International Journal Publishing
INFLUENCE: International Journal of Science Review
Volume 5, No. 3, 2023
https://influence-journal.com/index.php/influence/index

Analysis of Personal Data Vulnerabilities in Legal Online Loan Transactions

Afronal[1], Maria Puspita[2], Muhammad Erza Aminanto[3]
[1,2,3]Universitas Indonesia, Depok, Indonesia
Email: afronal55@gmail.com

Abstract. This research examines the vulnerability of personal data in online loan transactions in Indonesia. Advances in financial technology have created a rapidly growing fintech industry, which includes online lending services. However, the use of personal data in these transactions carries serious potential risks related to the vulnerability of personal data. In this research, the author uses a descriptive qualitative approach by combining interviews and secondary data analysis from literature related to personal data protection in Indonesia. The research results show that personal data used in online loan transactions has a high attraction for irresponsible online loan managers. The vulnerability of personal data in online loan transactions is reflected in various threats, including cyber-attacks that can cause serious financial and reputational losses for individuals involved in these transactions. This will ultimately cause social and psychological costs for the victim. Stricter measures in protecting personal data and strengthening security policies in online loan applications are necessary to reduce the risk of these vulnerabilities. This research also identifies legal provisions governing personal data protection and underscores the need for awareness of privacy rights and data security in the fintech industry.

Keywords: *Personal Data Vulnerability, Online Loan Transactions, Fintech, Personal Data Protection, Cyber Attacks.*

A. INTRODUCTION

One of the impacts of technological progress is the presence of innovations in financial technology that have led to the birth of the financial technology industry, which is better known as fintech. Fintech is an abbreviation for "financial technology," which refers to the application of technology to provide financial products and services more efficiently, innovatively, and easily accessible (Palmié et al., 2020). According to Bank Indonesia regulation Number 19/12/PBI/2017 concerning the implementation of financial technology, financial technology is the use of technology in the financial system that produces new products, services, technology, and/or business models and can have an impact on monetary stability, financial system stability, and/or efficiency, smoothness, security and reliability of the payment system (Saraswati et al., 2020).

In Indonesia, the fastest growing thing is Fintech Lending or Fintech Peer-to-Peer Lending or Information Technology Based Money Lending and Borrowing Services (LPMUBTI). Currently, this service is better known as Online Loans or Pinjol. Online loans often operate in an environment with minimal supervision and strict regulation. This enables practices that harm consumers such as high interest rates, hidden fees, and aggressive billing practices. This lack of transparency can harm the national economy and has the potential to create financial instability (Cherednychenko & Meindertsma, 2019).

The ease of applying for an online loan comes with risks that many customers do not understand. By simply showing personal documents such as KTP, KK, NPWP, and pay slips, anyone can apply for an online loan to meet their financial needs. The transaction value is fantastic and continues to increase every year (Mhlanga, 2021). The following is the value of Pinjol distribution in Indonesia based on data from the Indonesian Joint Funding Fintech Association (AFPI):

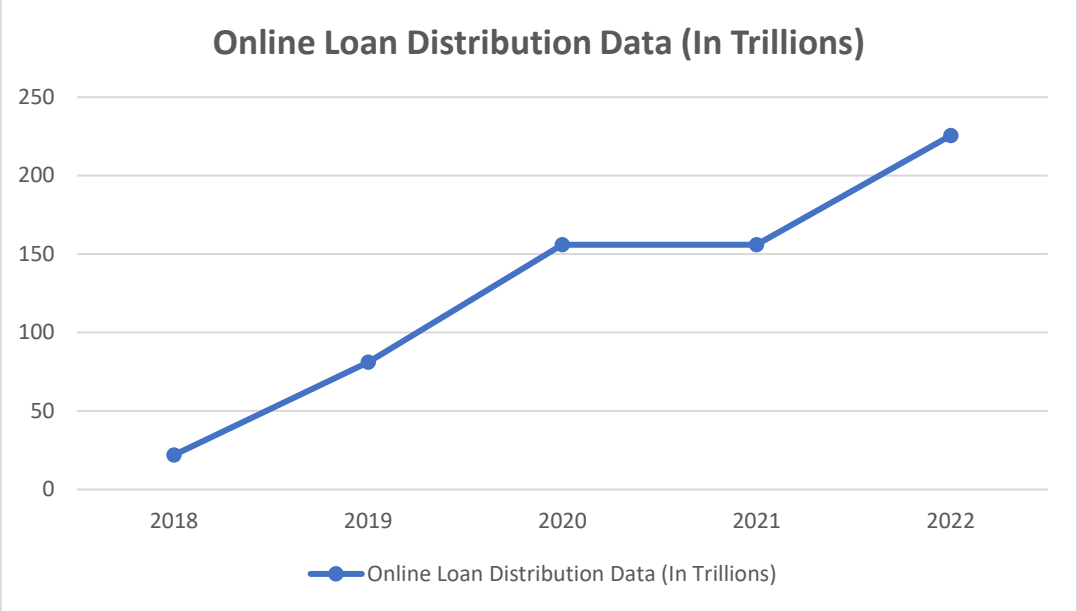

Figure 1. Data on Loan Distribution via Pinjol in Indonesia

From the table above, it can be seen that online loan distribution has increased significantly over the last few years. However, many problems are ultimately caused by this online loan. The ease of applying for an online loan comes with risks that many customers do not understand. By simply showing personal documents such as KTP, KK, NPWP, and pay slips, anyone can apply for an online loan to meet their financial needs. Based on YLKI data in the graph below:

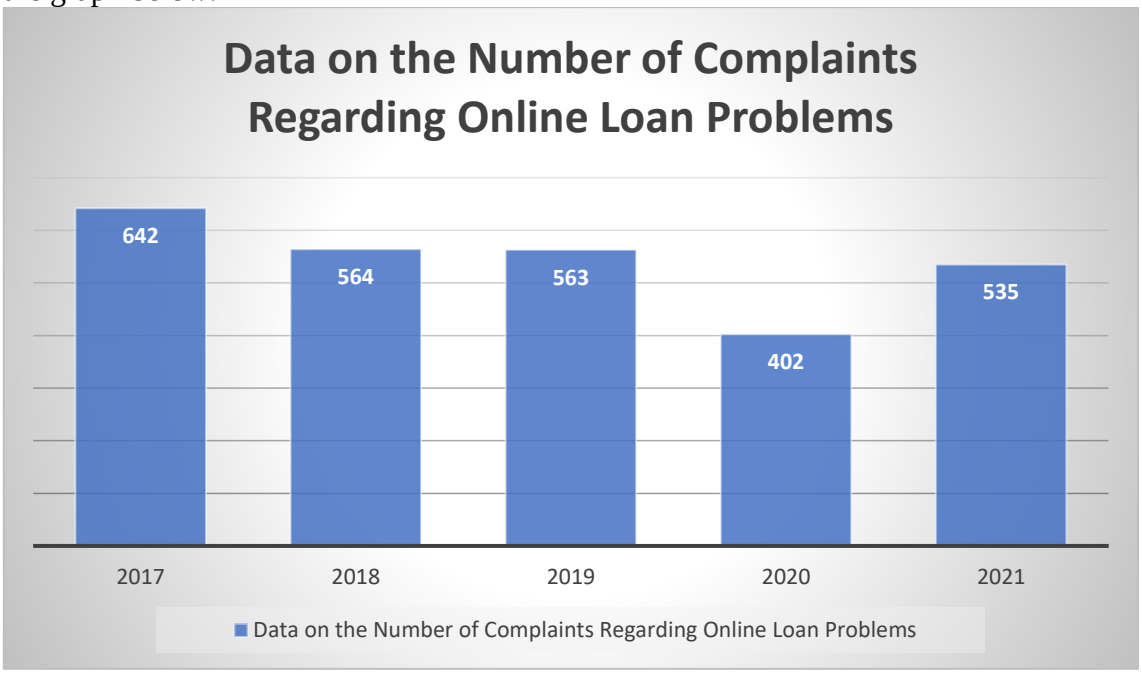

Figure 2. Number of Complaints Regarding Online Loan Problems for the 2017-2021 Period

Every year there are hundreds of complaints about Pinjol. The following is data held by YLKI regarding complaints about online loan problems. The problems that generally arise are in the form of disbursement without consent, threats of sharing personal data, billing all contacts, and billing using harsh words and sexual harassment. From this type of violation,

researchers concluded that it started with misuse of personal data held by Pinjol (Behera et al., 2023).

The vulnerability of personal data protection in online loan transactions is an issue of increasing concern along with the rapid growth of the fintech industry. According to Istiqamah, the risks in using online loans that usually occur are the high interest that has been set by the company, having to pay a service fee of 3-5 percent, a relatively short repayment limit, namely a maximum of 12 months; as well as the risk of data leakage and theft on online loan application users' cell phones (Hua & Huang, 2021).

In the context of online loan transactions, requests for consumer personal data are often justified as an effort to conduct better credit assessments and ensure that the borrower is an individual who is qualified to receive a loan. However, as stated by Priliasari, there are cases where the contact access provided by consumers is used by online loan companies for collection purposes. This raises privacy issues that need to be addressed (Hiller & Jones, 2022). According to Septiyani, individuals who become victims of misuse of personal data due to online loans will ultimately experience not only significant financial losses, but will also be threatened with loss of reputation, and experience serious emotional impacts (Brensinger, 2023).

Vulnerability of personal data in online loan transactions is a serious issue that requires in-depth attention. In this digital era, financial transactions, including online loans, require the collection of sensitive personal data, such as full names, identity numbers, addresses, and financial information. However, the security of this data is often inadequate, providing opportunities for cyber actors to access and misuse this data. Additionally, many online loan applications have not been properly verified, increasing the risk of unauthorized distribution of personal information. This not only has the potential to cause information leaks but can also lead to cases of fraud and identity theft which result in financial losses and psychological trauma for victims. Therefore, users need to verify the security and legitimacy of online lending platforms before sharing their data (Mogaji et al., 2020).

In an increasingly digitally connected era, challenges related to personal data protection have become increasingly complex. The continued growth of digitalization has brought us into an era where personal data has become a valuable commodity. In this context, vulnerability to personal data breaches does not only threaten individual privacy (Ahmad et al., 2021).

Based on the description above, this research aims to analyze the impact of personal data vulnerability on online loan transactions and provide recommendations to reduce the risk of personal data vulnerability. Based on the description above, this research aims to analyze the vulnerability of personal data in online loan cases using an intelligence approach. This research also aims to identify such vulnerabilities and provide better insight into their impact on digital resilience.

B. LITERATURE REVIEW

1. Vulnerability

According to Klein, vulnerability in ordinary language is a measure of the likelihood of future harm. Vulnerability is often related to the inability to overcome threats or events that may occur, thereby creating potential losses or negative impacts. Martha Fineman emphasized that the main emphasis of vulnerability theory is not human vulnerability, even though the theory starts from humans (Hansson et al., 2020). Fineman expressed that vulnerability must be understood as a universal constant, the human task then is to explore strategies that can reduce vulnerability. Thus, humans are not considered more or less vulnerable because they have certain characteristics and are at different stages in their lives with different levels of resilience (Sarmah et al., 2020).

Fineman takes the implications and politics of vulnerability theory seriously. He also proposed the idea of vulnerability from the perspective of state obligations. According to Fineman, the state is responsible for society's vulnerability because the state has legitimized and given power to social institutions. According to Pruckun, a vulnerability can be described as a weakness in an asset that can be exploited by threat agents. The term asset is used in this context to denote a resource that requires protection. A resource can be a person or persons or a group of people or a physical entity (for example, a critical piece of infrastructure) (Heikkilä et al., 2020).

Pruckun argues that vulnerability is the ability of an asset to withstand the danger posed by a threat. Losses can be anything from experiencing a minor disruption to a catastrophic situation. Vulnerability is a function of several factors - the attractiveness of the target, the feasibility of carrying out the attack, and the potential impact (Paul, 2022).

Since there is no single criterion for calculating vulnerability as each asset class may require specific considerations to be taken into account (and there may also be preferred institutional protocols), one common approach is to use a model like the image above. Vulnerability is described as the accumulation of something's attractiveness, the ease with which it can be attacked, and also what impact it will produce. Typically, these factors require considerations such as the status of the target, the potential for success of the attack, the potential for the threat agent to escape the attack, and the potential for causing losses (Masi et al., 2021).

In the context of personal data protection by the government. This understanding emphasizes the fundamental role of the state in protecting people from vulnerabilities related to their data. In this context, we can relate it to the way the Indonesian government protects the personal data of its citizens (Malgieri & Niklas, 2020).

2. Financial Technology and Online Loans

According to Rahayu, Fintech is a term used to refer to the latest advances in the field of financial services. It has become part of the world of new companies in the financial services sector, which plans to help streamline today's fast innovative progress to build the adequacy and productivity of financial services. According to Arjunwadkar, almost all FinTech companies provide services through their digital platforms, and can be accessed by customers through their mobile devices. Several sensors are being embedded in mobile devices to enhance smartphone hardware capabilities (Imerman & Fabozzi, 2020).

In Indonesia, financial technology is known as information technology-based money lending and borrowing services. Regarding fintech, it has been regulated in Financial Services Authority Regulation Number 77/POJK.01/2016 concerning information technology-based money lending and borrowing services. Article 1 Number 3 POJK 77/POJK.01/2016 states that information technology (fintech) based money lending and borrowing services are the provision of financial services to bring together lenders and loan recipients to carry out loan agreements in rupiah currency directly via electronic system using the internet network (Mutiara et al., 2019).

P2P Lending brings together fund owners (lenders) or what are usually called creditors with fund borrowers or debtors (borrowers) through an electronic application (without meeting face to face). According to Mateescu, P2P Lending is a description of an online market where lenders, also known as lenders, can lend to individuals or small businesses (borrowers) (Kgoroeadira et al., 2019). Online loans can be accessed by downloading on PlayStore for Android/IOS users and can be accessed via the website. These online loans offer easy terms with fast disbursement of funds. Required requirements include KTP, Family Card, NPWP, SIM, Telephone Number, and having a Bank Account. Then the file is photographed and

uploaded. Likewise, the payment method is quite easy by transferring between banks or through other payment methods (Castilla et al., 2023).

3. Personal Data

Personal data is often confused with the terms personal data (developed in Europe) or personal information (United States). Malaysia uses the term personal data, Singapore uses the term personal data, while the Philippines uses the term personal information, as do Japan and South Korea. The various terms used have substantially the same meaning. Meanwhile, according to the Big Indonesian Dictionary, personal data means data relating to a person's characteristics, for example, name, age, gender, education, occupation, address, and position in the family (Kozyreva et al., 2021).

Article 1 Paragraph (1) of the Personal Data Protection Law, defines personal data, namely: "Personal Data is any data about a person whether identified and/or identifiable individually or combined with other information either directly or indirectly through electronic and/or non-electronic systems" (Rahman & Wicaksono, 2021).

PP no. 82 of 2012 concerning Electronic Systems and Transaction Operators, defines personal data as "certain individual data that is stored, maintained, maintained as correct and protected as confidential" (Article 1 paragraph 27). There are two types of data types in the Personal Data Protection Law, namely general personal data and specific data, this is stated in Article 3 paragraph (1-3) of the Personal Data Protection Law. General data includes full name, gender, nationality, religion, and/or Personal Data combined to identify a person (Ducato, 2020). Meanwhile, specific ones include:

a. Health data and information;
b. Biometric data;
c. Genetic data;
d. Sexual life/orientation;
e. Political views;
f. Criminal record;
g. Child data;
h. Personal financial data;
i. Other data follow statutory provisions (Putri & Martha, 2021).

C. METHOD

This research is a type of descriptive qualitative research. According to Creswell, qualitative methodology is seen as a form of research that produces descriptive data obtained through information obtained from research subjects, complemented by data sourced from document studies. In this research, the data collection method used involved interviews. This interview was designed to gain in-depth insight into the vulnerability of personal data in electronic loan transactions in Indonesia. This approach provides a more practical and contextual view of the issue of personal data protection. Apart from interviews, this research also relies on secondary data sourced from literature related to personal data protection in Indonesia. This data covers various legal aspects, regulations, and the latest trends in personal data protection. This use of secondary data allows researchers to compare findings from interviews with Vulnerabilities of personal data in electronic loan transactions with broader frameworks that have been developed in the literature. This combined approach allows researchers to investigate the issue of personal data vulnerability more comprehensively and in-depth while ensuring that the resulting findings and analysis are well-founded and reliable based on empirical data and relevant theoretical frameworks (Sugiyono, 2018).

D. RESULT AND DISCUSSION

1. Level of Vulnerability of Personal Data in Online Loan Transactions

In online loan transactions, personal data vulnerabilities can open the door to various serious threats to information security. Tracking these threats is essential to identify and address potential risks that could affect the integrity, confidentiality, and availability of personal data. One threat that can arise is a cyber-attack, where online loan applications can exploit security gaps to access and steal sensitive consumer information. This threat can be detrimental to individuals involved in online loan transactions as it causes serious financial and reputational losses.

In vulnerability analysis, Prunckun provides 3 (three) elements that can be used to assess vulnerability, namely attractiveness, ease of attack, and resulting impact. Based on the results of an interview on December 7, 2023, Police Commissioner Akta Wijaya, S.H, S.I.K, M.Si, who serves as Head of Unit 4 Sub-Directorate III of Dittipidsiber Bareskrim Polri provided the following vulnerability assessment:

"*If I assess it using these variables, I can judge that attractiveness seems to be in the high category, right? "I mean, in terms of online loans, personal data can be bought and sold, so there are many factors that can motivate the perpetrators, and it seems like it's getting bigger and bigger here, right?*"

"*.....The ease of being attacked also seems to be high, if you look at the loan transactions, there are many loopholes in the application, yes, but the security policy of the application and its users also lacks control...*"

"*.....This impact seems quite dangerous because apart from personal data being stolen and used for crime or misused, it can cause financial loss for the victim*".

This is in line with Hendro Wijayanto's research which revealed disturbing practices in the fintech sector, especially related to the security of customers' data. They found that some fintech applications, during the installation process, performed activities similar to malware. This activity, which is suspected to be intentional by fintech administrators, aims to collect customers' data more widely. Data taken illegally can be misused and of course, be detrimental to customers.

This practice not only raises serious questions about the ethics and responsibilities of fintech companies but also represents a clear violation of the law. According to applicable regulations, application vendors are not allowed to access customer information or personal files without clear approval. This raises serious concerns regarding the protection of consumer privacy and data security, which should be a top priority in today's digital era. Awareness of privacy rights and data security must be increased, both by users and regulators, to ensure fair and transparent practices in the fintech industry.

From the analysis of interview results, it can be seen that the vulnerability of personal data in legal online loan transactions is a serious issue. Stricter measures in protecting personal data and strengthening security policies in online loan applications are necessary to reduce the risk of these vulnerabilities. This is of course contrary to the provisions of POJK NUMBER 77/POJK.01/2016 where P2P Lending Operators, in carrying out their business activities, have obligations related to the data they obtain, namely:

a. Maintain the confidentiality, integrity, and availability of personal data, transaction data, and financial data that it manages from the time the data is obtained until the data is destroyed;
b. Ensure the availability of authentication, verification, and validation processes that support irrefutability in accessing, processing, and executing personal data, transaction data, and financial data that it manages;

c. Guarantee that the acquisition, use, utilization, and disclosure of personal data, transaction data, and financial data obtained by the Operator is based on the consent of the owner of the personal data, transaction data, and financial data, unless otherwise determined by statutory provisions;
d. Providing other communication media besides the Information Technology Money Lending and Borrowing Service Electronic System to ensure continuity of customer service which can be in the form of electronic mail, call centers, or other communication media;
e. Notify in writing the owner of the personal data, transaction data, and financial data if there is a failure to protect the confidentiality of the personal data, transaction data, and financial data they manage.

Personal data has high appeal and is vulnerable to misuse in the context of online lending. Personal information held by individuals is often an attractive target for online loan providers. Such providers, if irresponsible, may exploit this personal data for their benefit, which could result in serious risks for the individuals who have provided the data. This vulnerability emphasizes the need for stringent measures to protect personal data and enhance security protocols in the online lending sector to protect sensitive user information.

2. Handling Cases of Misuse of Personal Data

In terms of enforcing regulations and handling legal processes for misuse of personal data, Police Commissioner Akta Wijaya, S.H, S.I.K., M.Si., who serves as Head of Unit 4 Sub-Directorate III of Dittipidsiber Bareskrim Polri. Based on the results of an interview on December 7, 2023, he gave the following answer:

"*For the alleged articles that are commonly used for criminals who misuse personal data, according to the ITE Law articles 32 and 35, the threat is 8 - 12 years. "But in terms of regulations, there is nothing special in the context of online loans*".

From the answer above it can be seen that there are no special regulations regarding misuse of personal data in the context of online loans. Without adequate regulations, online loan companies do not have a truly binding obligation to protect customers' data securely. This increases the risk of data leaks, where sensitive information such as bank account numbers, identity numbers, and addresses could fall into the wrong hands.

The high level of vulnerability of personal data in online loan transactions of course requires quite strong supervision. Monitoring and protecting personal data is a complex and multidimensional responsibility that requires cooperation from various parties. This is following the results of an interview on December 7, 2023, with Police Commissioner Akta Wijaya, S.H, S.I.K, M.Si, who serves as Head of Unit 4 Subdit III Dittipidsiber Bareskrim Polri:

"*Of course, there is collaboration from the National Police's Cyber Crime Section with other institutions or agencies. It's just that there is no specific collaboration regarding online loans. More cases of misuse of personal data. Collaboration with Kominfo, Dukcapil, and Kemenkumham to facilitate coordination*".

"*For the context of online loans, we involve service providers, there are several platforms. Then there is also a payment gateway which provides online disbursement and collection services for loan funds*".

From the interview above, it can be seen that there is a need for strong supervision of online loan transactions. The results of the interview also highlight the importance of cooperation between various parties, including the National Police's Cyber Crime Section, other institutions or agencies such as Kominfo, Dukcapil, and the Ministry of Law and Human Rights. This reflects a multidimensional approach to addressing personal data security issues.

The challenges that arise in overcoming personal data vulnerabilities in online loan transactions are very complex. According to Kompol Akta Wijaya, S.H, S.I.K, M.Si, who serves as Head of Unit 4 Sub-Directorate III of Dittipidsiber Bareskrim Polri in an interview on December 7, 2023:

> "*The challenge is quite difficult, sometimes the perpetrators are anonymous and transnational, so it requires expertise, facilities, and a fairly large budget. "Apart from that, the data needed is between bureaucracies, because there is no special task force for online loans, so sometimes the data takes a while to obtain*".

From the results of the interview above, it can be seen that special cooperation is needed so that the law enforcement process for criminals who misuse personal data in online loan transactions can proceed more quickly. In addition, the existence of various service providers and payment gateways in the online lending ecosystem can be a challenge in coordinating data protection efforts effectively. Furthermore, the rise of sophisticated cyber-attack techniques also poses a significant challenge, with anonymous and transnational actors continuing to innovate to steal users' data.

Finally, consumer awareness of the risks of personal data in online transactions also needs to be increased, so that they are more careful in sharing their personal information. All of these challenges emphasize the need for a comprehensive approach involving cooperation between various parties, stricter regulations, and better consumer education to address personal data vulnerabilities in online loan transactions.

This is following the results of an interview on December 7 2023 with Police Commissioner Akta Wijaya, S.H, S.I.K, M.Si, who serves as Head of Unit 4 Subdit III Dittipidsiber Bareskrim Polri:

> "*The National Police's Cyber Crime Section, we are involved in increasing public awareness of the risks of misuse of personal data. Through socialization or online. "We socialize the importance of protecting personal data and providing personal data according to needs, especially in online loan transactions*".

3. Impact of Personal Data Vulnerabilities in Online Loan Transactions

The existence of personal data used in online loan transactions opens the door to various serious cyber-attack threats. This can have social and psychological impacts that can be experienced by individuals involved in this transaction. Cyberattacks involving multiple individuals or even an online lending company can have far-reaching social impacts. This could include loss of public trust in online financial systems, stricter regulation, or social costs arising from responding to and recovering from such attacks.

The social costs of personal data vulnerability in online loan transactions may also include aspects involving the treatment of victims when they have to report data breaches to authorities, such as the police. Reporting a data breach can often be an uncomfortable experience for the victim. They may feel exposed, anxious, or even embarrassed because they have been the victim of a crime. This can impact the victim's psychological well-being and create additional social stress that they may face.

Additionally, the process of reporting and investigating data breaches can also take time and resources, both for individuals and authorities. This creates a social burden that must be borne by society and the legal system. Therefore, protecting personal data is not only important to prevent data vulnerability, but also to reduce the social impact that may arise when a data breach occurs and involves the authorities.

Victims of cyberattacks often experience significant psychological distress as a result of the privacy breaches they experience. These experiences can create a variety of emotional reactions that can impact the mental well-being of the affected individual. The psychological

stress that arises from cyber-attacks can have a negative impact on the victim's mental well-being. This can cause symptoms such as anxiety, depression, prolonged stress, and sleep disorders.

In the online lending ecosystem, potential threats to personal data include cyber-attacks, identity fraud, and information leaks. Alarming practices, such as unauthorized data collection, raise doubts regarding ethics and legality. This is contrary to existing data protection regulations. From the results of an interview with Kompol Akta Wijaya, S.H, S.I.K, M.Si, as Head of Unit 4 Sub-Directorate III Dittipidsiber Bareskrim Polri, the level of vulnerability of personal data in online loan transactions is included in the high category. This is because personal data has high attractiveness, is easy to attack, and has a big impact on its misuse.

The impact involves not only financial loss but also psychological distress and reputational damage that can significantly harm consumers. Therefore, a comprehensive solution is needed that includes strong privacy protections, stricter regulations, and effective countermeasures to protect consumers from the risk of personal data breaches in the increasingly complex and rapidly evolving fintech industry.

E. CONCLUSION

Online loan transactions are attractive to irresponsible loan managers because personal data is the main focus. The existence of personal data vulnerabilities in these transactions creates various threats, especially through cyber-attacks that can cause serious financial and reputational losses for the individuals involved. The impact of this cyber-attack is not only limited to material losses but also has the potential to cause significant social and psychological costs for victims. In dealing with the risk of this vulnerability, stricter measures are needed to protect personal data and strengthen security policies in online loan applications. This research emphasizes the need to implement proactive measures to reduce the risk of vulnerabilities that can affect many individuals. The implementation of sophisticated security policies and continuously evolving technologies can be important solutions for protecting the integrity of personal data. In addition, the importance of understanding the legal provisions governing personal data protection should not be overlooked. This research highlights the need for awareness of privacy rights and data security in the fintech industry. By understanding and respecting the legal aspects governing data protection, both loan managers and individuals carrying out transactions can together create a safer and more trustworthy online environment.

REFERENCES

1. Ahmad, T., Zhang, D., Huang, C., Zhang, H., Dai, N., Song, Y., & Chen, H. (2021). Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. *Journal of Cleaner Production*, *289*, 125834.
2. Behera, R. K., Bala, P. K., & Rana, N. P. (2023). Assessing factors influencing consumers' non-adoption intention: exploring the dark sides of mobile payment. *Information Technology & People*, *36*(7), 2941-2976.
3. Brensinger, J. (2023). Identity Theft, Trust Breaches, and the Production of Economic Insecurity. *American Sociological Review*, *88*(5), 844-871.
4. Castilla, R., Pacheco, A., & Franco, J. (2023). Digital government: Mobile applications and their impact on access to public information. *SoftwareX*, *22*, 101382.
5. Cherednychenko, O. O., & Meindertsma, J. M. (2019). Irresponsible lending in the post-crisis era: Is the EU consumer credit directive fit for its purpose?. *Journal of Consumer Policy*, *42*(4), 483-519.
6. Ducato, R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review*, *37*, 105412.

7. Hansson, S., Orru, K., Siibak, A., Bäck, A., Krüger, M., Gabel, F., & Morsut, C. (2020). Communication-related vulnerability to disasters: A heuristic framework. *International journal of disaster risk reduction*, *51*, 101931.
8. Heikkilä, M., Katsui, H., & Mustaniemi-Laakso, M. (2020). Disability and vulnerability: a human-rights reading of the responsive state. *The International Journal of Human Rights*, *24*(8), 1180-1200.
9. Hiller, J. S., & Jones, L. S. (2022). Who's Keeping Score?: Oversight of Changing Consumer Credit Infrastructure. *American Business Law Journal*, *59*(1), 61-121.
10. Hua, X., & Huang, Y. (2021). Understanding China's fintech sector: development, impacts and risks. *The European Journal of Finance*, *27*(4-5), 321-333.
11. Imerman, M. B., & Fabozzi, F. J. (2020). Cashing in on innovation: a taxonomy of FinTech. *Journal of Asset Management*, *21*, 167-177.
12. Kgoroeadira, R., Burke, A., & van Stel, A. (2019). Small business online loan crowdfunding: who gets funded and what determines the rate of interest?. *Small Business Economics*, *52*, 67-87.
13. Kozyreva, A., Lorenz-Spreen, P., Hertwig, R., Lewandowsky, S., & Herzog, S. M. (2021). Public attitudes towards algorithmic personalization and use of personal data online: Evidence from Germany, Great Britain, and the United States. *Humanities and Social Sciences Communications*, *8*(1), 1-11.
14. Malgieri, G., & Niklas, J. (2020). Vulnerable data subjects. *Computer Law & Security Review*, *37*, 105415.
15. Masi, A., Lagomarsino, S., Dolce, M., Manfredi, V., & Ottonelli, D. (2021). Towards the updated Italian seismic risk assessment: exposure and vulnerability modelling. *Bulletin of Earthquake Engineering*, *19*, 3253-3286.
16. Mhlanga, D. (2021). Financial inclusion in emerging economies: The application of machine learning and artificial intelligence in credit risk assessment. *International journal of financial studies*, *9*(3), 39.
17. Mogaji, E., Soetan, T. O., & Kieu, T. A. (2020). The implications of artificial intelligence on the digital marketing of financial services to vulnerable customers. *Australasian Marketing Journal*, j-ausmj.
18. Mutiara, U., Candanni, L. R., & Hasibuan, R. R. (2019). Construction of Financial Technology in Banking Systems in Indonesia. *Jurnal Hukum NOVELTY*, *10*(02), 150-163.
19. Palmié, M., Wincent, J., Parida, V., & Caglar, U. (2020). The evolution of the financial technology ecosystem: An introduction and agenda for future research on disruptive innovations in ecosystems. *Technological forecasting and social change*, *151*, 119779.
20. Paul, K. S. (2022). Surviving Meltdowns That Cannot Be Prevented: Review of Gaps in Managing Uncertainty and Addressing Existential Vulnerabilities. *Journal of Risk and Financial Management*, *15*(10), 449.
21. Putri, E. P., & Martha, A. E. (2021). The Importance of Enacting Indonesian Data Protection Law as a Legal Responsibility for Data Leakage. *Varia Justicia*, *17*(3), 287-303.
22. Rahman, F., & Wicaksono, D. A. (2021). Examining the Reference of Personal Data Interpretation in Indonesian Constitution. *Jurnal Penelitian Hukum De Jure*, *21*(2), 187-199.
23. Saraswati, B. D., Maski, G., Kaluge, D., & Sakti, R. K. (2020). The effect of financial inclusion and financial technology on effectiveness of the Indonesian monetary policy. *Business: Theory and Practice*, *21*(1), 230-243.
24. Sarmah, T., Das, S., Narendr, A., & Aithal, B. H. (2020). Assessing human vulnerability to urban flood hazard using the analytic hierarchy process and geographic information system. *International Journal of Disaster Risk Reduction*, *50*, 101659.

25. Sugiyono, S. (2018). *Metode Penelitian Pendidikan Pendekatan Kualitatif, Kuantitatif dan R & D*. Bandung: Alfabeta.