

Criminal Law Enforcement Against Digital Financial Services Sector Companies for Misuse of Consumer Personal Data

Ananda Putri Nur Amalina, Sahat Maruli Tua Situmeang

Fakultas Hukum, Universitas Komputer Indonesia, Bandung
sahat@email.unikom.ac.id

Abstract. This study aims to analyze criminal law enforcement against companies in the financial services sector for misusing consumers' personal data. The research method used is normative juridical, using both literature data which includes primary legal material in the form of applicable laws and regulations as well as secondary legal material in the form of scientific journal literature, books and other supporting sources and analyzed with a descriptive approach regarding the extent of sanctions imposed given as a result of misuse of personal data. The results of this study are criminal law provisions against companies in the financial services sector that misuse consumers' personal data are regulated in Law Number 27 of 2022 concerning Protection of Personal Data. Law enforcement against the protection of personal data by companies in the financial services sector requires legal political clarity from the current provisions. So it is necessary to take steps to optimize the application of criminal sanctions against companies in the financial services sector that misuse the personal data of their customers.

1. Introduction

Technological developments have provided real major transitions to various aspects of life. No exception to changes in patterns of behavior of society globally. Specifically, in the current era of globalization, almost all community activities depend on technology. One of them is towards economic and financial activities which are now starting to switch to digital technology-based financial services. One of these advances is marked by the presence of Financial Technology (Fintech). Financial Technology is the use of technology in the financial system that produces new products, services, technology and business models and has an impact on monetary stability, financial system stability, or the efficiency, smoothness, security and reliability of payment systems.[1] Fintech emerged as a new breakthrough that succeeded in producing system transformation towards practicality, ease of access, convenience and quite economical costs.

The implementation of financial technology has led to the decentralization of the financial system, namely a condition in which the functions of centralized financial intermediary institutions, namely banks, have been eliminated or reduced. The function of the bank from the economic aspect is an entity that collects public funds to be distributed to the community. In other words, the decentralization of the financial system has resulted in the implementation of the financial services sector no longer involving or at least no longer relying on traditional centralized intermediaries (banks), but can be carried out by the parties directly.[2] The impact of financial technology can be seen in the financial services sector, which is currently digital-based. Financial service products are formally offered by financial service institutions that are licensed, regulated and supervised by the Financial Services Authority (OJK). OJK regulates the entire financial services industry in Indonesia, which consists of the banking, capital market, insurance, financing, pension funds and other financial services industries. However, what will be discussed in this study is that financial technology is developing rapidly in three financial service

sectors including digital banking, the financing industry (Peer to peer lending), and the insurance industry. Through financial technology, the banking sector in Indonesia can simplify and accelerate financial transactions through electronic/digital means. This service can be performed by customers themselves to obtain information, register, open accounts, banking transactions, close accounts, and other needs. Other advanced features related to digital banking activities are e-wallets and electronic money which have the same function as cash to make all forms of payment.

The same phenomenon also occurs in the financing sector or commonly known as money lending services which after digitizing the system becomes Peer-to-peer lending (P2PL), where the company is the party providing online services to speed up the process which most consumers avoid on the grounds of the length of time conventional credit application process (visiting the office of the relevant financing institution). P2PL has also experienced significant development in Indonesia. Based on data from the Financial Services Authority of the Republic of Indonesia (OJK), until May 2021, there were 118 conventional P2PL companies and 9 registered sharia P2PL companies. Meanwhile, based on the composition of its use, there are two types of fintech with the largest usage composition in Indonesia. P2PL fintech occupies the first position with a percentage of 43%. The second position is occupied by fintech in the field of payments with a percentage of 33%. [3] Several insurance companies also provide mobile-based services, starting from the process of registering a policy to buying insurance products online, so there is no need to go to an insurance agent. Another form of digitization of insurance companies is filing claims online. Consumers only need to submit the necessary documents and evidence through the mobile system in submitting claims. Digital development transformation in the insurance company industry can also provide information that can make it easier for insurance policy holders to obtain information related to their insurance products.

However, it cannot be denied that today's information technology seems to be a double-edged sword, because in addition to contributing to the improvement of human welfare, progress and civilization, it is also an effective means of action against the law. [4] In addition to its sophistication that makes activities easier, digitalization in the financial services sector is still inseparable from the threat of crime that lurk. The potential for this crime arises from the risk of easy access to both transactions and authorizations. This threat also arises due to the storage of consumer data that is not based on the company's prudence. Crimes that are rife with consumers of financial services are consumers' personal data. Personal data is someone's data that is stored, cared for, kept true, and protected confidentially. Complaints about misuse of personal data experienced by consumers of financial services have often been received by the OJK, but law enforcement on personal data protection in Indonesia is still not effective even though this crime already has several regulations aimed at protecting consumers and their personal data.

One of the cases of misuse of personal data of users of financial services, especially financial services digital financing P2P Lending, namely the case that occurred with YI, who started by borrowing Rp. 1,000,000.00 (one million rupiah) through one of the P2PL applications for the purpose of paying for their child's education. YI followed all the requirements and instructions for registration in the P2PL application such as filling in personal data, uploading self photo, personal identity card, and others. After the loan application is approved by the P2PL organizer, the loan funds submitted are deducted by the P2PL for administrative costs. When it was due, YI's brother was required to pay the entire loan, but at that time YI's brother could not repay the loan until there was an accumulation of fines and interest of Rp. 70,000.00 (seventy thousand rupiah) per day. Furthermore, to pay off the loan, YI applied for a loan again through another P2PL application. Until finally the amount of YI's loan reached Rp. 30,000,000.00 (thirty million rupiah). Unable to pay, YI continued to receive phone calls from one of the P2PL operators he used with the aim of collecting loan payments accompanied by fines and interest from YI. The telephone call was also accompanied by a tone of threat from the collector. It didn't stop there, the terror of billing continued, the P2PL application that YI used also made a poster that included a photo of himself accompanied by threatening words that the poster would be distributed if YI did not pay off the loan immediately. The P2PL also created a Whatsapp group consisting of YI's friends and relatives, in the group conversation there was harassment by P2PL in the form of posting a photo of YI. It is

known that previously there had been a similar case against women who made loans through the P2PL application. Then the P2PL created a Whatsapp group and provided false information that the woman was "willing to take turns" in negative context for Rp. 1,054,000.00 (one million fifty four thousand rupiah) to pay off the loan.[5]

The rise of crimes that have occurred has created anxiety in the community that public trust will decrease in the available business services in the financial services sector. If this is allowed, of course it will have an impact on the condition and development of the national economy. Therefore, issues related to personal data protection are a very important concern. In other words, personal data security is a manifestation of a person's right to privacy which is important to protect.[6]

2. Method

In this study, the normative juridical method was used by proposing a rule of law, principles, and legal doctrines to answer existing legal problems. The data material used in this study is secondary data obtained from search results in the literature and from various journals. The technique used is literature study which is carried out through the processing of secondary legal materials. Data analysis was carried out using a statutory approach and a conceptual approach. The statutory approach is an approach that is carried out using legislation and regulations. While the conceptual approach is the approach taken by researchers according to existing legal regulations. [7]

3. Results and Discussion

1) Legal Arrangements Against the Misuse of Consumer Personal Data in the Financial Services Sector

The practice of misusing personal data and disturbing the privacy of consumers of financial services has been rife. This not only causes material losses but also traumatizes the community. Many cases have occurred where consumers often complain that their personal data is being disseminated by organizers without notification and without the consent of the owner of their personal data. OJK recorded no less than 19,711 public complaints from 2019 to 2021, including cases of serious violations, namely the distribution and misuse of personal data.[8] The usual mode is dissemination and disclosure of personal data accompanied by threats, blackmail to intimidation during the consumer billing process. Various types of personal data violations have claimed many victims, including: taking almost all of the information contained on consumer devices as many as 1330 victims, billing that is not only done to consumers or emergency contacts as many as 1100 victims, dissemination of personal data as many as 915 victims and ID cards used to file loans in other applications by the organizers of 1 victim.[9]

The irony is that this crime is often committed by financial service business actors who should pay attention to aspects of protecting consumers' personal data. There is a legal subject provision in Article 1 of Law Number 27 of 2022 concerning Personal Data Protection which states that legal subjects who can be held responsible for crimes against personal data include legal subjects of persons (natuurlijk persoon) and also corporations (rechtspersoon). Even though currently there are actually many regulations that regulate the protection of personal data for consumers in addition to Law Number 27 of 2022 concerning Personal Data Protection. Other provisions are in OJK Regulation Number 06/POJK.07/2022 concerning Consumer and Public Protection in the Financial Services Sector, Minister of Communication and Information Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, and Law no. 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions.

OJK Regulation Number 06/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector, specifically in Article 11 there is a prohibition for financial service businesses (PUJK) to provide personal data and/or information regarding consumers to other parties; PUJKs are also required to require approval from consumers of financial services to share personal data and/or information as a condition for using financial products and services; then PUJKs are prohibited from using consumer personal data and or information that has terminated product and/or service

agreements; PUJKs are prohibited from using the personal data and/or information of potential consumers whose applications for use of products and/or services are rejected and PUJKs are also prohibited from using personal data and/or information of potential consumers who withdraw applications for use of products and/or services.

Minister of Communication and Informatics Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems in Article 36 paragraph (1) regulates administrative sanctions related to violations of personal data in the form of: verbal warnings, written warnings, temporary suspensions, activities, and/or announcements on the website in network (online website). Meanwhile, Bank Indonesia Regulation Number 19/12/PBI/2017 concerning the Implementation of Financial Technology in Article 20 paragraph (2) regulates the sanctions given if the financial technology operator violates personal data, namely in the form of: 1) Written warning; and/or 2) Removal from the list of financial technology operators at Bank of Indonesia. [8]

Protection of personal data regulated in Law no. 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions listed in Article 26 paragraph (1) and (2) which states that: (1) "Unless otherwise specified by laws and regulations, the use of any information through electronic media that concerns a person's personal data must be done with the approval of the person concerned. (2) "Every person whose rights are violated as referred to in paragraph (1) can file a lawsuit for losses incurred under this law". The consequence of this article is that if someone uses other people's information through electronic media without first asking for or obtaining approval from the owner concerned, then that person can be sued for the losses he has done, unless there are other provisions in the laws and regulations. Minister of Communication and Informatics Regulation No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems, specifically article 26 regulates the rights of owners of personal data, namely "the right to confidentiality of his data, the right to submit complaints in the context of resolving personal data disputes, the right to get access to obtain his personal data history ; and has the right to request the destruction of certain personal data belonging to him in the electronic system". the right to file a complaint in the context of resolving personal data disputes, the right to get access to obtain a history of personal data; and has the right to request the destruction of certain personal data belonging to him in the electronic system". [10]

In the Law Number 27 of 2022 concerning Protection of Personal Data contains the strictest sanctions including administrative, civil and criminal sanctions related to the protection of personal data. In Article 57 paragraph (2) administrative sanctions are stated in the form of: 1) Written warning; 2) Temporary suspension of personal data processing activities; 3) Deletion or destruction of personal data and/or 4) administrative fines, a maximum of 2 (two) percent of annual income or annual revenue of variable violations. [11]

2) Law Enforcement Against Misuse of Consumer Personal Data in the Financial Services Sector

The thing that needs to be of common concern is related to the number of regulations that have been explained, whether their application in cases that are rife is effective against financial service companies that misuse consumers' personal data. The Investment Alert Task Force (SWI) has stopped 3,631 illegal P2PL activities or illegal online loans (pinjol) since 2018. In detail, there were 708 illegal loan platforms that were stopped from operating from January to October 2021. Meanwhile the number of illegal loan platforms that were stopped in 2018 was 404 platforms. The figure then jumped 269.5% to 1,493 platforms in 2019. [12]

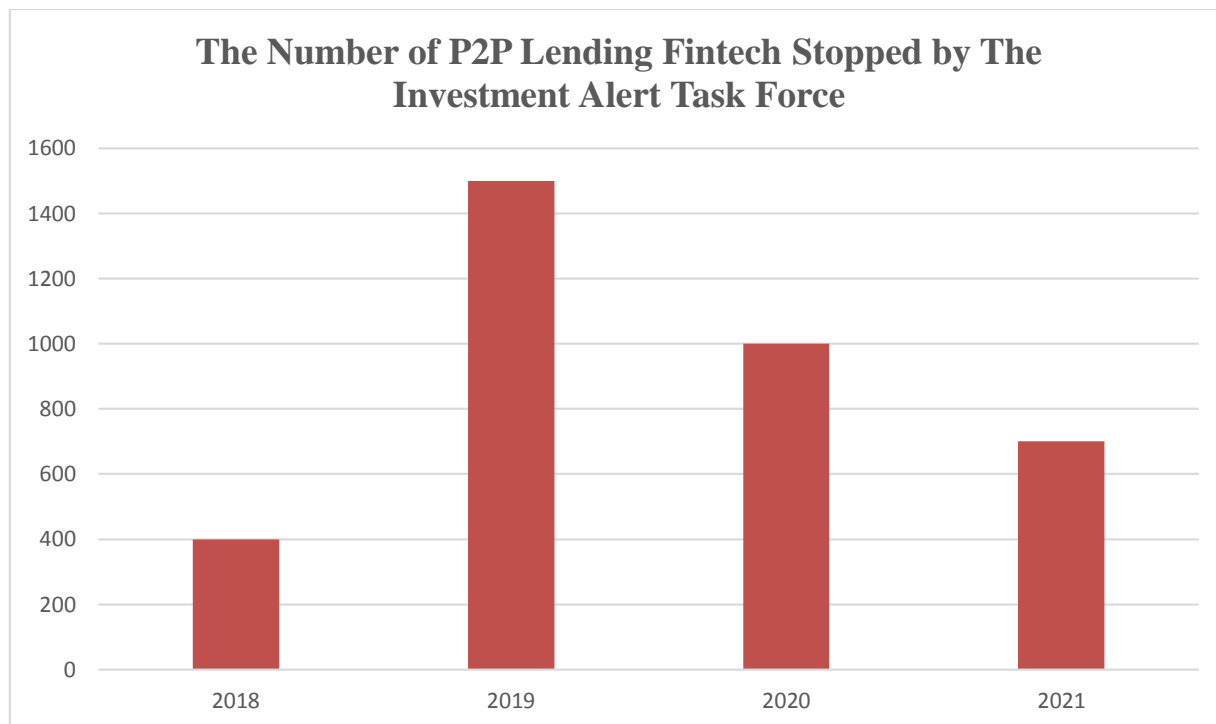


Figure 1. The Number of P2P Lending Fintech Stopped by The Investment Alert Task Force

One example of a financial services company in the P2PL field that misuses the personal data of its consumers is what PT. Vega Data together with its shadow company PT. Barracuda Fintech. This crime mode stems from the way the company works by sending messages to random cellphone numbers. The content is in the form of a message offering to borrow money quickly and without collateral. PT Vega Data Indonesia was also revealed to have changed the name of the online loan application several times to avoid and trick the OJK, as well as law enforcement agencies.

Then, in the loan application process, PT Vega Data includes a standard clause that requires prospective customers to give approval to PT Vega Data Indonesia to access all telephone contacts and information in the form of photos on the prospective customer's mobile device. This triggers the crime of debt collection with threats of violence and disseminating customer data to other parties which can end up defaming the customer's reputation.

Based on Decision Number 526/Pid.Sus/2020/PN Jkt. Utr September 22, 2020, the Panel of Judges sentenced PT Vega Data Indonesia and its shadow company, namely PT Barracuda Fintech Indonesia, using the approach of Law No. 8 of 1999 concerning Consumer Protection, namely by applying the criminal offense provisions stipulated in Article 62 paragraph (1) jo. Article 8 paragraph (1) letter f Law No. 8 of 1999 concerning Consumer Protection. However, the application of the legal basis for criminal acts regulated in Law no. 8 of 1999 concerning Consumer Protection has not been effective in providing a deterrent effect for these corporations. Individual defendants were brought to trial with charges arranged in alternative charges, therefore the Panel of Judges went straight to proving the indictment of Article 62 paragraph (1) jo. Article 8 paragraph (1) letter f of Law no. 8 of 1999 concerning Consumer Protection jo. Article 55 paragraph (1) 1st of the Criminal Code.

The problem in the case between PT Vega Data Indonesia and its shadow company, PT Barracuda Fintech Indonesia, at the time the decision was made, was that the Panel of Judges imposed criminal responsibility only on controlling personnel. In this case, the corporation should also be held criminally

responsible. This refers to the elements of corporate criminal responsibility in several laws and regulations, and is based on the doctrine or teachings of corporate criminal responsibility. [13]

As a corporation in the form of a Limited Liability Company, PT Vega Data must also comply with the provisions stipulated in Law no. 40 of 2007 concerning Limited Liability Companies, specifically regarding the responsibilities of the directors as stipulated in Article 92 paragraph (1) and (2) explains that the directors in carrying out the management of the company must be in accordance with the aims and objectives of the company, then the directors are given the authority to adopt policies that are deemed appropriate of course within the limits determined by law and the articles of association of the company in good faith and full responsibility.

Reflecting on the elements of corporate criminal liability in various statutory provisions, it would be better if the Panel of Judges in the case of PT Vega Data Indonesia and its shadow company PT Barracuda Fintech Indonesia could uphold the law through a systematic interpretation of the law. According to Sudikno Mertokusumo, systematic legal interpretation is interpreting laws and regulations through the method of connecting them with other laws or with the entire legal system. Judges see the law as a whole by connecting it with other laws. Through a systematic interpretation of the law, the Panel of Judges can impose corporate criminal responsibility on PT Vega Data Indonesia and its shadow company, PT Barracuda Fintech Indonesia, by connecting elements of criminal responsibility that exist in several statutory provisions. By looking at the handling of crimes against the protection of consumer personal data carried out by PT Vega Data and PT Bharracuda Fintech, it can be seen that there is a gap in the application of sanctions or punishments against the corporation itself. Precisely with the presence of newer regulations such as Law Number 27 of 2022 concerning Personal Data Protection which contains concrete and written provisions on criminal sanctions for corporations, law enforcement by the apparatus should also be able to compensate.

4. Conclusion

Developments in financial technology have made transaction and authorization activities for companies in the financial services sector in Indonesia fast-paced and practical. The digitalization of financial services has led to a decentralization of the financial system with its sophistication that can only be accessed using the internet. There are three financial services sectors that are experiencing rapid digitization developments, namely the digital banking sector, the financing industry or P2PL, and the digital insurance sector. Despite all the conveniences, digital financial services are very vulnerable to the security of consumer data. Given the increasingly real threat of misuse of personal data, Indonesia has several personal data protection provisions for consumers in the financial services sector, such as OJK Regulation Number 06/POJK.07/2022 concerning Consumer and Public Protection in the Financial Services Sector, Minister of Communication and Information Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, and Law no. 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, and Law Number 27 of 2022 concerning Protection of Personal Data. In order to achieve legal certainty, these updated laws and regulations should be accompanied by more optimal law enforcement efforts, especially against corporations as perpetrators of personal data abuse.

Acknowledgement

The author expresses his deepest gratitude to the Chancellor of the Universitas Komputer Indonesia and the ICOBEST committee who have helped publish the author's articles in ICOBEST activities.

References

- [1] A. E. Sinaga, "Consumer Protection for Personal Data Leakage to Akulaku Application Users Based on Financial Services Authority Regulation Number 1/POJK.07/2013 Concerning Consumer Protection in the Financial Services Sector," *Adigama Law Journal*, vol. 4, no. 2, pp. 4128–4150, 2021.
- [2] I. Rahadiyan, "The Development of Financial Technology in Indonesia and the Regulatory Challenges Faced," *Mimb. Huk.*, vol. 34, no. 1, pp. 210–236, 2022, doi: 10.22146/mh.v34i1.3451.
- [3] S. Batunanggar, "Fintech Development and Asian Development Bank Institute," *ADBI Work. Pap. Ser. FINTECH*, vol. 1014, no. 1014, pp. 1–12, 2019, [Online]. Available: www.adbi.org
- [4] U. Sabadina, "Politics of Criminal Law Information Technology Crime Prevention Related to Leakage of Personal Data by Online-Based Corporations," *J. Lex Renaissance.*, vol. 6, no. 4, pp. 799–814, 2021, doi: 10.20885/jlr.vol6.iss4.art11.
- [5] A. Rinaldi and E. Fahamsyah, "Consumer Protection in the Financial Services Sector for Misuse of Personal Data in Online Credit Applications," *Adigama Law Journal*, vol. 3, no. 1, pp. 964–987, 2020.
- [6] F. P. Carolin and R. Apriani, "Analysis of Personal Data Protection Regulations for Fintech Lending Users in OJK Regulation Number 06/Pojk.07:2022," *J. Ilm. Wahana Pendidik.*, vol. 8, no. 8, pp. 88–96, 2022, doi: 10.5281/zenodo.6613275.
- [7] R. Ariana, "Legal Protection for Users of Online Loan Services Against Debt Collector Threats and Sales of Consumer Data," *Pro Law Journal.*, vol. 11, no. 3, pp. 1–23, 2016.
- [8] S. Suyatno, "An Analysis of Fintech User Personal Data Protection Based on a Normative Juridical Approach in Indonesia," *YUME J. Manag.*, vol. 5, no. 3, pp. 481–491, 2022, doi: 10.37531/yume.vvix.325.
- [9] H. Agusta, "Protection of Personal Data of Borrowers in Information Technology-Based Borrowing and Borrowing Transactions (Peer to Peer Lending)," *Krtha Bhayangkara*, vol. 14, no. 2, pp. 163–192, 2020, doi: 10.31599/krtha.v14i2.189.
- [10] Indonesia, "Law Number 19 of 2016 Concerning Information and Electronic Transactions," 2016.
- [11] Indonesia, "Personal Data Protection Act," no. 016999, pp. 1–50, 2022.
- [12] C. Annur, "The Investment Alert Task Force Closes 3,631 Illegal Online Loans until October 2021," *katadata.co.id*, 2021. <https://databoks.katadata.co.id/datapublish/2021/12/20/satgas-waspada-investasi-tutup-3631-pinjaman-online-ilegal-hingga-oktober-2021#:~:text=Secara rinci%2C%20ada%20708%20platform,menjadi%201.493%20platform%20pada%202019.>
- [13] Suseno AW dan Yeti Sumiyati, "Corporate Responsibility of Illegal Fintech Lending in the Perspective of Consumer Protection," *Law Rev.*, vol. XXI, no. 1, pp. 117–144, 2021.
- [14] I. M. M. Subawa, "Protecting personal data in financial technology in indonesia," *Int. J. Business, Econ. Law*, vol. 22, no. 1, pp. 59–68, 2020, [Online]. Available: http://ijbel.com/wp-content/uploads/2020/09/IJBEL22_210_Mulyawan.pdf
- [15] I. Dewi Sartika Saimima and V. Gola Patria, "The Fintech Phenomenon: Protection of Consumer Privacy Data in Online Lending," *J. Kaji. Ilm.*, vol. 21, no. 2, pp. 185–194, 2021, doi: 10.31599/jki.v21i2.564.
- [16] H. Wijaya and H. Herwastoeti, "Criminal & Civil Liability Related to Misuse of Illegal Fintech Customer Data During The Covid-19 Pandemic," *Audit. Comp. Law J.*, vol. 3, no. 1, pp. 1–9, 2022, doi: 10.22219/aclj.v3i1.19873.