursements. Required conditions include KTP, Family Card, NPWP, SIM, Telephone Number and have a Bank Account. Then the file is photographed and then uploaded. Likewise, the payment method is quite easy with transfers between banks or through the nearest Indomaret or Alfamart.

At present there are many disadvantages experienced by consumers in online loans, especially illegal online loans, as in the case that recently occurred the discovery of a "meme" spreading on WhatsApp that reads "I hereby declare that I am willing to be rotated for Rp. 1,054,000 for pay off my debt in the InCash application. Satisfaction guaranteed, those who are interested, contact immediately." This case can be solved criminally with the suspicion of spreading good name, but what needs to be seen in a civil context is how to protect customer personal data from being disseminated (Arifiyanto et al., 2020).

In the context of dissemination of personal data also found in RupiahPlus online loans. RupiahPlus is an unsecured credit platform launched by PT Digital Synergy Technology which has been registered and supervised by the Financial Services Authority (OJK) as one of the providers of information technology-based money lending services. In the RupiahPlus case, RupiahPlus charged credit payments by misusing the contact number list on the customer's cellphone. In fact, many people contacted from the list of contact numbers did not know anything about the loan.

Thus what RupiahPlus did not only violated consumer protection, but also disturbed the privacy of others who were not related to the loan. Seeing the many cases of misuse of personal data, it is very important to protect personal data. The importance of providing protection for personal data is starting to strengthen along with the increasing number of cell phone and internet users. A number of cases that have emerged, especially those related to the leakage of personal data and leading to acts of fraud or criminal acts of pornography, have strengthened the discourse on the importance of making laws to protect personal data. Personal data protection relates to private aspects (Kusnadi, 2021).

The private aspect is the idea of maintaining personal integrity and dignity. The right to privacy is also an individual's ability to determine who holds information about them and how that information is used. The concept of data protection implies that individuals have the right to determine whether or not they share or exchange their personal data. Apart from that, individuals also have the right to determine the conditions for carrying out the transfer of such personal data. Further, privacy protection. The right to privacy has grown so that it can be used to formulate the right to protect personal data.

In the context of transformative justice, it provides a sense of justice when one approach is intended to end a conflict. Facing digital transformation and very tough global competition, as well as the very strategic factor of big data, for legal certainty, the Personal Data Protection Agency that will be formed, and of course Law Enforcement Officials (APH), must consistently apply this principle. Legal certainty is an essential and fundamental element in the rule of law in Indonesia, because philosophically and pragmatically one of the objectives of law is certainty. Conflicts in personal data protection, especially in the case of online loans in Indonesia, must provide transformative justice in such a way as to wisely place restrictions on very personal matters, not applicable to the processing of personal data by individuals in personal or household activities.

Of course there are several indicators that can cause conflict in the aspect of personal data protection, especially in the case of online loans, including in the form of restrictions (Sinaga & Putri, 2020): (a) the prohibition of obtaining or collecting personal data that does not belong to himself, with the intention of benefiting himself or others, which can result in loss of the personal data subject; (b) the prohibition of disclosing personal data that does not belong to himself with the intention of

benefiting himself or another person which could result in the loss of the subject's personal data; (c) prohibition of using personal data that does not belong to him, with the intention of benefiting himself or others which can result in loss of the personal data subject; (d) prohibition of making false personal data or falsifying personal data with the intention of benefiting oneself or another person which could result in harm to another person.

### 1. PROBLEM

By looking at the considerations above, this research examines philosophically there is legal injustice in protecting the dignity of victims' personal data in various online loan cases in Indonesia and how consumer protection law formulations protect personal data when making online loan transactions. There have been many studies discussing the relationship between perpetrators and victims, but this is very different from what was studied, especially the dynamics and paradigm of protecting consumer personal data in online loan transactions in Indonesian positive law. This research has positive findings in the development of consumer protection law and electronic transactions in Indonesia and further research can be carried out in Indonesia regarding the relationship between the perpetrator and the victim.

Some of these legal arguments are structured within the framework of fair law enforcement between perpetrators and victims of online loan transactions within the scope of personal data protection based on the constitution in Indonesia, as well as offering solutions in its settlement. Therefore, this article has no conflict of interest with anyone.

### 2. RESEARCH METHOD

The research used in this research process uses a type of normative legal research (Van Hoecke, 2016). By using library materials or secondary materials that have been collected. Legal research is also a process to determine legal rules, legal principles, and legal doctrines in order to answer the legal issues faced. The basic materials used in this study came from library data. Everything related to data analysis is narrated holistically so that a complete combination is found and conclusions can be drawn in a balanced and structured manner using a deductive method.

### 3. RESULT AND DISCUSSION

#### 3.1 Several Cases and Analysis of Potential Forms of Online Loan Settlement in Indonesia

The rise of illegal online lending practices, according to economic observers, is caused by weak regulations, both from the supervisory system to law enforcement against fraudulent companies. On the other hand, this practice is also due to difficult economic conditions due to the Covid-19 pandemic and also the consumptive behavior of a digital society. From 2018 to October, 15<sup>th</sup> 2021, the Ministry of Communication and Information has closed 4,874 online loan accounts. Bareskrim Polri has arrested three suspects in an illegal online loan case from the Andalan Bersama Savings and Loan Cooperative and confiscated around IDR 21 billion (R. A. E. Wahyuni, 2020).

The Solusi Andalan Bersama Savings and Loans Cooperative, which has 34 illegal applications, is the suspected perpetrator of the terror of a mother in Wonogiri, Central Java, who decided to commit suicide because she was wrapped up in illegal online loans. In Wonogiri, when the victim committed suicide because of the heavy threats, it turned out that he had loans in 23 illegal applications, where the applications were managed by the Andalan Bersama Savings and Loan Cooperative. The Director for Economic and Special Crimes at Bareskrim Polri Brigadier General Helmy Santika said on the same occasion that the three suspects were JS, DN and SR. This case is one of a total of 15 cases of illegal online loans being handled by the National Police with 50 suspects - acting as operators, threats to financiers (Hu & Zheng, 2016).

Based on what has been stated above, it is necessary to analyze in relation to the fundamental basis of the Indonesian state which is mandated in Article 28 G (1) which states that everyone is essentially entitled to personal self-protection, both data are also related to the fundamental concept of a family right. , honor, dignity, and property under his control, and is entitled to a sense of security and protection from threats of fear in doing or not doing something which is a form of human rights.

This is reinforced by Article 30 (1) providing an interpretation that administrators are required to maintain the confidentiality, integrity and availability of personal data, transaction data and financial data that they manage from the time the data is obtained until the data is destroyed. There are many regulations that regulate the protection of personal data by showing the importance of personal data to be protected, but these regulations are still scattered in various regulations, so they cannot provide optimal and effective protection for personal data as part of privacy. Therefore it is necessary to formulate a law that can specifically provide personal data protection (Dawei et al., 2018).

Regulation of electronic transactions plays an active role as an indicator that protects society and the state from all disturbances of hacking, misuse, violations and crimes based on personal data



both carried out from within and outside the country. This is in line with the application of transformative law theory that the author is currently developing. Progressive application of extraterritorial jurisdiction and new legal principles, to welcome digital transformation, in line with this transformative legal theory (Hikmah, 2021). The principle of transformative law emphasizes that law, in addition to functioning to maintain order, justice, certainty and benefit, also functions as an infrastructure for transformation in various fields. Based on this principle, law is projected and functioned pragmatically as an instrument supporting transformation and not an obstacle to the transformation itself.

The many loopholes on the websites of companies or government agencies make it easier for a hacker or hacker with malicious intent to break into people's personal data (Chng et al., 2022). In addition, the lack of literacy in digital data security and the absence of definite laws in digital crime has opened the way for hackers to carry out their bad habits. This is supported by data compiled by katadata.id, Indonesia is in third place with the most number of accounts experiencing data leaks in the third quarter of 2022. With more than 12 million hacked accounts and cases increasing every month, the government must improve to overcome hacker attack in digital space for public security.

When looking at the reasons for hackers stealing personal data, quoted from dataindonesia.id, financial gain is the biggest motive for hackers to do hacking. The financial crisis during the pandemic forced everyone to make money in various ways. The high selling price of illegal personal data can make hackers earn millions to billions of rupiah every month. Meanwhile, social and political issues are also the motivation for hackers to hack data. Like the famous hacker named Bjorka who spread the personal data of several officials and public figures including the Minister of Communication and Information.

Bjorka's action is considered as an act of hacktivism which aspires to weak digital data security and the government's lack of efforts to protect it. Even though some people turned their backs on Bjorka's action because they felt that the hacker conveyed aspirations that they shared, this action was still a digital crime. This hacking action that occurred not only violated social norms, but also caused public unrest. There are still other ways to convey aspirations, such as submitting them on the lapor.go.id website, the government's official information system that accommodates aspirations and complaints from the public online. (Kohler et al., 2000).

Therefore, a clear legal umbrella is needed to reduce the number of personal data hacks. It is for this purpose, the Ministry of Communication and Information of the Republic of Indonesia (Kominfo). The role of companies and government agencies is also needed to strengthen digital data architecture. Companies and agencies that collect the public's personal data must be wise and responsible in managing the data they have. Companies can recruit capable people to manage their databases so that hackers do not easily commit data theft.

As a data owner, you can also take precautions to increase digital data security literacy, such as not using the same password for each account, being wise in sharing personal data (KTP, e-mail, etc.), and being careful when visiting sites or download fraudulent or phishing applications. Keep in mind, personal data is a matter of privacy that we both have to be able to take care of properly.

In this regard, there are several examples of cases of personal data misuse, including the following (Niffari, 2020):

- Online lending, where the transaction mechanism fills in data online and then in the event of a late payment it is not uncommon to use collectors to intimidate customers, the customer's family, to the leadership where the customer works. And some are even able to access data from the customer's cellphone.
- Online transportation, where consumers can experience sexual harassment via a WhatsApp number.
- Copying of customers' ATM card data and information (skimming), where the skimming actor withdraws funds elsewhere.

Based on these examples, it can be concluded that there is metadata in the form of personal data provided for various purposes (banking, e-commerce, and so on), voluntarily submitted and stored as digital data by business actors (or anyone who receives and stores personal data), is very vulnerable to being misused by recipient-data storage or stolen (hacked) by third parties. The misuse of personal data is so terrible, that everyone must understand how efforts can be made in order to protect their personal data.

In an effort to protect personal data, the following are steps that can be taken to maintain privacy while surfing the internet (Noor & Wulandari, 2021):

1. Use VPN

Virtual private network (VPN) is a service that allows each user to have a secure and private connection from a device to the internet network. This VPN service is usually used for computer or smartphone devices, with the aim of filtering internet connections so that users are not easily traced.

By using a VPN, online activities are not easily identified by other parties, protect online activities, and protect data from hackers.

## 2. Make a strong password

Memorizing a password is the first line of defense against hackers, so never use a password that is easy to guess and always use a complex password consisting of a combination of letters, numbers, and symbols.

## 3. Activate Double Factor Authentication Future

Two-factor authentication (2FA) is an extra layer of protection used to ensure online account security beyond usernames and passwords. In practice, this 2FA requires a code other than a password to log into certain accounts on the internet, where this code can be sent via text message to cellphone or email. This 2FA feature is considered very effective for protecting accounts when a hacker manages to find out your username and password. Because the hacker still won't be able to get into your account because you don't have an additional code.

## 4. Implementing the Data Encryption

Encryption is a process of securing data or information by changing plain text into text that humans cannot understand. In practice, data encryption will randomize information or data sent over the internet network. That way, other unauthorized parties cannot monitor activities and data sent online.

## 5. Using *Incognito Mode*

As is well known, that every browser can store history and passwords where this can make you vulnerable to hacking threats. The solution, you can use private browsing mode or incognito mode when using a public computer. With private browsing or incognito mode, all history and cache data will be erased when the browser is closed.

## 6. Activate Tracker Blocker

Most websites on the internet have used tracking tools on their websites, where these tracking tools aim to find out information about their visitors for marketing purposes, but unfortunately, these tracking tools can retrieve user data, such as location, computer IP, device used, and other information. If you want to maintain privacy, then you should use the tracker blocker feature on the computer or smartphone you are using.

## 7. Clean *Cookies* Periodically

Cookies are small pieces of data sent from a website and stored on a user's computer by a website browser when the user is opening a website page. Sites that are opened can use cookies on the device and make browsing activities faster, however, these cookies can make activity on the internet traceable by the site.

## 8. Always Be Careful in Giving Permissions

Every time you install an application on your cellphone, the application will definitely ask for certain permissions, for example permission to access certain cameras, mics, and folders. Make sure to only grant permissions to trusted apps, and only to the features that the app needs.

Some people may ask, what steps can be taken if they find that personal data has been misused by irresponsible parties, especially in fintech operations. It is stated in Article 26 (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, that every person whose rights are violated as referred to in the Article above, can file a lawsuit for damages generated.

Please note, in the use of information technology, personal data protection is a part of personal rights (privacy rights). Personal rights are the right to enjoy a private life and be free from all kinds of disturbances, the right to be able to communicate with other people without spying, and the right to monitor access to information about a person's personal life and data. Means, if someone feels aggrieved because their identity is used in the misuse of personal data, then that person can file a lawsuit for the losses obtained, the lawsuit in question is an Unlawful Action lawsuit.

When personal data is misused or even the system provider company fails to protect the user's personal data, there are two legal steps that the user can take (Primanta, 2020):

- First, the user can submit a complaint to the Ministry of Communication and Informatics of the Republic of Indonesia on the basis that the electronic information system provider has failed to protect the user's personal data.
- If the user wants compensation, then they can take the second step, namely filing a lawsuit in court.

By looking at some of the explanations above, the researcher's view is that the misuse of personal data is an extraordinary crime, which provides an argument that there are acts of unlawful acts committed by both individuals and groups of people to enrich personal assets and not in accordance with the constitution in Indonesia. With the note that the researcher provides universal principles for maintaining human dignity and worth as creatures of God Almighty based on a sense of social justice for all Indonesian people. When this misuse of personal data relates to the dynamics of

online loans in Indonesia, of course researchers argue that misuse of the law regarding all types of loans that result in fraud, is not justified in accordance with regulations and the constitution in Indonesia.

### 3.2 Philosophical Aspects of Legal Injustice Against Dignity and Dignity in Protecting Victims' Personal Data (Consumers)

Technological developments in Indonesia are growing rapidly. This is evidenced by the current millennial generation being able to explore the internet via cellphones and other electronic devices that can facilitate access to information and telecommunications. Supported by technology and advances in human resource thinking, it will add potential in the development of this digitalization era. In line with this digitization, many Indonesian people access information by collaborating in various fields, such as e-commerce, trading through electronic systems, and protecting consumers' personal data in online business.

This shows that there is a deviation from the behavior of the P2PL platform in using the personal data of customers or consumers. Even though 2020 has decreased, breaches of personal data are still an issue that must be considered considering that personal data is often misused in business transactions related to the use of information technology as found by the International Computer Science Institute (ICSI) which found that user data had been forcibly collected by 1,325 android applications. ICSI observes more than 88,000 applications on the Google Play Store and tracks data transfers from applications when users refuse the requested permissions. (Suryono et al., 2021).

This shows that information technology-based business actors have a great opportunity to violate personal data protection. According to Safenet's study, theft or misuse of personal data has three motives. First, the economic motive, this violation was carried out through illegal buying and selling of data. The second is political motives, this type of violation is carried out by utilizing data obtained illegally in the context of gaining power, such as openly disclosing personal data of political opponents. Third, the motive for the threat, which is carried out in order to threaten other people so that they feel afraid.

Based on these facts the protection of personal data in P2PL transactions is an important matter to study and find a constitutional basis so that all parties understand the importance of protecting personal data and its existence has a strong legal basis. The establishment of laws and regulations requires a constitutional basis, both formal and material, as the basis for the legitimacy of these regulations.

Personal data attached to a person is a basic right that must be protected by law in order to achieve the legal objectives of justice, certainty and benefit, as stated by Gustav Radbruch (Radbruch, 2002), that the law must be able to protect basic human rights that are harmed by others. Providing state protection for personal rights can increase human values and relations between individuals and society and can limit government power. Therefore, protection of personal data is important to realize in this information technology era.

In an effort to provide protection and welfare for parties, especially consumers of fintech lending, the state must make regulations or a set of regulations that can guarantee legal certainty in accordance with people's lives in facing new values. In the era of technology, transaction security is very important because its existence can build trust for consumers and business people. In order to strengthen consumers' bargaining position and ensure legal certainty in transactions, it is necessary to establish regulations that protect consumers in transactions using electronic means.

One form of consumer protection is protection of personal data, so that consumers' rights are protected and have legal certainty. Legal certainty is one of the teachings in the ideals of law (*idee des recht*) consisting of legal certainty (*rechmatigheid*), justice (*gerechtigheit*) and expediency (*doelmatigheid*). (Herlina, 2019).

These three legal ideals must proportionally exist in the applicable legal system so that a just and prosperous society can be realized harmoniously as mandated by the Preamble to the 1945 Constitution which functions as the philosophical foundation of the nation and state which adheres to the rule of law principle. In a legal state, the government has an obligation to realize justice and prosperity, as stated by Aristotle that the state must guarantee the realization of justice for every citizen.

Therefore, existing laws (*ius constitutum*) and existing laws (*ius constituendum*) must be realized in order to bring about justice. If it is related to the concept of progressive law, all regulations that hinder the realization of justice must be abandoned. In fintech lending transactions, the personal data of borrowers and lenders remains a privacy right that must be protected. Fintech lending platforms may not disseminate personal data that they control for purposes outside of the fintech lending transaction process, because such personal data is a person's privacy rights whose existence is guaranteed by the 1945 Constitution.

The state is the executor of people's sovereignty which must provide guarantees for the protection of citizens against the misuse of personal data. There are several reasons for the importance of protecting personal data (Bell, 2010);

- a. Prevent someone pretending to be you (phishing);
- b. Protecting financial data;
- c. Avoiding theft and robbery with information technology intermediaries and support;
- d. Avoiding Gender-Based Violence Online (KBGO) such as cyber grooming (deceiving), online harassment, hacking or hacking, invasion of privacy, threats to distribute personal photos or videos and defamation.

In the era of information technology, ensuring the security of personal data as information is something that must be done, including by implementing the CIA (Confidentiality) model, which is directed at providing protection for information so that it is not accessed by unauthorized parties. Integrity, which is done for protecting information from being changed by irresponsible people. Availability, giving rights to authorized parties to access information when needed).

Confidentiality is related to the necessity of the P2PL platform to store customer data by applying the principle of internal use only and encrypting it. on private data entered on its server. To ensure confidentiality, the P2PL platform also needs to be literate to its customers to create strong passwords (password strength) and not easily trust other people (attackers) in using information technology.

Integrity is carried out to ensure that every data that enters the server is maintained for accuracy, consistency and validity so that it cannot be changed and protected from threats that arise either intentionally or unintentionally. To maintain data integrity, several things can be implemented (Jayani, 2019);

- a. Apply strong encryption on data storage media;
- b. Implement strong validation to guarantee the legality of the access made;
- c. Tightening of access control so that not everyone can access the data stored.

*Availability is a method to ensure that data is ready to be accessed anytime and anywhere. To ensure that every company can implement several things, among others:*

- a. Having a disaster recovery plan;
- b. Have multiple power supply;
- c. Perform data backup regularly.

In a philosophical context, in the context of data protection, it is important to distinguish between data that was legally obtained but misused and data that was collected illegally (e.g. without consent) or stolen (through computer hacking). Data theft generally involves cyberattacks or data harvesting in other ways where the data subject is not aware of the collection or modification of their data. Meanwhile, the term data misuse is usually applied to personal data that was initially voluntarily and lawfully provided by a customer to a company, but then used (whether by the company or a third party) for purposes that are beyond the scope of legitimate reasons.

Personal information in the form of metadata that is collected by an individual, whether voluntary or mandatory, for various purposes is stored as digital data by a second party. Even though this metadata is very vulnerable to being stolen or misused by third parties for purposes that benefit them. For this reason, the need to manage personal information is important because personal data concerns one's privacy rights. The concept of privacy is the idea of maintaining personal integrity and human dignity. Apart from that, fundamentally, personal data can have economic value for third parties who do have the opportunity to make use of it.

Personal data can be interpreted as all information relating to a person's identity. It could be the expression of physical, physiological, genetic, psychological, economic, cultural and social identity. Personal data also contains information that is private in nature which differentiates its characteristics from other people. Until when Indonesia talks about personal data, Indonesia refers to all data or information that can be directly or indirectly linked to an individual or legal entity (Valerio et al., 2019).

On Government Regulation No. 82 of 2012 concerning Implementation of Electronic Systems and Transactions Article 1 (27) and Regulation of the Minister of Communication and Information Technology No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems Article 1 number 1 states that what is referred to as personal data is (Jimenez et al., 2019): *"Personal data is certain individual data that is stored, maintained, and kept true and protected by confidentiality."*

Decision Number 438/Pid.Sus/2020/PN.JKT.UTR has issues that can be raised, including: there is an opportunity to position a special institution for the protection of personal data that is in line with efforts to codify personal data protection laws; and there are difficulties in realizing the implementation of right to be forgotten in positive law in Indonesia. Interest in the difficulty of data deletion requests that have been widely disseminated or known as the principle of right to be forgotten. This is due to the many procedural and lengthy stages of the case in court. Even though law



is a product of politics, when the law exists, politics must obey the laws that govern it (Asep Bambang Hermanto, 2020).

Providing protection to the right to privacy means protecting the right to freedom of speech. That is, the right to privacy guarantees protection from the threat of fear to do or not do something that is a human right. The Electronic Information and Transaction Law is one of the components that underlies personal data, the fundamental thing of this law is actually an effort to accelerate the benefits and functions of law (regulations) within the framework of legal certainty. The provisions stipulated in the Electronic Information and Transaction Law, although the regulations are general, are quite comprehensive and accommodate all matters related to cyberspace. (Djanggih & Qamar, 2018).

### **3.3 The Legal Paradigm in the Protection of Consumer Personal Data Against Online Loan Transactions**

The results of previous studies, research conducted by Egi Anggriawan (Anggriawan, 2021) with the journal title "Legal Protection Against Debtors Threatened by Creditors in Online Debt Agreements" which focuses on legal security and user protection for debtors when threatened or terrorized, looking at it from the criminal law perspective of the Criminal Code, while this research examines legal protection from a protection perspective. Consumer law and the ITE Law as well as possible legal settlement steps. Then research was conducted by Muhammad Olifiansyah (Olifiansyah, 2021) with the journal title "Legal Protection of Personal Data Theft and the Dangers of Using Online Loan Applications" which focuses on legal protection for debtors related to the legitimacy of loans through illegal online loans, while this research examines legal protection from the perspective of consumer law protection and the ITE Law as well as steps possible legal solutions. Then research conducted by Raden Ani Eko Wahyuni, Bambang Eko Turisno (R. A. E. Wahyuni & Turisno, 2019) with the journal title "Illegal Financial Technology Practices in the Form of Online Loans Viewed From Business Ethics" which focuses on illegal online lending practices from the perspective of business ethics and legal sociology of legal compliance, while this research examines legal protection from the perspective of consumer law protection and legal protection. ITE and legal settlement steps that can be taken.

The condition of consumers who are weak and suffer many losses requires increased efforts to protect, so that consumer rights can be enforced. On the other hand, it should be noted that in providing protection to consumers, it should not actually kill the businesses of business actors, because the existence of business actors is essential in the country's economy. Therefore, provisions that provide protection to consumers must also be balanced with provisions that provide protection to business actors, so that consumer protection does not actually reverse the consumer's position from a weak position to a stronger one, and vice versa, a weaker business actor. Consumer protection is all efforts that guarantee legal certainty to provide protection to consumers.

Law Number 8 of 1999 concerning Consumer Protection was formulated with reference to the philosophy of national development in the context of building a complete Indonesian human being based on the state philosophy of the Republic of Indonesia, namely the state ideology Pancasila and the state constitution. This Law on Consumer Protection is an umbrella that integrates and strengthens law enforcement in the field of consumer protection, and does not deny that the possibility is still open for the formation of a new law which basically contains provisions that protect consumers, especially victims of debtors from illegal fintech.

Problems with the implementation of peer to peer lending-based financial technology still arise, so there is a need for laws and regulations because existing regulations have not been able to protect the interests of the community and the government through the Financial Services Authority (OJK) needs to increase awareness, outreach and anticipate and take action against illegal information technology service-based money lending service providers, namely by cooperating with all components, namely the Ministry of Communication and Informatics, the National Police to control unregistered and unlicensed applications so that the implementation of peer to peer lending based financial technology has legal certainty, justice, benefits and protection for public (Noor & Wulandari, 2021).

The researcher's view philosophically is first, ontologically there is legal uncertainty in imposing sanctions on online lending practices resulting in many victims experiencing fraud, so it is necessary to protect one's personal data and corporate crime in online lending practices using third party services such as debt collectors to threatening, carrying out acts of intimidating collection, spreading personal data, and sexual harassment through electronic media. Second, epistemologically there is a moral hazard for online lending practices (Jebari et al., 2021), thereby causing risks to victims and state losses to be able to commit crimes from the perspective of personal data protection and perpetrators of criminal acts in fraud in protecting personal data and corporate crimes in online lending practices. Third, axiologically injustice in imposing sanctions on online lending practices generally places more emphasis on administrative sanctions. Therefore, not only prioritizing the justice of a corporate crime

against illegal online lending practices, but also emphasizing aspects of personal data protection against illegal online lending practices in positive law in Indonesia.

The three aspects above provide a juridical basis that there are no preventive and repressive legal protection measures to protect victims of fraudulent online lending practices in the protection of one's personal data in positive law in Indonesia, resulting in minimal control and control. On the other hand, the Financial Services Authority (OJK) needs to take administrative legal action, for example revoking business licenses for corporate crime in illegal online lending practices in Indonesia. In addition, the researchers also argue that there is a legal vacuum in setting sanctions against illegal online lending practices in the protection of personal data of individuals and perpetrators of crimes regulated in RI Law No. 27/2022, so that the legal rationale is through Article 29 jo 45 of Law of the Republic of Indonesia Number 19 of 2016 concerning Information and Electronic Transactions (RI Law No.19/2016) with Article 26 jo 29 of the Financial Services Authority Regulation Number 77/POJK.01/2016 concerning Information Technology-Based Borrowing and Borrowing Services, along with Article 378 Criminal Code on Fraud.

This is sociologically, there is a social gap in providing a sense of justice for online loan providers to users and victims of online loan fraud, resulting in social conflict caused by legal ignorance in people's lives towards online loans and the consequences and legal risks.

At the theoretical level, the theory of dignified justice provides a transformative justice in resolving online loan conflicts in providing a sense of fairness to consumers in a form of personal data protection. (Asshiddiqie, 2006). A result of reflections and philosophical thoughts about the world, especially in this case, namely law, dignified justice is broader than just the concept of distributional justice, commutative justice and various other justices. Justice is a specific legal objective, which is sufficient to extend the concept of law, does not describe the overall purpose of law. Justice only determines the form of law. First, to determine the content and objectives, second, namely, expediency. In addition to these two legal objectives, there is a third objective, namely legal certainty. Ideally, the law should accommodate these three purposes.

### CONCLUSION

From a normative juridical perspective, Pemmen Kominfo No. 20/2016 concerning Protection of Personal Data in the electronic system which has been in effect since December 2016 has not been sufficient to provide protection either preventively or repressively to consumers in the form of online loans. Therefore, the government needs to immediately provide protection for customers' personal data so that it is not misused. In addition, there is a legal vacuum in setting sanctions against illegal online lending practices in the protection of personal data of individuals and perpetrators of crimes regulated in RI Law No. 27/2022, so that the legal rationale is through Article 29 jo 45 of the Republic of Indonesia Law Number 19 of 2016 concerning Information and Electronic Transactions (RI Law No.19/2016) with Article 26 jo 29 of the Financial Services Authority Regulation Number 77/POJK.01/2016 concerning Information Technology-Based Money-Lending Services, along with Article 378 of the Criminal Code concerning Fraud.

However, several things that need to be considered in a form of transformative justice are that the legal ideals must exist proportionally in the applicable legal system so that a just and prosperous society can be realized harmoniously as mandated by the Preamble of the 1945 Constitution which functions as the philosophical foundation of a nation and state that is adhering to the rule of law principle. Furthermore, at the level of dignified justice theory, it provides transformative justice in resolving online loan conflicts in providing a sense of justice to consumers in a form of personal data protection. In the end there are several ways that can be taken to ensure a transformative form of justice, including: (a). implement strong encryption on data storage media; (b). apply strong validation to guarantee the legality of the access being made; and (c). tightening of access control so that not everyone can access the data stored.


### ACKNOWLEDGEMENT

1. This article was not funded by anyone, either by private or government institutions.
2. This article follows the rules and ethics of writing that apply and all references that support the writing of this article can be reached.

### REFERENCES

- [1] A. Basha, S., Elgammal, M. M., & Abuzayed, B. M. (2021). Online peer-to-peer lending: A review of the literature. *Electronic Commerce Research and Applications*, 48. <https://doi.org/10.1016/j.elerap.2021.101069>
- [2] Anggriawan, E. (2021). Legal Protection for Debtors Threatened by Creditors in Online Debt and Credit Agreements. *JOURNAL OF LAW GLORY*, 3(2). <https://doi.org/10.30999/jph.v3i2.1440>
- [3] Arifiyanto, M. N., Nurjaya, I. N., Negara, T. A. S., & Sugiri, B. (2020). Legal politics regulation of self

- assessment system principles for taxpayer property reporting in general provisions and taxation procedures. *Research, Society and Development*, 9(11). <https://doi.org/10.33448/rsd-v9i11.10105>
- [4] Asep Bambang Hermanto. (2020). VIEWS ABOUT WHAT IS LEGAL POLITICS? *Syria Studies*, 7(1).
- [5] Asshiddiqie, J. (2006). Hans Kelsen's Theory About Law. In *Sekretariat Jenderal & Kepaniteraan Mahkamah Konstitusi RI* (Issue Jakarta).
- [6] Bell, J. (2010). Wolfgang Friedmann (1907-1972), with an Excursus on Gustav Radbruch (1878-1949). In *Jurists Uprooted: German-Speaking Emigré Lawyers in Twentieth Century Britain*. <https://doi.org/10.1093/acprof:oso/9780199270583.003.0016>
- [7] Budianto, A., Sihombing, J., Krissanti, V. D., Jamin, S., Pramono, R., & Purwanto, A. (2020). Obligation to prove appearance document authenticity as deemining claim exception. *Journal of Advanced Research in Law and Economics*, 11(3 (49)), 761-770.
- [8] Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. In *Computers in Human Behavior Reports* (Vol. 5). <https://doi.org/10.1016/j.chbr.2022.100167>
- [9] Darmiwati, & Syahfitri, T. (2021). Dampak Pinjaman Online Untuk Masyarakat. *Update.Com*, 2(3).
- [10] Dawei, L., Anzi, H., & Gen, L. (2018). Big Data Technology: Application and Cases. In *Handbook of Blockchain, Digital Finance, and Inclusion* (Vol. 2). <https://doi.org/10.1016/B978-0-12-812282-2.00004-8>
- [11] Dewi, S. (2009). Cyber Law Privacy Protection for Personal Information in E-Commerce Under International Law. In *Widya Padjadjaran, Bandung*.
- [12] Djanggih, H., & Qamar, N. (2018). Application of Criminological Theories in Cyber Crime Management (Cyber Crime). *Pandecta: Research Law Journal*, 13(1). <https://doi.org/10.15294/pandecta.v13i1.14020>
- [13] Erna Priliastari. (2019). THE IMPORTANCE OF PERSONAL DATA PROTECTION IN ONLINE LOAN TRANSACTIONS. *national Legal Magazine*, 49(2), 1-27. <https://doi.org/10.33331/mhn.v49i2.44>
- [14] Herlina, N. (2019). Penerapan Sanksi Administrasi dalam Hukum Perlindungan Konsumen. *Jurnal Ilmiah Galuh Justisi*, 7(2), 13.
- [15] Hikmah, N. N. (2021). Mengelola transformasi digital. *Jurnal Manajemen Dan Bisnis*, 1(1).
- [16] Hu, B., & Zheng, L. (2016). Digital finance: Definition, models, risk, and regulation. In *Development of China's Financial Supervision and Regulation*. [https://doi.org/10.1057/978-1-137-52225-2\\_2](https://doi.org/10.1057/978-1-137-52225-2_2)
- [17] Jayani. (2019). *Fintech P2P Lending and Payments Growing Fastest*. Katadata.
- [18] Jebari, J., Táíwò, O. O., Andrews, T. M., Aquila, V., Beckage, B., Belaia, M., Clifford, M., Fuhrman, J., Keller, D. P., Mach, K. J., Morrow, D. R., Raimi, K. T., Visioni, D., Nicholson, S., & Trisos, C. H. (2021). From moral hazard to risk-response feedback. *Climate Risk Management*, 33. <https://doi.org/10.1016/j.crm.2021.100324>
- [19] Jimenez, D., Valdes, S., & Salinas, M. (2019). International Journal of Technology for Business (IJTB) Popularity Comparison between E-Commerce and Traditional Retail Business. *International Journal of Technology for Business*, 1(1).
- [20] Kohler, A., Sipos, V., Sonntag, E., Penksza, K., Pozzi, D., Veit, U., & Bjork, S. (2000). Makrophytenverbreitung und standortqualität im eutrophen Bjorka-Kavlinge-Fluss (Skane, Sudschweden). *Limnologica*, 30(3). [https://doi.org/10.1016/S0075-9511\(00\)80060-2](https://doi.org/10.1016/S0075-9511(00)80060-2)
- [21] Kusnadi, S. A. (2021). LEGAL PROTECTION OF PERSONAL DATA AS A PRIVACY RIGHT. *AL WASATH Jurnal Ilmu Hukum*, 2(1). <https://doi.org/10.47776/alwasath.v2i1.127>
- [22] Niffari, H. (2020). PROTECTION OF PERSONAL DATA AS PART OF THE HUMAN RIGHTS TO PROTECTION OF PERSONAL PERSON A Comparative Review With Legislation In Other Countries. *Law And Business Journal (Selisik)*, 6(1). <https://doi.org/10.35814/selisik.v6i1.1699>
- [23] Noor, A., & Wulandari, D. (2021). Constitutional Foundation of Personal Data Protection in Fintech Lending Transactions in Indonesia. *World of Law Scientific Journal*. <https://doi.org/10.35973/jidh.v0i0.1993>
- [24] Nurmantari, N. N. A. D., & Martana, N. A. (2019). Legal Protection of Personal Data Borrowing in Online Loan Application Services. *Kertha Wicara: Journal of Law Science*, 8(12), 1-14. <https://ojs.unud.ac.id/index.php/kerthawicara/article/view/50656>
- [25] Olifiansyah, M. (2021). Legal protection for theft of personal data and the dangers of using online loan applications. *Journal of De'rechtsstaat Law*, 7(2).
- [26] Primanta, A. I. (2020). Criminal liability on the misuse of personal data. *Jurist-Diction*, 3(4). <https://doi.org/10.20473/jd.v3i4.20214>
- [27] Purba, N., Tanjung, A. M., Sulistyawati, S., Pramono, R., & Purwanto, A. (2020). Death Penalty and Human Rights in Indonesia. *International Journal*, 9, 1357.
- [28] Radbruch, G. (2002). Introducción a la filosofía del derecho. In *Breviarios. Filosofía del derecho* (Vol. 42).
- [29] Saiedi, E., Mohammadi, A., Broström, A., & Shafi, K. (2022). Distrust in Banks and Fintech Participation: The Case of Peer-to-Peer Lending. *Entrepreneurship: Theory and Practice*, 46(5).

- 
- <https://doi.org/10.1177/1042258720958020>
- [30]Sinaga, E. M. C., & Putri, M. C. (2020). LEGISLATION FORMULATION FOR PERSONAL DATA PROTECTION IN THE INDUSTRIAL REVOLUTION 4.0. *Jurnal Rechts Vinding: Media Development of National Law*, 9(2). <https://doi.org/10.33331/rechtsvinding.v9i2.428>
- [31]Suryono, R. R., Budi, I., & Purwandari, B. (2021). Detection of fintech P2P lending issues in Indonesia. *Heliyon*, 7(4). <https://doi.org/10.1016/j.heliyon.2021.e06782>
- [32]Valerio, C., William, L., & Noémier, Q. (2019). The Impact of Social Media on E-Commerce Decision Making Process, *International Journal of Technology for Business (IJTB)*. *Springwish Publisher, Bratislava*, 1(1).
- [33]Van Hoecke, M. (2016). Methodology of Comparative Legal Research. *Law and Method*. <https://doi.org/10.5553/rem/.000010>
- [34]Wahyuni, R. A. E. (2020). Strategy Of Illegal Technology Financial Management In Form Of Online Loans. *Jurnal Hukum Prasada*, 7(1). <https://doi.org/10.22225/jhp.7.1.1324.27-33>
- [35]Wahyuni, R. A. E., & Turisno, B. E. (2019). ILLEGAL TECHNOLOGICAL FINANCIAL PRACTICES IN THE FORM OF ONLINE LOANS IN VIEW OF BUSINESS ETHICS. *Journal of Indonesian Legal Development*, 1(3). <https://doi.org/10.14710/jphi.v1i3.379-391>
- [36]Wahyuni, W. (2021). LEGAL Aspects of ONLINE LOAN TRANSACTIONS. *Tadayun: Sharia Economic Law Journal*, 2(1). <https://doi.org/10.24239/tadayun.v2i1.14>