Available online at: http://jurnal.president.university.ac.id

PROBLEMATIKA HUKUM

| ISSN (Print) 2477-1198 | ISSN (Online) 2503-4812 |

HARMONIZATION OF FINANCIAL SECTOR REGULATIONS WITH THE FDIC LAW AND THE P2SK LAW REGARDING THE USE OF PRIVACY RELIABILITY CERTIFICATES BY FINANCIAL SECTOR BUSINESSES

Agnes Monica Siagian[1], Muhamad Amirulloh[2]

[1] *Faculty of Law, Universitas Padjadjaran, Unpad*, *E-mail: agnes20003@mail.unpad.ac.id*

[2].*Faculty of Law, Universitas Padjadjaran, Unpad*, *E-mail: muhamad.amirulloh@unpad.ac.id*

Article

Keywords:

Keywords: Privacy Reliability Certificate, Financial Technology Industry, Consumer Protection.

Article History

Received: Apr,21,2024;
Reviewed: Apr,25,2024;
Accepted: May,29,2024;
Published: Jun,10,2024

Abstract

Information and communication technology has changed the behavior of society and human civilization worldwide. Its development has made the world borderless, and significant social changes are taking place rapidly. In addition to contributing to the improvement of welfare, progress and human civilization, it has also become an effective means for illegal acts. Illegal acts occur in the development of the financial technology industry. In order to prevent unlawful acts, it is necessary to use privacy reliability certificates by financial sector companies based on Bank Indonesia Regulation No. 3 of 2023 and OJK Regulation No. 6 of 2022.The research method used is normative juridical. The research is conducted using primary data in the form of field studies as well as the use of library materials or secondary data that includes primary, secondary and tertiary legal materials. This research aims to find out how the implementation of the obligation to use the Privacy Reliability Certificate by financial sector companies based on the Indonesian Cyber Law, in order to better ensure consumer protection.

1. INTRODUCTION

The development of science and technology including telecommunications, media and informatics globally has had an impact on changing the mindset and perspective of the community in carrying out various activities that are oriented towards aspects of ease and speed in exchanging access to information.[1]

The widespread use of Information and Communication Technology (ICT) globally is characterized by digitalization euphoria that impacts individuals, businesses/private sectors, governments, and influences almost all sectors. The use of digitalization has become a driver of economic and social growth with the context of an information-oriented world society.[2]

In its development, the development of the internet economy in Indonesia is the massive number of internet users in Indonesia. The digital economy in Indonesia has a positive impact, but this has also become a new challenge for the government in producing policies. Emerging from the development of the digital economy, it also gave birth to new business models, there is integration between business sectors, as well as changes in business models in pre-existing sectors.

In the financial sector, which is one of the industrial sectors that is quite developed along with the development of Information and Communication Technology (ICT). The banking industry is one of the industries that uses ICT as a forum and means of service to its customers.

As a result of the development of information technology and fintech, it has made it easier for consumers and businesses to transact. Initially, transactions were carried out physically, which then developed to be carried out online, access to goods and services that were previously difficult to reach by consumers can now be easily accessed. Electronic transactions (*E-Commerce*) also provide fast access and services for consumers when purchasing goods. For business actors, the presence of electronic transactions also provides convenience considering that they can easily promote and offer potential customers about the goods or services they have.

With the development of the fintech industry in Indonesia, it cannot be separated from the existence of government supervisory institutions. These institutions are Bank Indonesia and the Financial Services Authority (OJK), which are two government institutions that have the authority to monitor the development of the fintech industry. These two supervisory institutions carry out different tasks and functions. Bank Indonesia focuses on regulating and supervising fintech players in the field of *payment* financial services, while the Financial Services Authority

[1] Sugeng, *Indonesian Telematics Law*, 1st printing, Jakarta: Prenadamedia Group, 2020, p.1
[2] *Ibid*, p.2

(POJK) No. 6 of 2022 concerning Consumer and Community Protection in the Financial Services Sector. OJK focuses on fintech players in the field of funding financial services (*lending*). Each institution has regulations that must be known and obeyed by fintech players to maintain a balance of sustainability. Bank Indonesia has Bank Indonesia Regulation (PBI) No. 3 Year 2023 on Bank Indonesia Consumer Protection. Meanwhile, OJK has regulations governing fintech, namely Financial Services Authority Regulation (POJK) No. 6 of 2022 concerning Consumer and Community Protection in the Financial Services Sector.

Electronic transactions run in the field or means of information and communication technology, called the internet. With the speed and sophistication of modern communication facilities today, the internet is very vulnerable to information security attacks. Without an information security system, electronic transactions become very easy to experience information security disturbances which can cause a sense of distrust for electronic transaction actors, especially the financial sector. The inconvenience of conducting electronic transactions has led to the development of issues regarding trust in electronic transactions both within the national, regional and global scope. There are four criteria for information security in electronic transactions, namely *confidentiality*, *authenticity*, *integrity* and *non-repudiation*.[3]

To organize *trusted e-transactions*, the regulation stipulates that business actors offering products through Electronic Systems must provide complete and correct information relating to contract terms, producers, and products offered (Article 9 of the ITE Law). In addition, the regulation also stipulates that business actors who organize electronic systems can be certified by the Reliability Certification Institute (Article 10 of the ITE Law). Article 41 of PP PSTE also explains that the Implementation of Electronic Transactions in the public or private sphere that use Electronic Systems for the benefit of public services must use Reliability Certificates and / or Electronic Certificates.

These electronic transactions must be safe and reliable. Thus, every electronic transaction that uses an electronic system must have a certificate of reliability and electronic certificate. This is the mandate of Articles 41 and 42 of Government Regulation (PP) No.82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP PSTE). Information security standards emphasize aspects of requirements, procedures, policies, management and education and training. The standardization referred to here is not like a technical standard (specification), the direction of a technology or product, and does not guarantee the functioning of an information security tool.

[3] Ahmad Budi Setiawan, *"Study of Electronic Certificate Standardization and Reliability in the Implementation of Electronic Transaction Systems,"* Post and Telecommunication Bulletin, Vol. 12 no. 2, June 2014, p. 120. 120.

In many sectors, such as the banking industry where there has been competition in terms of the services that businesses provide. Information technology (IT) is widely used in a competitive environment in order to provide banking services to customers. In fact, the emergence of information systems technology in particular has changed the retail banking consumption process as community interaction in service delivery has become increasingly developed. Therefore, the community or face-to-face interaction between customers and bank employees is replaced by customer interaction through technology. Even a large amount of IT is used to improve the efficiency and effectiveness of banking services. With the changing patterns of consumer behavior with the increasing use of technology in banking services, it is necessary to foster customer confidence in using technology-based services, namely internet banking.[4]

Quoting from data from the Ministry of Communication and Information, in the last three years, there have been 29 institutions whose data was breached. In May 2021, the data of 279 BPJS Health participants was leaked and sold on Raid Forums for 0.15 Bitcoin or around IDR 87.1 million.[5] It can be said that the issue of consumer protection and personal data protection in electronic transaction activities is still an important issue to be studied further. Furthermore, regarding consumer rights and obligations of business actors, there is an issue of personal data that still lacks protection and the issue of fraud and data leakage of both consumers and business actors who transact, especially in the financial sector.

Electronic transaction activities require consumers to enter a number of their personal data into the electronic system before they can carry out transaction activities, this personal data request can usually be used by businesses as data on consumer behavior and marketing interests of the products of business actors. However, it is not uncommon for the personal data owned by consumers to be misused by businesses when consumers enter their personal data for the first time on online buying and selling sites or in writing bank customers themselves. The sale of personal data that causes the leakage of customer data, to other companies or product offerings that violate consumer rights can occur from the lack of protection or security guarantees for personal data from consumers provided to business actors. Consumers who conduct online transactions are also faced with several examples of the risk of their rights being violated in the form of consumer fraud. Article 4 of Law of the Republic of Indonesia Number

[4] A. Yaqin and A.M. Ilfitriah, *"The Effect of Service Quality on Satisfaction and Loyalty of E-Banking Bank Customers in Surabaya,"* Journal of Business and Banking, Vol. 4 No.2, 2014, pp. 245-260.

[5] Ministry of Communication and Information, Kominfo's Fast Movement to Protect Personal Data, https://www.kominfo.go.id/content/detail/34813/gerak-cepat-kominfo-melindungi-data-pribadi/ 0/article, accessed on April 16, 2024, at 12.01 WIB.

8 of 1999 concerning Consumer Protection regulates basic consumer rights such as the right to choose, the right to comfort and safety and the right to be heard.[6] However, in practice, in electronic transactions, consumer losses of products that do not match the advertisements, product defects or even products that are not delivered still often occur.

Consumers who will carry out electronic transaction activities have the principle of *trust* that must be upheld by each business actor and consumer. The principle of trust will then lead to the desire of consumers to carry out electronic transaction activities on a particular site, starting from entering personal data to sending money for payment for the product. This gives consumers confidence and guarantees the security of the transaction so that a certificate of reliability of the sector owned by the business actor is needed. With various cases related to personal data, it certainly violates the privacy rights of Data Subjects which allow individuals to limit other people's access to themselves and their information. With the passing of the PDP Law, it is more accommodating regarding the use of personal data in the financial sector in more detail so that Financial Sector Business Actors who process personal data are no longer careless by discrediting the security systems they have to be adequate and equivalent to the PDP Law and Consumers can feel more secure about their personal data that will be processed.

The existence of this reliability certificate will ideally provide a sense of trust from potential consumers and consumers, because the inclusion of eligibility by business actors (Banks) issued by the Reliability Certification Institute will help implement security guarantees for consumers and the reliability of the Bank.

This article will examine how the implementation of the obligation to use privacy reliability certificates in financial sector regulations by BI and OJK and its impact on practices by payment fintech businesses.

2. RESEARCH METHODOLOGY

The research method used is normative juridical. The research was conducted using primary data in the form of field studies as well as the use of library materials or secondary data which includes primary, secondary and tertiary legal materials.[7] Normative legal research includes research on legal principles, legal systematics, the level of legal synchronization, legal history and legal comparisons.[8] Research on how the use of privacy reliability certificates by financial sector business actors will analyze and review secondary data by direct observation through electronic systems managed by Financial Sector Business

[6] Law Number 8 Year 1999 on Consumer Protection.
[7] Soerjono Soekanto, *Introduction to Legal Research,* 3rd Edition, Jakarta: UI Press, 2019, p. 52.
[8] *Ibid,* p.51.

Actors (Website and or Application).

The research stages carried out as follows, literature study in the form of, Primary Legal materials, namely applicable laws and regulations, Secondary Legal materials, are legal materials that provide explanations regarding information or as support for primary legal materials which can be in the form of books, journals, or magazines written by legal scholars, theories, and expert opinions, as well as internet sites related to these problems and the like, and Tertiary Legal materials, are legal materials that provide guidance from primary legal materials and secondary legal materials, general dictionaries, legal dictionaries, large dictionaries.

The data collection technique by collecting written data includes books, official documents, reports, especially those on consumer protection for personal data leaks and through primary data collection in the form of literature study, where literature study is a type of secondary data with data obtained not directly from the first source, but from data recorded in the form of legal materials.[9]

Thus, the analysis design made by the author will use qualitative juridical data analysis techniques, which assess the results of data processing that are not in the form of numbers and emphasize legal analysis on the deductive inference process, in the form of drawing conclusions from general to specific and inductive inference using formal and argumentative ways of thinking.[10]

3. ANALYSIS AND DISCUSSION

3.1 Financial Payment Technology as a Financial Sector Business Actor

The definition of Fintek is contained in Bank Indonesia Regulation Number 19/12/PBI/2017 on the Implementation of Financial Technology, as 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 the efficiency of the smoothness, security, and reliability of the payment system.

Fintech is categorized into two categories: Conventional and Sharia Fintech. In Indonesia, Fintek is categorized as *Payment* System (*Payment, Settlement, and Clearing*); Market *Aggregator (Market* Support); Investment Management and Risk Management (*Personal/Financial Planning)*; Lending, Financing, and Capital Provision (*Crowdfunding and P2P Lending);* and Other Financial Services (*Others*).

[9] Soerjono Soekanto and Sri Mamudji, Normative Legal Research A Brief Overview, Rajawali Press, Jakarta, 1990, pp. 14-15. 14-15.

[10] M. Syamsuddin, Operationalization of Legal Research, Grafindo Persada, Jakarta, 2007, p. 133. 133.

According to Roy S. Freedman, Fintech is concerned with building systems that model, value, and process financial products such as bonds, stocks, contracts, and money. At the very least, financial products are represented by price, time, and credit. Like commercial systems, financial systems incorporate trading systems and trading technology to enable the buying and selling of products at different times and in different market spaces. This includes arbitrage, which is the simultaneous buying and selling of the same product in different markets, but at the same time.[11]

Startup fintech companies and/or established companies, basically focus their efforts on innovating new business models to face the challenges that exist in the financial industry.[12] Fintech is also defined as the application of digital technology in terms of financial problems in society.[13] As a digital technology innovation in financial services, fintech produces a product related to the provision of financial services. [14]

Fintek relies on secure communication protocol standards to initiate and synchronize communication, to authenticate users, and to ensure that users can communicate smoothly. In the process, it enables the rapid exchange of information, news, and transmissions across both public and private communication networks. In its operation, fintech integrates mathematics, statistics, economic models, and analytical systems; which will be integrated with messages, transactions, order processing, and payment systems. All activities that occur in fintech must be carried out according to existing rules, procedures, and guidelines.

In Law Number 4 of 2023 Article 1 point 40 concerning Financial Sector Development and Strengthening (P2SK Law), "40. Financial Sector Business Actors, hereinafter abbreviated as FSIs, financial market infrastructure business actors, business actors in the payment system, supporting institutions in the financial sector, and other financial sector business actors both carrying out business activities conventionally and based on Sharia Principles in accordance with the provisions of laws and regulations in the financial sector."

Then according to the Financial Services Authority Regulation Number 6 of 2022 Article 1 point 2 concerning Consumer and Community Protection in the Financial Services Sector, the definition of financial sector business actors is, " 2. Financial Services Business Actors, hereinafter abbreviated as PUJK, are Financial Services Institutions and / or parties that carry out business activities of raising funds, channeling funds, and / or managing funds in the

[11] Roy S. Freedman, Introduction to Financial Technology, California: Elsevier, 2006, pp. 1.
[12] Ryan Randy Suryono, "Financial Technology (Fintech) in Axiological Perspective", *Journal of Telematics and Information Society*, Vol. 10 No.1, 2019, pp. 55.
[13] Meyer Aaron, et. al., "Fintech: Is This Time Different? A Framework for Assessing Risks and Opportunities for Central Banks", Bank of Canada Staff Discussion Paper, 2017, pp. 2.
[14] Jay D. Wilson Jr, Creating Strategic Value Through Financial Technology, Canada: Wiley Finance, 2017.

financial services sector." According to Bank Indonesia Regulation Number 3 of 2023 Article 1 point 5 concerning Bank Indonesia Consumer Protection, "5. Payment Service Providers are banks or institutions other than banks that provide services to facilitate payment transactions to service users.

Regarding the obligation of the Custodian Center, it is clearly stated in the P2SK Law Article 239 paragraph (2), "(2) The obligation of the Custodian Center as referred to in paragraph (1) shall be implemented by applying the basic principles of processing personal data protection as stipulated in the provisions of laws and regulations regarding personal data protection." In this article, it is clearly stated that it is the obligation of the Custodian to process customers' personal data by referring to the PDP Law. However, in PBI 3/2023, Article 32 and Article 36 regarding the obligations of PUSK do not mention the obligation to use a Privacy Reliability certificate. POJK 6/2022 states in Article 11 paragraph 5, "(5) In the event that a PUJK uses information technology to manage data and/or personal information of Consumers, PUJK must use reliable information technology and ensure the security of data and/or personal information of Consumers by conducting periodic feasibility and/or security checks." Compared to the PDP Law, Article 39 paragraphs (1) and (2) of the PDP Law requires the Controller of personal data to implement a security system for personal data. The security system referred to in this case is a Certificate of Reliability. In the POJK, this is already stated in the phrase must use reliable information technology and ensure the security of data and / or consumer personal information, but the method used by the author feels inappropriate and ineffective, namely by checking feasibility and / or security periodically.

3.2 Overview of the Privacy and Personal Data Reliability Certificate

The word "Certification" comes from the Latin "certus" which means "determined, settled, fixed, settled, purposeful". Certification is a procedure by which a third party provides written assurance that a product, process or service conforms to specific characteristics.[15] A certificate is a written or printed mark or certificate (statement) from an authorized person that can be used as evidence of ownership or an event.[16] Reliable itself means: 1. trustworthy; 2. giving the same results on repeated tests or trials.[17] Whereas reliability is the act of being reliable. [18]

[15] Paolo Balboni in his dissertation, Trustmarks-Third-Party Liability Of Trustmark Organizations In Europe", P.10 quoting from Rae, A. et al. (1995) Software Evaluation for Certification. Principles, Practice and Legal Liability (London: McGraw Hill Book Company).
[16] Kamus Besar Bahasa Indonesia, "Certificate", https://kbbi.kemdikbud.go.id/entri/sertifikat, accessed on September 21, 2023.
[17] *Ibid.*, "Reliable", https://kbbi.kemdikbud.go.id/entri/andal, accessed on September 21, 2023.
[18] *Ibid.*, "Reliability", https://kbbi.kemdikbud.go.id/entri/keandalan, accessed on September 21, 2023.

According to article 1 point 27 of the PSTE Regulation, a Reliability Certificate is, "A document stating that a Business Actor conducting an Electronic Transaction has passed an audit or conformity test from a Reliability Certification Body." Meanwhile, in article 67 paragraph (2) of PP PSTE, a Reliability Certificate is, "A guarantee that the business actor has met the criteria determined by the Reliability Certification Body."

Some of the terms Certificate of Reliability found in the literature are *Trustmark*, including privacy certificates of reliability as Privacy Seals, are technological instruments that serve to protect consumers' personal data. [19]

Another term Techopedia, mentioned the word certificate of reliability with *E-Commerce trustmark*. E-commerce trustmark is an electronic transaction badge, image or logo displayed on a website to indicate that the website's business has been proven trustworthy by the issuing institution. [20]

Some call certificates of reliability other than trustmarks, *trust icons*. *Trust icons* are generally badges, signs, seals or the like that when displayed on a website are intended to increase trust in the website.[21]

Privacy Policy Reliability Certificate, according to the Explanation of Article 76 paragraph (1) letter c of PP PSTE is a Reliability Certificate whose guarantee of reliability is to provide certainty that consumers' Personal Data is properly protected.[22] The Reliability Certification Body is responsible for several things in carrying out the certification process and aims to provide guarantees to business actors (in this case as electronic system organizers) so that the implementation of information technology and electronic transactions can run well.

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions Article 1 point 27 states:[23]

"Reliability Certificate is a document stating that Business Actors organizing Electronic Transactions have passed an audit or conformity test from a Reliability Certification Body."

Where "Business Actors" to include the reliability certificate as a sign that they have qualified a safe, reliable and trustworthy system. Reliability certificates in practice are issued

[19] Muhamad Amirulloh and Helitha Novianty Muchtar, "Implementation of Legal Certainty Principles and Pathetic Dot Theory in Relation to The Obligation Of Privacy Trustworthiness Certification To Safeguard Consumer Personal Data in E-Commerce.". SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4567892.

[20] Technopedia, *"E-commerce Trustmark"*, http://www.techopedia.com/definition/1491/e-commerce-trustmark> accessed on September 21, 2023.

[21] William Levins, "Do you need Trust Icons on your ecommerce site?", "https://www.nuvonium.com/blog/view/do-you-need-trust-icons-on-your-ecommerce-site", accessed on September 21, 2023.

[22] Muhamad Amirulloh, The Urgency of Reliability Certificates for Financial Institutions in Indonesia, https://blogs.unpad.ac.id/muhamadamirulloh/2023/05/30/urgensi-sertifikat-keandalan-bagi-lembaga-keuangan-di-indonesia/, accessed on April 25, 2024.

[23] Article 1 point 27 of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

by a registered Reliability Certification Body in Indonesia issued by the Minister of Communication and Information Technology.

In Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions Article 75 paragraph (1) states,[24] "Reliability Certification Bodies can issue Reliability Certificates through the Reliability Certification process." The inclusion of a reliability certificate on the *website* of electronic system actors indicates that the *website* has gone through a certification process. The provision of reliability certificates in Indonesia is also more clearly regulated in Article 1 number 11 of Law Number 19 of 2016 Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions detailed through Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions Article 76 paragraph (1) which applies three aspects of security in the form of:[25] Identity Registration is a certificate of reliability where the guarantee of reliability is only in the form of security which states that the identity of the electronic system actor is true; Electronic System Security is a certificate of reliability where the guarantee of reliability is to provide certainty regarding the process of delivering or exchanging data through the *website of* the electronic system actor and Privacy Policy is a certificate of reliability where the form of guarantee of reliability is to provide certainty that the personal data of electronic system users is protected confidentially as it should be.

Protection guarantees must certainly be provided by electronic system actors to generate trust from electronic system users. The Certificate of Reliability itself has 3 principles, namely as follows:

1) Reliability Principle

   Reliability as an ability possessed by a particular system that can adapt to the needs of its use, where Law Number 11 of 2008 concerning Electronic Information and Transactions amended by Law Number 19 of 2016 concerning Electronic Information and Transactions. Law Number 11 of 2008 concerning Electronic Information and Transactions Article 15 paragraph (1) states:

   "Every Electronic System Operator must operate the Electronic System reliably and safely and is responsible for the proper operation of the Electronic System." Therefore,

[24] Article 75 paragraph (1) of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

[25] Tesanolica, N. & Wulandari, T. B. (2021). "Inclusion of a Certificate of Reliability (Trustmark Logo) as a Form of E-Commerce Consumer Protection in Review of Applicable Regulations". *Dialogia Iuridica: Journal of Business and Investment Law volume 13, no. 4*. pp. 83-84.

the Electronic System Operator is responsible for the implementation of its electronic system.

2) Safety Principles

According to the ITE Law, security can be proven by protecting the electronic system both physically and non-physically. The use of information technology service providers carried out by electronic system actors must be based on a written agreement, while still paying attention to the principles of prudence, risk management and based on a reasonable cooperative relationship.

3) Consumer Protection Principles on Reliability Certificates

The inclusion of a reliability certificate or *trustmark logo* on an electronic system signifies legal certainty, especially for electronic system users. As for legal certainty itself provides two understandings where the first, there are rules that are general in nature so that individuals can know an act that is permitted or an act that is prohibited. Second, the creation of legal security for individuals caused by the arbitrariness of the government (state), in this case security is obtained from these general regulations so that individuals can find out what the state can impose on individuals and outside of these things, and the state may not impose on its people as users of electronic systems.

In Indonesia, the protection of personal data is a growing issue and a matter of public concern. The government makes laws and regulations relating to privacy and personal data protection in various aspects. This raises the issue of data privacy when personal data is provided.[26] So that October 17, 2022 Indonesia passed Law No. 27 of 2022 concerning Personal Data Protection, Article 1 paragraph (2) of the PDP Law: "Personal Data Protection is an overall effort to protect Personal Data in the course of processing Personal Data in order to guarantee the constitutional rights of Personal Data subjects." It is emphasized that the subject of personal data according to Article 1 paragraph 6 of Law No. 27 Year 2022 on Personal Data Protection is an individual to whom Personal Data is attached. Furthermore, Article 24 of the PDP Law reads: "In processing Personal Data, the Personal Data Controller is obliged to show proof of consent given by the Personal Data Subject."

[26] Richard D. Emmerson, Soewita Suhardiman, Eddy Murhty Kardono, Indonesia Report in Annual Review of Data Protection and Privacy Laws, Financier World Wide, December 2012, p. 62.

3.3 Implementation of the Obligation of Privacy Reliability Certificate in PBI and POJK and its Practice by Payment Fintek

The provision regarding the obligation to use the Privacy Reliability Certificate in Article 39 of the PDP Law has also been regulated in the financial sector in article 239 of the P2SK Law as explained in point 1. The P2SK Law is a law that specifically applies to financial sector businesses including payment fintech, thus the financial sector regulations, namely PBI No. 3/2023 and POJK No. 6/2022 should refer to article 239 of the P2SK Law.

In PBI No. 3/2023 there are two articles that mention the obligation of FSIs to protect personal data, namely Articles 32 and 36, but these two articles also do not clearly mention the use of Privacy Reliability Certificates. In POJK No. 6/2022 in Article 11 paragraph (5) it is stated that PUJK must use reliable information technology and must ensure the security of consumer information data, but in an ineffective way and also does not mention the use of a Privacy Reliability Certificate for Centrals. By not mentioning the Privacy Reliability Certificate, there is legal uncertainty. Gusta Radbruch stated four basic things about the meaning of legal certainty, namely:[27]

1. Law is a positive thing which means that positive law is legislation.
2. The law is based on a fact, meaning that the law is made based on reality.
3. The facts contained or listed in the law must be formulated in a clear way, so that it will avoid confusion in terms of meaning or interpretation and can be easily implemented.
4. Positive laws should not be easily changed.

In the third point, the PDP Law clearly regulates the obligation of Custodian to ensure the security of consumer personal data processing by requiring the use of personal data, as well as the P2SK Law. However, the regulations in POJK and PBI that regulate Custodian are not in line with what is written in the PDP Law and P2SK Law. It can be said that the legal facts formulated cause confusion in the interpretation of the law itself. So that in practice many PUSKs have not used the Privacy Reliability Certificate because of this legal uncertainty.

In practice, one of the payment fintechs from the Gojek platform, namely gopay. PT Gojek Indonesia was established in 2010 in Jakarta. The company was founded by Nadiem Makarim on the background of a problem experienced by the *founder* (Nadiem Makarim), namely the lack of availability of ojek transportation compared to other types of transportation. In addition, Nadiem Makarim observed the situation in the field that most ojek drivers only spend time to hang out waiting for passengers in certain areas, making it quite difficult for

[27] Satjipto Rahardjo, 2012, The Science of Law, Bandung, Citra Aditya Bakti, pp. 19

users to find ojek. From these problems, he observed that there is an opportunity to create a new business so that it can be a solution to the problem, namely a media link between ojek users and ojek drivers.

Then it has its own payment method *(e-wallet*), namely GoPay. GoPay is one of the payment services on the Gojek Application in the form of a digital wallet that can be used to make payment transactions or other financial transactions through the GoPay feature on the Gojek Application. GoPay payment services can be used to pay for services on the Gojek Application, Merchant GoPay business partners, use PayLater, to transfer balances to fellow GoPay users or bank accounts.

Figure 1. Gopay Privacy Policy
Source: Gopay Website

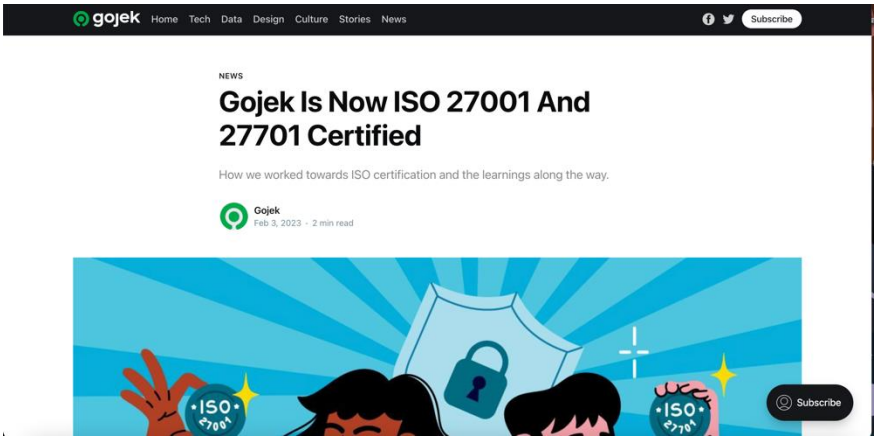

Figure 2. Gopay Privacy Policy
Source: Gopay Website

GoPay as a payment fintech has facilitated the rules regarding the privacy reliability certificate, namely 27701. Where it can make it easier for fintech related to the problem of fulfilling legacy requirements. GoPay and Gojek are committed to the community to maintain digital security through the Aman Bersama Gojek initiative by continuing to urge the public

to implement the JAGA step. That is, J: Do not transfer outside the application and be more careful when making transactions, A: Secure personal data, G: Use identification such as biometric verification or PIN for transactions, A: Immediately report anything suspicious to customer service or authorities if you are a victim of cybercrime.[28]

GoPay develops various technologies to maximize the security system, one of which is the biometric identification feature for authorizing users who will make transactions when making payments at business partners or transferring GoPay balances to other users. This feature is part of Gojek SHIELD, a security technology system to protect users from the risk of cybercrime. [29]

This is an obligation to use a privacy Certificate of Reliability for GoPay payment fintech actors, in accordance with the Personal Data Protection Law, as stated in Article 1 Point 2 and Article 39 of the PDP Law as an overall effort to protect personal data in all stages of data processing to guarantee the constitutional rights of Personal Data subjects.

These regulatory changes will have an impact on changes in consumer behavior that require new or modified products and services. The broad scope of fintech has led some fields such as e-commerce, banking, and financial technology to create special regulations related to consumer protection, especially the protection of consumer personal data. [30]

4. CONCLUSION

PBI No. 3/2023 and POJK No. 6/2022 have not explicitly regulated the use of Privacy Reliability Certificates for Financial Sector Business Actors. However, if we reflect on the PDP Law, the norms related to the use of Reliability Certificates between the PDP Law and the P2SK Law are "*dwingend*" with the use of the phrase "mandatory" in Article 39 paragraph (1) and (2) of the PDP Law. This creates legal uncertainty and has an impact on the practice of financial technology.

Based on the results of the research that has been conducted, it is concluded that the business actors studied, namely Gopay from Gojek, have obtained a certificate of reliability of the ISO 27701 privacy reliability system. GoPay as a payment fintech actor, has followed the rules written in the Personal Data Protection Law, in accordance with Article 39 of the PDP Law as an overall effort to protect personal data in all series of data processing to guarantee the constitutional rights of Personal Data subjects.

---

[28] GoPay, "GoPay Continues to Prioritize User Information Security with ISO 27001: 2013 Certification", https://gopay.co.id/blog/keamanan-informasi, accessed on February 17, 2024, at 16:38 WIB.
[29] *Ibid.*
[30] Adis Nur Hayati & Antonio Rajoli, "Analysis of Refund Compensation Mechanisms in E-CommerceTransactions in View of Consumer Protection Law", *Scientific Journal of Legal Policy*, Volume 15, no 3, 2021.

REFERENCES

Books

Ashshofa, B. (2013). Legal research methods. Jakarta: Rineka Cipta.

Balboni, P. (2008). Trustmarks: Third-party liability of trustmark organizations in Europe.

Freedman, R. S. (2006). *Introduction to financial technology*. Elsevier.

Ilmar, A. (2012). *State control rights in the privatization of SOEs*. Jakarta: Kencana.

Kusumaatmadja, M. (1986). Legal Development in the framework of national development. *Bandung: Binacipta.*

Kusumaatmadja, M., & Sidharta, B. A. (2018). Introduction to the Science of Law: A First Introduction to the Scope of Applicability of Legal Science, Book I, Alumni.

Rahardjo, S. (2000). The *science of law*. Bandung: Citra Aditya Bakti.

Soekanto, S. (2006). Introduction to legal research. 3rd ed. Jakarta: UI Press.

Soekanto, S. (2007). Normative legal research: A brief overview. Jakarta: Rajawali Press.

Syamsudin, M. (2007). Operationalization of legal research. Jakarta: Grafindo Persada.

Wilson Jr, J. D. (2017). *Creating strategic value through financial technology*. John Wiley & Sons.

Regulations

Constitution of the Republic of Indonesia Year 1945;

Law Number 27 Year 2022 on Personal Data Protection;

Law Number 8 Year 1999 on Consumer Protection;

Law No. 19/2016 on Electronic Information and Transactions;

Law No. 4 of 2023 on Financial Sector Development and Strengthening;

Bank Indonesia Regulation No. 3 Year 2023;

Financial Services Authority Regulation No. 6 of 2022;

Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions;

Government Regulation No. 80/2019 on Trading Through Electronic Systems.

Other sources

Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of Fintech: A new post-crisis paradigm. *Geo. J. Int'l L., 47*, 1271.

Denisa, A. P., Amirulloh, M., & Muchtar, H. N. (2023). Privacy Reliability Certificate As A Form

Of Consumer Protection In The Field Of Information And Electronic Transactions. *Journal of Rechts Vinding: Media for National Law Development*, *12*(2).

Amirulloh, M., & Muchtar, H. N. (2023) Implementation of Legal Certainty Principles and Pathetic Dot Theory in Relation to The Obligation Of Privacy Trustworthiness Certification To Safeguard Consumer Personal Data in E-Commerce.

GoPay. GoPay Continues to Prioritize User Information Security with ISO 27001: 2013 Certification. https://gopay.co.id/blog/keamanan-informasi.

Hayati, A. N., & Ginting, A. R. (2021). Analysis of Refund Compensation Mechanisms in E-Commerce Transactions Viewed from Consumer Protection Law. *Scientific Journal of Legal Policy*, *15*(3), 509-526.

Ministry of Communication and Information, Kominfo's Fast Movement to Protect Personal Data, (2021) https://www.kominfo.go.id/content/detail/34813/gerak-cepat-kominfo-melindungi-data-pribadi/ 0/article.

Puslitbang Aptika and IKP. (2019). Development of Digital Economy in Indonesia.

Setiawan, A. B. (2014). Study of Electronic Certificate Standardization and Reliability in the Implementation of Electronic Transaction System. Post and Telecommunication Bulletin, 12(2), 119-134.

Suryono, R. R. (2019). Financial technology (fintech) in axiological perspective. *Masyarakat Telematika Dan Informasi Journal of Information and Communication Technology Research*, *10*(1), 52.

Tesalonica, N., & Wulandari, B. T. (2021). Inclusion of a Certificate of Reliability (Trustmark Logo) as a Form of E-Commerce Consumer Protection in Review of Applicable Regulations. *Dialogia Iuridica*, *13*(1), 79-96.

Van Ark, B., Erumban, A., Corrado, C., & Levanon, G. (2016, October). Navigating the new digital economy: driving digital growth and productivity from installation to deployment. Conference Board, Incorporated.

Yaqin, A., & Ilfitriah, A. M. (2015). The Effect of Service Quality on Satisfaction and Loyalty of E-Banking Bank Customers in Surabaya. *Journal of Business & Banking*, *4*(2), 245-160.