E-ISSN: 2622-7045 I P-ISSN: 2654-3605
UNES LAW REVIEW
https://review-unes.com uneslawreview@gmail.com +62 856-5804-3983
DOI: https://doi.org/10.31933/unesrev.v6i4
Received: 25 June 2024, **Revised:** 13 July 2024, **Publish:** 17 Juliy 2024

Legal Protection for Consumers for Personal Data in the Use of Financial Technology

Alexander Salim[1], Hono Sejati[2], Tri Susilowati[3]
[1] Universitas Darul Ulum Islamic Centre Sudirman GUPPI, Indonesia
Email: aleksander_ki@yahoo.com
[2] Universitas Darul Ulum Islamic Centre Sudirman GUPPI, Indonesia
Email: sejatihono@gmail.com
[3] Universitas Darul Ulum Islamic Centre Sudirman GUPPI, Indonesia
Email: tri.susilowati.undaris@gmail.com

Corresponding Author: aleksander_ki@yahoo.com

Abstract: Financial technology is a term that refers to the use of technology to improve and simplify financial services. Fintech includes a variety of applications, services, and products that use technology to provide more efficient, faster, and more accessible financial services for consumers and businesses. Although the Fintech business offers many benefits, its enactment also carries potential risks. The two major risks faced are consumer data security and transaction errors. The risk of data privacy security is that Fintech often relies on digital data, so cyber security and data privacy risks are a big concern, cases of hacking, identity theft, and data leaks can have a significant impact on consumers, while what is meant by the risk of transaction errors is that the majority of Fintech transactions are digitally conducted, technical errors or system failures can result in transaction errors, which can be detrimental to consumers or companies. These two risks can cause losses for all parties involved in the Fintech business. The emergence of online crimes, such as data interception, hacking, and cybercrime in financial transactions, has made people skeptical of online transactions. Legal protection for consumers' personal data is essential because personal data includes sensitive information to identify, track, or exploit individuals. Forms of legal protection related to fintech personal data are regulated in Minister of Communication and Information Regulation Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, Financial Services Authority Regulation Number 13/POJK.02/2018 concerning Digital Financial Innovation, and Financial Services Authority Regulation Number 1/POJK. 07/2013 concerning Consumer Protection in the Financial Services Sector

Keyword: Financial Technology; Consumer protection; Personal data.

INTRODUCTION

Trapped in an era where digital technology evolves rapidly, technological Modern life today cannot be separated, especially since it is very dependent on the latest/advanced

technological advances "hitech" or "advanced technology" in the fields of data and electronics via international networks (the internet). The development of information technology, especially interconnection-networking (internet), has had a major influence on all aspects of human life. Modern life today is very dependent on technological advances.[1]

The Indonesian Internet Service Providers Association (APJII) stated that in 2023, there would be 221.5 million Internet users in Indonesia. This high number of internet service users has led to a rapid growth of Fintech companies in the country. Alvin Taulu, who is the Head of the Fintech Licensing Sub-Section at the Financial Services Authority (OJK), stated that by 2023, the total transactions from the peer-to-peer (P2P) lending industry would be IDR 55.98 trillion. Other data regarding this can be obtained as well. As of October 2023, there were 101 Fintech companies licensed and registered with the OJK. It is worth noting that as of December 2022, the number of registered Fintech companies was 102.

Fintech companies are experiencing rapid growth because Fintech provides a variety of advantageous financial services. With Fintech, people can carry out economic activities more effectively and efficiently, especially in the financial sector.[2] Financial technology is a term that refers to the use of technology to improve and simplify financial services, Fintech includes a variety of applications, services, and products that use technology to provide more efficient, faster, and accessible financial services for consumers and businesses. The following are some examples of financial technology:

a. Electronic payments

   Fintech enables electronic financial transactions, such as payments via mobile applications, digital wallets, and online money transfers.

b. Digital financial services

   Fintech provides financial services that can be accessed online, such as digital banking, cardless credit, and online investment.

c. P2P lending

   Fintech allows people to borrow and lend money through digital platforms, without the involvement of traditional banking institutions.

d. Crowdfunding

   Fintech supports fundraising through online platforms, allowing individuals and businesses to raise capital from a large number of people.

e. Robo-Advisors

   It is an automated system that provides investment advice and manages portfolios based on algorithms, without direct interaction with human advisors

f. Blockchain Technology and Cryptocurrencies:

   Fintech also includes blockchain technology that enables decentralized transactions and digital currencies such as Bitcoin and Ethereum

g. Insurtech

   Fintech also includes innovations in the insurance industry, such as digital insurance policy offerings and automated claims.

Although the Fintech business offers many benefits, its implementation also carries potential risks. The two main risks faced are the risk of consumer data security and the risk of transaction errors. The risk of data privacy security is that Fintech often relies on digital data, so cyber security and data privacy risks are a big concern, cases of hacking, identity theft, and data leaks can have a significant impact on consumers, while what is meant by the risk of transaction errors is that the majority of Fintech transactions are carried out digitally, technical errors or system failures can result in transaction errors, which can be detrimental to consumers or companies. These two risks can cause losses for all parties involved in the Fintech business. The emergence of online crimes, such as data interception, hacking, and cybercrime in financial transactions, has made people skeptical of online transactions.[3]

The rapid development of technology in today's society can change the mindset of the population globally, both in positive and negative aspects. Technology has a very significant role in improving people's welfare, but at the same time, it can also encourage unlawful actions. Consumer protection refers to actions to protect consumers while they meet their needs. Law Number 8 of 1999 concerning Consumer Protection (UUPK) Article 1 paragraph (1) states that consumer protection is any effort that ensures legal certainty to protect consumers.[4]

Based on the background description of the legal issues that are interesting to discuss, namely what is the form of legal protection for consumers over personal data when using financial technology?

METHOD

Method

The research method used to write this is a normative legal research method, which is legal research carried out by examining library materials and secondary data, where the approach used will be a normative juridical (statute approach) with a descriptive-analytical nature.[5]

Approach

The normative approach is a method used to examine problems in the context of law and statutory regulations, including rules that can be used as a basis for examining problems and their legal consequences. In this case, examples are Law Number 8 of 1999 concerning Consumer Protection and the Minister of Communication and Information Regulation Number 20 of 2016 concerning the protection of personal data in electronic systems. A normative approach is taken in certain statutory regulations or written laws relating to law enforcement associated with personal data in electronic systems. The research describes the situation of the object being studied, with a focus on regulations and the concept of legal protection for consumers of personal data in the use of Fintech.[6]

RESULT AND DISCUSSION

Financial Technology According to Indonesian Law

The fintech industry represents a pioneering advancement in finance intertwined with contemporary technological advancements. It leverages progressions in information technology to foster innovations within the financial services arena, characterized by swiftness and user-friendliness. Fintech enterprises abbreviated as LJK electronically, engage in the provision of financial services through the utilization of information technology, thereby epitomizing a business model rooted in technological integration.[7]

Fintech enterprises, through their utilization of electronic platforms for delivering financial services to consumers, fall within the purview of regulations governing both electronic systems and financial services. Consequently, the oversight of fintech businesses is the responsibility of various governmental bodies, including the Ministry of Communication and Information of the Republic of Indonesia, known as Kemkominfo, which serves as the regulator for electronic systems, along with Bank Indonesia and the Financial Services Authority, responsible for regulating financial services.

The regulatory framework delineating the scope of fintech activities is primarily outlined in Bank Indonesia Regulation Number 19/12/PBI/2017, which addresses the implementation of fintech. Notably, Article 3 paragraph (1) of this regulation categorizes fintech into five distinct types, as follows:

a. Payment system

Payment systems in financial technology (Fintech) include various types of methods and platforms that facilitate financial transactions electronically. Fintech payment systems provide convenience, speed, and flexibility in conducting financial transactions electronically

b. Market support

Fintech is a technology that utilizes information technology and/or electronic technology to facilitate the provision of faster and cheaper information about products and/or Financial Services Institutions to the public.

c. Investment management and risk management

Investment management and risk management are two critical aspects of the financial technology (Fintech) industry. The two are interrelated, as effective investing requires a good understanding of risk, and strong risk management supports safer investment strategies.

d. Financing loans, and capital provision

Lending, financing, and capital provision stand as foundational domains within the financial technology (Fintech) sector, characterized by the application of technology to revolutionize how both enterprises and individuals obtain funds and administer their financial affairs.

e. Other financial services

Apart from the four things mentioned earlier.

Additionally, the realm of financial technology is subject to regulatory oversight under the purview of the Financial Services Authority (OJK). As mandated by the Financial Services Authority Regulation, the OJK is entrusted with the establishment and implementation of a comprehensive regulatory and supervisory framework encompassing all facets of the financial services sector. Consequently, fintech enterprises operate within a system of supervision administered by the Financial Services Authority. This regulatory landscape is delineated in Financial Services Authority Regulation No. 77/POJK.01/2016 specifically addressing technology-based money lending and borrowing services.[7]

The regulation seeks to implement digital financial innovation responsibly so that with this regulation, consumers who use digital finance feel safe because there is a legal umbrella. In Article 2 Paragraphs (1) and (2) concerning the objectives of Digital Financial Innovation, the scope of fintech business in the Financial Services Authority Regulation is divided into various types, namely transaction settlement, capital accumulation, investment management, insurance, market support, financial support, and financial services activities.

In the execution of fintech enterprises through the utilization of tools such as electronic contracts, the realm of financial technology is subject to regulatory frameworks delineated in Law Number 19 of 2016, which amends Law Number 11 of 2008 concerning Electronic Information and Transactions. This legislative framework, notably elucidated in Article 1 paragraph (17) and Article 18, provides comprehensive guidelines concerning electronic contracts within the fintech domain. The electronic contract in question is an agreement between two parties made using an electronic system.

Legal Protection for Consumers for Personal Data in the Use of Financial Technology

Ensuring legal safeguards for consumers of personal data is imperative due to the sensitive nature of such information, which harbors the potential for identification, tracking, or exploitation of individuals. In the absence of robust legal protections, consumers are vulnerable to a spectrum of risks, including identity theft, fraudulent activities, and breaches of privacy. The paramount importance of legal safeguarding of personal data lies in its efficacy in thwarting unauthorized exploitation by external entities. Through the

establishment of clear regulatory frameworks, both corporate entities and individuals benefit from well-defined boundaries outlining the collection, utilization, and sharing of personal data. Furthermore, legal protection mechanisms for personal data serve to uphold consumers' rights to privacy, fostering an environment wherein individuals can divulge personal information devoid of apprehension regarding its inappropriate utilization.

Personal data pertains to data concerning an identifiable individual and is preserved, secured, and handled with accuracy while maintaining confidentiality. Safeguarding personal data within electronic systems encompasses endeavors aimed at shielding such data across its lifecycle, from acquisition to disposal. These endeavors entail measures designed to forestall unauthorized access, utilization, and divulgence of personal data. At the core of implementing personal data protection within electronic systems lies the foundational principle of honoring privacy and the vested interests of pertinent individuals. Minister of Communication and Information Regulation Number 20 of 2016 concerning the protection of Personal Data in Electronic Systems, especially Article 26 states that:

a. Everyone has the right to confidentiality of their data,
b. Submit a complaint in resolving personal data disputes regarding failure to protect the confidentiality of personal data by electronic system operators to the minister.
c. Get access or the opportunity to change or update personal data without disrupting the personal data management system unless otherwise determined by other laws and regulations,
d. Obtain access or the opportunity to obtain historical personal data that has been submitted to the electronic system operator as long as it is still by the provisions of statutory regulations,
e. Request to destroy certain individual data belonging to him in the electronic system managed by the electronic system operator, unless determined by the provisions of statutory regulations.

Apart from that, Article 2 paragraph (1) of the Minister of Communication and Information Regulation Number 20 of 2016 concerning the protection of personal data in Electronic Systems states that the protection of personal data in Electronic Systems includes protection of acquisition, collection, processing, analysis, storage, display, announcement, sending, dissemination. , and destruction of personal data. Furthermore, Article 27 states that users are obliged to maintain the confidentiality of the Personal Data they obtain, collect, process, and analyze. Furthermore, when using personal data it must only be to the user's needs, other user obligations are to protect personal data and documents containing such personal data from from acts of misuse, and the final obligation is responsibility for personal data in their control, whether controlled by an organization under their authority or individually, if an act of misuse occurs.

Furthermore, Article 28 Chapter V of the Minister of Communication and Information Regulation Number 20 of 2016 concerning the protection of personal data in Electronic Systems, explains the obligations of electronic system operators, including:

a. Carry out certification of the Electronic System which it manages by the provisions of statutory regulations.
b. Maintain the truth, validity, confidentiality, accuracy, and relevance as well as suitability to obtain, collect, process, analyze, store, display, announce, send, disseminate, and destroy Personal Data;
c. Notify the Personal Data Owner in writing if there is a failure to protect the confidentiality of Personal Data in the Electronic System he manages, with the following notification provisions:
    1) must be accompanied by the reasons or causes of failure to protect the confidentiality of Personal Data;

2) can be done electronically if the Personal Data Owner has given consent to do so which was stated at the time of obtaining and collecting his Personal Data;
3) it must be ensured that it has been accepted by the Personal Data Owner if the failure contains potential losses for the person concerned; And
4) written notification is sent to the Personal Data Owner no later than 14 (fourteen) days after the failure is discovered

d. has internal rules regarding the protection of Personal Data that are by statutory provisions.
e. provide an audit track record of all Electronic System implementation activities that it manages.
f. provide options to the Personal Data Owner regarding the Personal Data they manage which can/or cannot be used and/or displayed by/to third parties with Consent as long as it is still related to the purpose of obtaining and collecting the Personal Data;
g. provide access or opportunity to Personal Data Owners to change or update their Data without disrupting the Personal Data management system, unless otherwise determined by statutory provisions;
h. destroy Personal Data by the provisions in this Ministerial Regulation or the provisions of other laws and regulations that specifically regulate each Sector Supervisory and Regulatory Agency for that purpose
i. Provide a contact person who can be easily contacted by Personal Data Owners regarding the management of their Data.

Any entity that obtains, collects, processes, analyzes, stores, displays, publishes, transmits, or distributes personal data without permission or violates these regulations and other legal regulations will be subject to administrative sanctions. These sanctions can be in the form of verbal warnings, written warnings, temporary suspension of activities, or announcement of violations on the website, this is stated in Article 36 of the Minister of Communication and Information Regulation Number 20 of 2016 concerning the protection of personal data in Electronic Systems

Apart from the Minister of Communication and Information Regulation Number 20 of 2016 concerning the protection of personal data in Electronic Systems, the protection of consumer personal data is also regulated in the Financial Services Authority Regulation Number 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector, according to the POJK financial technology organizers are required to safeguard 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.

Furthermore, in Article 31 paragraph (1) of the Financial Services Authority Regulation Number 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector, organizers are required to implement the basic principles of consumer protection which include transparency, fair treatment, reliability, confidentiality and security of personal data consumers, and handling complaints and resolving consumer disputes in a simple, fast and affordable manner. Then Article 39 paragraph (1) of the Financial Services Authority Regulation Number 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector also explains the provisions for sanctions for violators, which states that without reducing criminal provisions in the financial services sector, the Services Authority Finance has the authority to impose administrative sanctions on any party who violates the provisions of this Financial Services Authority Regulation, including parties who cause the violation.

The next legal basis is related to the legal protection of consumer personal data, namely Financial Services Authority Regulation Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector. The aim of Financial Services Authority

Regulation Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector is to ensure that consumers in the financial services sector have adequate protection and can make transactions safely and comfortably. This OJK regulation guarantees the rights and interests of consumers, apart from that it also increases transparency, encourages the responsibility of financial service institutions, regulates supervision and sanctions, increases consumer confidence, and prevents business practices that are detrimental to consumers. By regulating various aspects of consumer protection in the financial services sector, POJK 1/2013 helps create a safer and more transparent environment for consumers and encourages financial services institutions to act with responsibility and integrity.

Based on Article 1 number 3 of the Financial Services Authority Regulation Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector, it is stated that consumer protection is the protection of consumers covering the behavior of Financial Services Business Actors. Furthermore, Article 2 explains that consumer protection applies the principles of transparency, fair treatment, reliability, confidentiality, and security of consumer data or information, handling complaints, and resolving consumer disputes in a simple, fast, and affordable manner. Violations of this POJK can result in the application of administrative sanctions as described in Article 53. The array of administrative sanctions that may be enforced comprises written admonitions, pecuniary penalties, constraints on business operations, temporary cessation of business activities, and the annulment of operational licenses.

One of the fundamental features and goals of legislation is to safeguard the community. Law serves as the primary mechanism for guiding diverse societal transformations, thereby facilitating the advancement of the nation and state toward a more favorable trajectory.[8]Law plays a pivotal role in overseeing the utilization and advantages of scientific and technological advancements to enhance human well-being and longevity. Within the Fintech sphere, a key objective of legislation is consumer protection. Legal safeguards aspire to uphold human rights potentially infringed upon by the actions of others, thereby extending this protection to the community to ensure their enjoyment of rights guaranteed by law.[9]

The Financial Services Authority, tasked with overseeing the financial services sector, is anticipated to effectively shield consumers from potential harm posed by Financial Services Business Actors (PUJK), particularly within the realm of Fintech. Endowed with regulatory authority over financial services operations, the OJK is obligated to provide consumer protection for those engaging in financial services, encompassing both fund depositors and users of services rendered by financial institutions.

CONCLUSION

Financial technology is a term that refers to the use of technology to improve and simplify financial services. Fintech includes a variety of applications, services, and products that use technology to provide more efficient, faster, and more accessible financial services for consumers and businesses. Although the Fintech business offers many benefits, its implementation also carries potential risks. The two main risks faced are the risk of consumer data security and the risk of transaction errors. The risk of data privacy security is that Fintech often relies on digital data, so cyber security and data privacy risks are a big concern, cases of hacking, identity theft, and data leaks can have a significant impact on consumers, while what is meant by the risk of transaction errors is that the majority of Fintech transactions are carried out digitally, technical errors or system failures can result in transaction errors, which can be detrimental to consumers or companies. These two risks can cause losses for all parties involved in the Fintech business. The emergence of online crimes,

such as data interception, hacking, and cybercrime in financial transactions, has made people skeptical of online transactions.

Legal protection for consumers of personal data is essential because personal data includes sensitive information that can be used to identify, track, or exploit individuals. Forms of legal protection related to fintech personal data are regulated in Minister of Communication and Information Regulation Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, Financial Services Authority Regulation Number 13/POJK.02/2018 concerning Digital Financial Innovation, and Financial Services Authority Regulation Number 1/POJK. 07/2013 concerning Consumer Protection in the Financial Services Sector. The Financial Services Authority, as the institution responsible for supervising the financial services sector, is expected to be able to protect consumers from Financial Services Business Actors (PUJK) who have the potential to harm consumers' interests, especially in the Fintech context. As an institution that has the authority to supervise business activities in the financial services sector, the OJK must be able to protect consumers who use financial services, both those who place funds and those who use the services provided by financial services institutions.

.

REFERENCES

B. Nawawi Arief, "KEBIJAKAN PENANGGULANGAN CYBER CRIME DAN CYBER SEX," *LAW REFORM*, vol. 1, no. 1, p. 11, Jan. 2006, doi: 10.14710/lr.v1i1.12177.

F. Margaretha, "DAMPAK ELECTRONIC BANKING TERHADAP KINERJA PERBANKAN INDONESIA," *Jurnal Keuangan dan Perbankan*, vol. 19, no. 3, Dec. 2015, doi: 10.26905/jkdp.v19i3.49.

I. A. W. Chrismastianto, "Analisis SWOT Implementasi Tekonologi Finansial terhadap Kualitas Layanan Perbankan di Indonesia," *Jurnal Ekonomi dan Bisnis*, vol. 20, no. 1, p. 137, Apr. 2017, doi: 10.24914/jeb.v20i1.641.

L. Abubakar and T. Handayani, "Financial Technology: Legal Challenges for Indonesia Financial Sector," *IOP Conf Ser Earth Environ Sci*, vol. 175, p. 012204, Jul. 2018, doi: 10.1088/1755-1315/175/1/012204.

P. Soerjowinoto, *Buku Pedoman Metode Penelitian Karya Hukum dan Skripsi*. Semarang: Fakultas Hukum Unika Soegijapranata, 2006.

R. H. Sumitro, *Metodologi Penelitian Hukum dan Jurimetri*, 4th Print. Jakarta: Ghalia Indonesia, 1990.

Sulistyandari, "Fintech Indonesia User Legal Protection in Balance Borrowing Money Based on Information Technology," *SHS Web of Conferences*, vol. 54, p. 06003, Nov. 2018, doi: 10.1051/shsconf/20185406003.

E. Warassih, "Peran Politik Hukum Dalam Pembangunan Nasional," *Gema Keadilan*, vol. 5, no. 1, pp. 1–15, Oct. 2018, doi: 10.14710/gk.2018.3592.

S. Rahardjo, *Ilmu Hukum*, Cet. V. Bandung: Citra Aditya Bakti, 2000.