http://dx.doi.org/10.18860/j.v11i2.7921

THE RISKS OF PERSONAL DATA THEFT IN FINTECH-BASED ONLINE LOAN APPLICATIONS DUE TO THE ABSENCE OF LAW IN INDONESIA

Dwi Nugrahayu Devianti, Prija Djatmika, Sukarmi
Faculty of Law, Universitas Brawijaya, Indonesia
Email: ayudevianti13@yahoo.com

Abstract

The online loan via financial technology (fintech) is currently a new buzz in Indonesian society. Its facilities and ease in proposing the loan are very much attracting. However, this online loan practice often raises legal issues; one of them is personal data misuse. This article analyzes the usage of other people's personal data in fintech services. This is a doctrinal legal research with statute approach. The results reveal that personal data protection has yet firmly ruled in legislation. This proves that privacy is not an urgent matter to safeguard. It then implies to the many cases on personal data theft in online loan. The operators of fintech services are responsible to protect customers' personal data. Those found guilty to misuse the personal data will be subject to criminal sanction.

Pinjaman online melalui teknologi finansial menjadi trend baru masyarakat Indonesia. Berbagai fasilitas dan kemudahan dalam pengajuan pinjaman menjadi daya tarik tersendiri. Namun, praktik pinjaman online sering menimbulkan persoalan hukum, salah satunya adalah penyalahgunaan data pribadi. Artikel ini bertujuan menganalisis penggunaan data pribadi orang lain dalam layanan finansial teknologi. Artikel ini berasal dari penelitian hukum doctrinal dengan pendekatan peraturan perundang-undangan. Hasil penelitian ini menunjukkan bahwa perlindungan data pribadi belum diatur secara tegas dalam peraturan perundang-undangan. Kondisi ini menunjukkan bahwa privasi bukan persoalan yang urgen untuk dilindungi. Hal ini berimplikasi terhadap maraknya pencurian data pribadi dalam pinjaman online. Penyelenggara jasa layanan finansial teknologi memiliki tanggung jawab untuk melindungi data pribadi nasabah. Penyelenggara yang terbukti menyalahgunakan data pribadi dapat dikenai sanksi pidana.

Keywords: *financial technology, online loan, personal data.*

Introduction

Fintech is an abbreviation of Financial Technology or in Indonesia it is called as *Teknologi Finansial* (TekFin). According to The National Digital Research Center (NDRC) in Dublin, Ireland, *Fintech* is defined as "innovation in financial services" which is a breakthrough from financial sector that has the sense of modern technology.[1] Some *Fintech* companies in Indonesia are CekAja, UangTeman, Pinjam, CekPremi, Bareksa, Kejora, Doku, Veritrans, and Kartuku.[2] Allah says in QS. Al-Baqarah [2]: 245 "Who is it that would loan Allah a goodly loan so He may multiply it for him many times over? And it is Allah who withholds and grants abundance, and to Him you will be returned."[3] The verse explains that those giving loan in the name of Allah, then He will increase the people's merit. It means that everyone is suggested to lend others who are in need.

The realization of *Fintech* based on *peer-to-peer lending* needs certain regulation since *Fintech* is included in micro prudential so its activities are always supervised by *Otoritas Jasa Keuangan* or the *Financial Services Authority* (hereinafter mentioned as OJK). One of essential factors in the sustainability of Indonesian *Fintech* system is the public trust on the guarantee of personal data security used in online loan service, according to The Regulation of Ministry of Communication and Informatics No. 20 of 2016 concerning Personal Data Security in Electronic System. Personal data is an individual data which validity and confidentiality are saved and guarded.[4] Practically, the emergence of these *Fintech* companies which are officially registered and supervised by the OJK also causes new law problems.

Take an example, *RupiahPlus*, an online loan application, suddenly called a party who never once had any business related to debts. At that time, Ali Akbar was called by *RupiahPlus* on debts made by his Junior High School's friend, whereas, in fact, they have never kept in touch for so long. Because of this, OJK issued an official Reminder Letter level 1 to *RupiahPlus*. According to the letter, *RupiahPlus* broke at least two rules. First, it breaks The OJK Regulation (known as *POJK*) No. 1 of 2013 concerning Data Protection of Financial Services Consumer. Second, the

1 Ernama, Budiharto, & Hendro S., Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology,Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 (Semarang: Diponegoro Law Journal, Vol. 6, No.3, 2017), 1.

2 Ernama, Budiharto, Hendro S., Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology,Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016, 2.

3 Departemen Agama Republik Indonesia, *Alquran dan Terjemahnya* (Jakarta: CV JArt,2004), 39.

4 The Regulation of Ministry of Communication and Informatics No. 20 of 2016 concerning Personal Data Security in Electronic System.

company breaks The Regulation of Ministry of Communication and Informatics No. 20 of 2016 on Personal Data Security in Electronic System. [5]

For data verification reasons, identity card and self-portrait pictures of the borrower are then saved, spread, and even misused by the online loan application developer. Besides, the Legal Aids in Jakarta also note that the application developer accesses almost all data from borrower's device. This becomes the root problem of the spread of personal data and the information from borrower's device. It is definitely a violation against privacy rights. Based on the complaints received by the Legal Aids in Jakarta, 48% informers used 1 to 5 online loan applications, however there are also those using 36 to 40 applications.

The informers use many online loan applications because they need to propose the loan from different applications to cover the interest, fine, or even provision from previous debts. "This causes the application users trapped into 'an evil circle' of online loan applications usage," said Jeany as quoted from the website of Legal Aids, Jakarta. The worse thing is that 25 of 89 application operators reported to the Legal Aids are the ones registered in OJK. This shows that even though the online loan applications are officially listed in the OJK's database, they are not problem-free.[6]

Besides, users' personal data can be easily exploited by irresponsible parties to get more advantages. One of the crimes is robbing the data, then multiplying it to be used as the identity of fictional borrower in different applications of loan service *fintech*.

One of the realizations of personal data security is written in The Law No. 19 of 2016 on the Amendment of Law No. 11 of 2008 concerning Technology and Electronic Information; Section 26 states[7] that Article (1) unless it is determined by legislation, the use of each information through electronic media regarding one's personal data must be known by the related person. Article (2) those whose rights are violated according to the article (1) can file a lawsuit for the loss based on this law.

On the basis of the aforementioned section, information technology usage and personal data security are privacy rights, thus, when there is a misuse of ID card number and Family Registry, it means that there is no guarantee on personal data security and protection. Grounded on this background description, the

5 https://tirto.id/menggadai-data-diri-demi-ngutang-pinjaman-online-dgLB accessed in February 20, 2019

6 https://www.hukumonline.com/berita/baca/lt5c389ac751125/berkaca-dari-kasus-vloan--masyarakat-diminta-waspada-lakukan-pinjaman-online accessed in February 2, 2019

7 Article 26, The Law No. 11 of 2008 concerning Technology and Electronic Information.

authors are concerned to write the article entitled "Juridical Implication of People's Personal Data Usage for The *Fintech*-Based Loan Service in The Perspective of Legislation in Indonesia".

Research Methods

The research method employed in this study is juridical-normative by applying statute approach – by reviewing the laws related to the research theme, as well as analytical and conceptual approach. Conceptual approach is done when the researcher does not move from the existing law, for instance, there is yet or no laws on certain problems.[8]

Primary law resources are the legal that is bound, in the form of legislation i.e. The Law No. 19 of 2016 on the Amendment of Law No. 11 of 2008 concerning Technology and Electronic Transaction; the Regulation of Ministry of Communication and Informatics No. 20 of 2016 issued in December 1, 2016; the Regulation of the Financial Services Authority (POJK) No. 77/POJK.01/2016 concerning Information Technology-based Loan Service; the Regulation of the Financial Services Authority Number 1/POJK.07/2013 concerning the Consumer of Financial Service Sector Protection; and the Regulation of the Financial Services Authority Number 13/POJK.02/2018 concerning Digital Finance Innovation in the Financial Service Sector.

This study implements library research by applying *card system*. The analysis technique of legislation material is done by analyzing the obtained data, normative analysis method will also be used – by interpreting and discussing the research data based on law definition, law norms, law theories, and doctrine related to the main problem.

Discussion

This study discusses financial technology and personal data that have connection and indirectly give notary beneficial. *Fintech* field is an establishment in the technology-based banking sector. Banking credit has strong connection with notary; besides, personal data protection is the thing that must be paid more attention by notary.

Notary should take roles in protecting the personal data written in the issued certificate, reviewed in the Article 4 Section 2, The Legislation on Notary Public states that a notary will keep the certificate content secret as well as the

8 Johnny Ibrahim, Teori & Metodologi Penelitian Hukum Normatif (Malang: Bayumedia, 2007), 99.

information obtained in the notarial implementation. It means that the notary is not allowed to spread the information written in the certificate as well as the content of certificate's appearer containing parties' identity related to notarial certificate. So, the notary takes part in protecting personal data from the leakage that can be misused by irresponsible people.[9]

Positive Law in Indonesia which Gives Legal Protection Related to Personal Data of Fintech-Based Loan Service Users

Data security and confidentiality issues are two of critical aspects of an information system. This shows how weighty the information is to be sent and received by whom it is concerned. The information will be useless if, on its way, it is bugged or intercepted by irresponsible person. Hence, information system security has been the buzz when electronic transaction was first introduced. The tight and sophisticated security and information technology developments do not greatly contribute to society[10].

The connectivity of information system and internet gives high chance to cyber-crime. This is a challenge for the law enforcer. The law in most of countries does not cover *cyberspace*. Now, almost all countries compete to prepare legal foundation for internet. Regarding the existing incident and the needs of data security in computer, data security's scope of a computer system covers all aspects including physical, access, file and data, and network securities[11].

The personal data policy is the matter accommodated by service provider to protect the private data of service users. It also includes varied clauses regarding the personal data utilization and tabulation. To date, the regulation on personal data protection in Indonesia is still spread in several rules. Therefore, the comprehensive regulation of personal data protection is essentially needed because there is yet such law becoming the *lex specialis* concerning personal data protection, particularly in *fintech* business.

The following are regulations on personal data that must be safeguarded and governed: 1) The Law No. 24 of 2013 Article 58 Section (2); 2) The legal protection of customer data in The Law No. 11 of 2008 concerning information technology and electronic transaction Article 26 Section (1); 3) The legal protection of personal data in The Law No. 19 of 2016 on Electronic Information and Transaction; and

9 Article 4 Section 2, The Law No. 30 of 2004 concerning the notary position.

10 G.A Barger, Lost in Cyberspace : Inventors, Computer Piracy and Printed Publications under Section 102 (b) of the Patent Act of 1994, (Detroit : Mercy L. Rev), 353.

11 Purwanto, Penelitian Tentang Perlindungan Hukum Data Digital (Jakarta: Badan Pembinaan Hukum Nasional, 2007), 49.

4) POJK No. 77/01 of 2016 Article 29 (d).

The online loan application like *Tunaiku* is an example that the requirements in registering loan application is very simple. Those are uploading self-portrait with identity card, filling the data based on the ID card, and being Indonesian citizen[12]. Another online loan application is *UangTeman* which only requires its customer to prepare the supporting document such as ID card picture, the new self-portrait, and a copy of salary slip.[13] The citizen's administrative law has yet covered the protection of personal data used in *fintech* application. Self-portrait should be categorized in personal data which must be guarded not to trigger the misuse of other people's personal data to take out a loan in an online application, so it can be assumed that there is a personal data leakage used by the irresponsible third party to register in an online loan application.

Qard means *al-qath'u* (cutting)[14], that the property given to the debtor is a part of the creditor's property.[15] The legal basis of *qard* is written in the Quran, sunnah, and ijma'(consensus), those are: 1) QS. al-Baqarah [2]: 245 "Who is it that would loan Allah a goodly loan so He may multiply it for him many times over? And it is Allah who withholds and grants abundance, and to Him you will be returned"[16]; 2) QS. Al-Hadid [57]: 11 "Who is it that would loan Allah a goodly loan so He will multiply it for him and he will have a noble reward?"[17]; 3) QS. Al-Maaida [5]: 2 "And cooperate in righteousness and piety, but do not cooperate in sin and aggression."[18] Based on the study, by reviewing the law on personal data security in *fintech*-based loan service, the researcher will explain the positive law in Indonesia which gives legal protection related to personal data of *fintech*-based loan service users.

The Law No. 19 of 2016 on the Amendment of The Law No. 11 of 2008 Concerning Electronic Information and Transaction

Article 26 of The Law on Electronic Information and Transaction provides the protection against illegal personal data usage. The aforementioned article obliges to legally ask permission to the data owner before using the personal information in electronic media. Those disobey this rule can be filed for the loss.

12 https://tunaiku.com/, accessed in August 21, 2019 at 4.53 PM.
13 https:/uangteman.com/, accessed in August 22, 2019 at 8.47 PM.
14 Mahmud Yunus, *Kamus Arab-Indonesia* (Jakarta: Hidakarya Agung, t. th), 337.
15 Ahmad Wardi Mulich, Fiqh Muamalat (Jakarta: AMZAH, 2010), 273-274.
16 Departemen Agama Republik Indonesia, Alquran dan Terjemahnya, 39.
17 Departemen Agama Republik Indonesia, Alquran dan Terjemahnya, 538.
18 Departemen Agama Republik Indonesia, Alquran dan Terjemahnya, 101.

In the explanation, the article states that personal data is one of privacy rights. In the section (1) of that article also explains further about the definition of privacy right. The content is that, in the utilization of Information Technology, personal data protection is a part of privacy rights.

Based on the analysis of legal protection theory, Article 26 of The Law on Electronic Information and Transaction has firmly stated that the realization of legal protection for someone in utilizing a certain information technology is the obligation of a person to have permission for every usage of people's personal data in an information technology system unless it is governed further by the law and someone's rights are guaranteed to file a lawsuit if they feel wronged because of the illegal use of their personal data. It is because the law protects someone's concern by giving him/her the authority to strive for fulfilling the needs. This authority, or is often called as the *right*, is fulfilled in a proper measurement both in terms of the width and the depth.[19]

In the perspective of legal protection theory, Article 30 of The Law on Electronic Information and Transaction has strongly said, the realization of legal protection for someone in utilizing a certain information technology is that one is prohibited to get electronic information by disobeying, breaking, exceeding, or busting security system. It means that every act of a person who does not get the data owner's permission or whoever does not have the authority to use certain personal data, unless it is governed further by the law, is prohibited based on this article.

Article 31 of The Law on Electronic Information and Transaction explains that the interception is included in one of prohibited acts unless it is done by the authorized legal parties, which is ruled further based on the law. According to the legal protection theory, this aforementioned article firmly enunciates, on the realization of legal protection for someone who uses certain information technology, that the interception of other people's personal data without the rightful authority and owner's concern is considered as breaking this article.

According to Satjipto Raharjo, what it means by legal protection is to give defense toward Human Rights violated by other people and this protection is presented to society so they can enjoy all rights given by the law. The law can be functioned to discover the protection, which is not only adaptive and flexible, but also predictive and anticipative. The law is needed for those who are weak and not powerful in terms of social, economy, and politic to obtain social justice.[20]

19 Satjipto Rahardjo, *Teori Dasar Ilmu Hukum* (Bandung: PT. Citra Aditya Bakti, 2000), 53.
20 Satjipto Rahardjo. *Teori Dasar Ilmu Hukum*. 53.

Thus, the Article 31 of the Law on Electronic Information and Transaction can give limitation to which extent someone has the right to access people's personal data for the sake of law enforcement. Meanwhile, if only there is the involvement of data processor in a corruption act, illegal consumer analysis, fraud, money laundering, terrorism fund, embezzlement, and so forth, and if this is known but is considered as an act of intentional omission by the business owner, then he/she will be charged by the rule written in the Article 31 of the Law on Electronic Information and Transaction.

Article 35 of the Law on Electronic Information and Transaction forbids everyone who intentionally and illegally uses others' personal data as if it is authentic and is fraud as the real owner. Whereas in fact, it is known that the data is used without the concern of the real data owner.

If it is analyzed, the legal protection theory is the one provided to legal subjects in the form of instruments, both preventive and repressive. In other words, legal protection is a self-portrait of the law function which has concept that law provides justice, certainty, benefit, and peace.[21]

Then, the embodiment of legal protection in the article's provision is about the prohibitions for anyone who deliberately violates the law to do manipulation, creation, change, omission, and demolition of Electronic Information and/or Electronic Document with the aim that the information is deemed as authentic data.

POJK No. 77/POJK.01 of 2016 Concerning Technology-Based Money Loan Services

Article 26 POJK No. 77/POJK.01/2016 concerning Information Technology-Based Money Loan Services, if it is analyzed using legal protection theory, i.e. a form of protection provided to the legal subjects based on the information of the aforementioned POJK article, we know that the service providers are obliged to ask the permission from the data owner by giving authentication or authorization before accessing the personal data as an assurance that the person complies with the provisions of the law.

However, the article, as mentioned in the point number 5, "to notify in writing to the owner of personal, transaction, and financial data if there is a failure in protecting the confidentiality of personal, transaction, and financial data they manage", has yet explained in specific about the accountability when they have failed in securing the data. The article only affirms the obligation in informing to

21 Satjipto Rahardjo. *Teori Dasar Ilmu Hukum*. 19.

the owner of personal, transaction, and financial data if there is a system failure in their management and does not explicitly explain the compensation mechanism and the efforts to improve the management of personal, transaction, and financial data provided by the service provider or the application developer. It also includes *data breach* that is known and is not prevented or resolved, so the accountability is charged to the entrepreneurs. Hence, the expansion and additional obligations should be done to ensure that the data manager, if involved in a criminal act, can be held accountable.

Article 28 POJK No. 77/POJK.01/2016 concerning Information Technology-Based Money Loan Services, if analyzed using legal protection theory, mentions a form of legal protection provided to legal subjects. The article obliges to every provider of online loan service to own and perform a security system to evade trouble, failure, and loss due to a law-breaking act to break into security system of an information technology-based loan service application. What it means by "breaking" is an attempt against the law with the intention of making a profit from electronic document saved in an electronic *fintech* application system.[22]

Furthermore, Electronic Document is defined as an Electronic Information that is made, forwarded, sent, received, or saved in a form of analogue, digital, electromagnetic, optical, and the like which can be seen, displayed, and/or heard via Computer or Electronic System; it is not limited to writing, voice, image, map, plan, picture or the like, alphabet, sign, number, access code, symbol or perforation that have meaning or can be comprehended by those who understand it.[23] The article clearly mentions the obligation of a kind of mechanism of data security system, particularly the personal data of *Fintech*-based loan services users.

Article 39 POJK No. 77/POJK.01/2016 concerning Information Technology-Based Money Loan Services, if analyzed using legal protection theory, mentions a form of legal protection provided to legal subjects. The article firmly forbids the technology-based loan service provider to, in any way, give data and/or information about the users to the third party. The provider, as ruled in the mentioned article, takes role as Electronic System operator i.e. a person, state administrator, business entities, and society which provide, manage, and/or operate Electronic System, both individually and collectively, to the users of Electronic System for their own needs and/or others'.[24]

---

22 Falguni Desai, "*The Evolution of Fintec*h" https://www.forbes.com/sites/falgunidesai/ 2015/12/13/ the-evolution-of fintech/2/#445f1f363dd0, accessed in June 11, 2019

23 Article 28 POJK No. 77/POJK.01/2016 *concerning Information Technology-Based Money Loan Services*

24 Article 1 POJK No. 77/POJK.01/2016, Tentang Layanan Pinjam MemjamUang Berbasis Teknologi.

The article 39 POJK No. 77/POJK.01/2016 has adequately explains that it requires the operator not to submit the users' personal data to the third party unless it is granted by the data owner. This creates the chance to personal data misuse if the user is negligent and not vigilant in using *fintech*-based loan service by not reading the requirement and rules in using that application.

Law No. 82 of 2012 Concerning the Implementation of Electronic Systems and Transactions

Article 15, in accordance with the provisions of Article 15 of Law 82 of 2012 concerning the Implementation of Information Systems and Electronic Transactions, states that every provider of technology-based loan services should be able to guarantee and protect the personal data it manages.

The Regulation of the Minister of Communication and Information Technology No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems

In order to implement the provisions of Article 15 paragraph (3) of the 2012 Government Regulation Number 82 concerning the Implementation of Electronic Systems and Transactions, it is necessary to stipulate the Regulation of the Minister of Communication and Informatics concerning Personal Data Protection in Electronic Systems. In the 2012 Government Regulation (GR) Number 82 regarding the Implementation of Electronic Systems and Transactions, Article 20 paragraph (2), the Electronic System provider is required to provide a security system comprises the procedures, prevention systems and control of threats and attacks that may cause disruption, failure and loss.

The formulation of a Ministerial Regulation on the Security Systems is mandated by GR of the Implementation of Information Systems and Electronic Transactions in Article 20 Paragraph (4), which states: further provisions regarding the security system as mentioned in paragraph (2) is regulated in a Ministerial Regulation. The referred Ministerial Regulation is the 2016 Regulation of the Minister of Communication and Informatics Number 4 concerning the Information Security Management Systems.[25]

If it is analyzed based on the theory of legal protection, Article 1 Paragraph (4) of the 2016 Regulation of the Ministry of Communication and Informatics Number 20 concerning the Protection of Personal Data in Electronic Systems is

25 http://bsn.go.id/main/berita/detail/7561/bsn-selenggarakan-sosialisasi-peraturan-menteri-kominfo-no.-4-tahun-2016#.XRhoGVwzY2w Accessed in June 16, 2019

a form of legal protection given to legal subjects. Hence, it is compulsory to ask for the consent of the personal data owner, which is further referred to as the Agreement. It is a written statement, which is made manually and/or electronically, provided by the Personal Data Owners who have received a complete explanation of the actions of obtaining, collecting, processing, analyzing, storing, displaying, announcing, sending, and distributing Personal Data as well as the confidentiality or non-confidentiality.

A statement related to Article 2 of the 2016 Regulation of the Ministry of Communication and Informatics Number 20 concerning the Protection of Personal Data in Electronic Systems has occurred. If it is analyzed based on the theory of legal protection affirmed as a form of legal protection provided to legal subjects regarding data availability, Article 28 (f) states that the personal data processor is in fact a legal entity. Therefore, a regulation concerning the responsibility of the entrepreneurs in providing *fintech* services as well as collecting and processing the data is necessary to be enacted. In relation to this, the government sets an obligation to the electronic system providers or P2P Lending providers to protect any matters that encompass confidentiality, integrity, and availability of personal data, also the transaction and financial data that are managed by the providers since they were first obtained until the destruction.

The Urgency of Personal Data Protection Regulations in Fintech-Based Loan Services

The rapid development of information technology-based industries has made the public aware of the importance of protecting their personal data confidentiality from various threats of data misuse. The concerns about breaches of privacy and protection of personal data have spread among the society in Indonesia. It happened since, sociologically, most countries in Asia, including Indonesia, initially had no awareness about privacy. It is inseparable from the history of Asian people who have been living in communal societies that have no attention for privacy. Basically, the term privacy that is associated with human right originated in the West (not from Indonesia).[26]

Privacy, later, becomes crucial in the era of information and communication technology, so the need for the enactment of laws that regulate the protection of privacy and personal data is an urgent agenda. The incidents of the misuse of personal data that have recently arisen prove the importance of the law that regulates the personal data protection.

26 Academic Script of Naskah Akademik RUU (The Bill) of PDP p. 126

This has made the financial technology (*fintech*) providers restless because numerous people applied for online loans using fake identities. A Twitter account, @hendralm, has once revealed a data trading involving identity numbers, family registration certificate, and one's self-portrait photograph while holding Residential Identity Card. These data were obtained through various channels offering fast loans. This data trading is carried out on various social media such as Instagram and Facebook. Unfortunately, the demand is quite high. These individuals deliberately use other people>s data to apply for online loans to peer-to-peer (P2P) lending platforms or paylater features provided by any giant e-commerce. If the loan has been disbursed, they will not be charged for anything. Consequently, the original owner of the identity card becomes the victim.[27]

Another case was disclosed by a *fintech*-based loan services named Danamas, a P2P lending company, a subsidiary of the Sinarmas Group, which focuses on financing productive loans to phone credit sellers. Danamas also provides loan features through Traveloka. The frauds were both committed by the Danamas' and Traveloka's customers. The fake borrowers applied for a loan to Danamas using other people's data, self-portrait photographs showing others' identity card. To deceive *fintech* that ran a location verification, these fraudsters deliberately went to the residence of the identity cards owner. As a result, the disbursed funds cannot be reimbursed, and Danamas couldn't do much. It could only encourage the victims, the original owner of the identity card, to report this case to the police because the one that experienced a loss was not the platform, but the lenders or funders.[28] This demonstrates that the provision of the data authenticity verification that is conducted using the *Know Your Customer* principles, which is implemented by the online-based loan service providers, cannot completely prevent the misuse of other people's personal data for the unilateral benefit committed by the fraudsters.

Danger can arise from theft of personal data, systems damage that allow data breaches (including personal data), misuse of personal data that has been controlled by the entrepreneurs [29] or other parties that can access consumers' personal data (the government, for example).[30] The need for this regulation is considered important because personal data is the right to privacy of someone.

27 Bandar Data Ilegal Bobol Fintech Lending, https://finansial.bisnis.com/read/20190806/ 89/1132988/ bandar-data-ilegal-bobol-fintech-lending, accessed in August 13, 2019

28 Bandar Data Ilegal Bobol Fintech Lending, https://finansial.bisnis.com/read/20190806/ 89/1132988/ bandar-data-ilegal-bobol-fintech-lending, accessed in August 13, 2019

29 See the google privacy policy, which states the right to change and distribute the personal data without asking permission from the data owners.

30 As occurred in the iCloud hacking; The Academic Script of RUU (the Bill) of PDP p. 44

It may also have economical values for the third parties who have the intention to exploit it.

The threats caused by a legal vacuum regarding the personal data protection will be very detrimental to consumers because there are many threats caused by negligence and theft. These may be triggered by the inadequate personal data protection system initiated by the *fintech* sector's entrepreneurs or the deliberate action of the entrepreneurs or labors of the *fintech* business sector that intend to break into people's personal data for certain purposes. This risk may cause other countries that already have better personal data protection regulations, the consumers, and potential consumers of *fintech* services put a bad label to the *fintech* in Indonesia.

This is associated with the hadith narrated by Uqbah bin 'Amir stating that Rasulullah SAW has declared:

> *"I heard the Messenger of Allah says: 'The Muslim is the brother of another Muslim, and it is not permissible for a Muslim to sell his brother goods in which there is a defect, without pointing that out to him'." (HR. Ahmad, Ibnu Majah, Daruquthni, Hakim and Tabrani)*

In another hadith narrated by Adda 'bin Khalid, regarding *khiyar aib* (rights granted by Islamic law against the buyer and seller whether to continue or cancel the contract in place due to defect) he said,

> *"Adda' bin Khalid bin Hawdhah said to me: 'Shall I not read to you a letter that the Messenger of Allah, wrote to me?'. In it was: 'This is what 'Adda' bin Khalid bin Hawdhah bought [from] Muhammad the Messenger of Allah. He bought from him a slave' or 'a female slave, having no ailments, nor being a runaway, not having any malicious behavior. Sold by a Muslim to a Muslim."*

Juridical implication for the people who misuse other people's personal data and the original owner of the personal data used by other people in loan service legal relationships among the parties involved in a loan service:

1. Legal Relationship between the Provider and Borrower

   The provider and the borrower have a legal relationship documented in a form of an agreement. This agreement is an Information Technology-based loan service agreement. It is issued when the borrower has accepted all terms of use determined by the provider and submits a loan application based on the conditions that have been determined by the provider.[31]

31 Ernama, Budiharto, & Hendro S., Pengawasan Otoritas Jasa Keuangan Terhadap Vinancial Teknology, Peraturan Otoritas Jasa keuangan Nomor 77/POJK.01/2016, Diponegoro Low Jurnal, Vol.6, No.3 (2017): 33.

2. Legal Relationship between the Provider and Lender
   The provider and the lender have a legal relationship documented in the form of an agreement concerning the implementation of Information Technology-based loan service. It is issued because the lender binds himself to the provider to provide loans/funding for the borrower who submit the loan application through the provider. This agreement of implementation is considered to be the start of the loan agreement that will occur.[32]

3. Legal Relationship between the Borrower and the Lender
   The lender and the borrower have a legal relationship documented in the form of a loan agreement. Lending and borrowing, according to Article 1754 of the Civil Code, is an agreement whereby one party gives the other party a certain amount of goods that can be used up, on the condition that the latter party will return the same amount of goods of the same type and quality.[33]

Juridical Implications of Other People's Data Users in Loan Services

As a user of other people's personal data, in terms of applying for loans in loan services, one can be categorized as a perpetrator of information theft, subject to sanctions under article 30 paragraph (2) of Law Number 11 of 2008 concerning Electronic Information and Transactions. Based on the article, the perpetrators of information theft have fitted the elements of article 30 paragraph (2) of the ITE Law, by any methods including infiltrating a computer security system either by using certain *software* or others aiming to steal someone's data or information in accordance with the provisions of Article 46 paragraph (2).

Next, regulations have been made for those who use other people's personal data when they carry out activities, such as changing, adding, reducing, transmitting, destroying, removing, replacing, or hiding Electronic Information and/or Electronic Documents belonging to other people or public property. Article 32 Paragraph (1) to Paragraph (3) has regulated the criminal sanctions that can indict a person who deemed to have violated the provisions of Article 32 as regulated in Article 48 paragraph (1) to paragraph (3).

32 Ernama, Budiharto, Hendro S., Ernama, Budiharto, & Hendro S., Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology, Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016, Diponegoro Law Journal, Vol. 6, No.3 (2017): 33.

33 Ernama, Budiharto, Hendro S., Ernama, Budiharto, & Hendro S., Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology, Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016, Diponegoro Law Journal, Vol. 6, No.3 (2017): 11.

Based on the progressive legal theory that the use of other people's personal data is categorized as an identity fraud, then this is indeed a very distressing act for the society. The digital era has made it easier for someone to find and access our personal data, such as photos and personal identities. In contrast, the contents of Article 58 paragraph (2) of law number 24 of 2013 does not state that ones' photos are personal data that must be protected.

There are also no other regulations regarding the protection of personal data that state personal photos and data should also be categorized as personal data, considering the technological advances perspective. This could be the reason why personal data still can be easily misused by others for online loan applications. The establishment of a personal data protection law is urgently needed because technological developments are also advancing very rapidly. Through the existence of adequate laws, technological developments can be used safely.

The Juridical Implications of Original Owners of Personal Data in Loan Services

As the owner of the original personal data and also as a victim of an information theft, the victim has the right to legal protection. This legal protection provision must be optimized considering the victims who are, particularly, economically weak. The legal protection can be implemented in the form of compensation, restitution and legal assistance as regulated in Government Regulation Number 44 of 2008 concerning Compensation, Restitution and Assistance to the Witnesses and Victims. For a criminal act of personal data theft, it is more appropriate for the victim to get Restitution.

The theft of personal information is one of the most common threats of crime today, which is carried out by stealing other people's important data. These important data, of course, contains personal data (name, address, email, cellphone number, etc.) and the data related to finance, including bank data (account numbers), ATM data, and credit card data.

One of the personal data protection forms is regulated in Law number 19 of 2016 concerning the amendments to Article 26 of the Law number 11 of 2008 regarding Electronic Technology and Information;[34]

(1) "Unless provided otherwise by Rules, use of any information through electronic media that involves personal data of a Person must be made with the consent of the Person concerned."

34 Law Number 11 of 2008 concerning Electronic Technology and Information, Article 26

(2) "Any Person whose rights are infringed as intended by paragraph (1) may lodge a claim for damages incurred under this Law."

Based on the contents of the article above, the use of information technology and protection of personal data is a part of personal rights (privacy rights). Therefore, the alleged misuse of Identity Card and Family Registration Card numbers reflects that there is no guarantee from the security and protection of personal data. Apart from being regulated in the ITE Law, the protection of personal data in electronic systems has also been regulated in the Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, in article 3 and article 6.

Based on the words of Allah in QS. Al-Muthaffifin in the Quran, it is stated:

> *"Woe to the defrauders! Those who take full measure when they buy from people, but give less when they measure or weigh for buyers. Do such people not think that they will be resurrected for a tremendous Day. The Day all people will stand before the Lord of all worlds?"*

This paragraph explains that in trade or business, both traditional and modern, there should be no elements of fraud that can harm any party. The fraudsters here are those who cheat in measuring and weighing.

In a hadith narrated from Abu Hurairah, it is mentioned:

> *"From Abu Hurairah ra, he said," Rasulullah prohibited buying and selling by throwing stones and buying and selling gharar (the price, goods, time and place that are not clear). "*

OJK/Financial Services Authority, as the agency authorized to supervise and regulate *Fintech* services, has also issued OJK regulation number 77/POJK.01/2016 concerning Information Technology-Based Loan Services for the *fintech* service providers. Meanwhile, the prohibition to provide users' data to third parties along with the exemptions is regulated in article 39 and if the entire sanctions for violations of obligations and the prohibitions are violated, the sanctions are specified in article 47.

Article 47 paragraph (1) to (3) do not specify any criminal sanctions related to the violation of the article. OJK only imposes administrative sanctions to the service providers if any violation of the article provisions occurs because the service providers are deemed capable and legally responsible to the storage of the users' personal data by agreeing on the submission of personal data during the verification process to complete the required stage in order to use the services.

The owner of the original data will get into troubles if it turns out that the data to be registered to one of the lending-borrowing service providers is already registered or is already active on a lending-borrowing basis. The verification process that has been conducted by complying with the rules should not cause any problems in these *fintech* activities. A proactive attitude from the service providers is obligatory to ensure the data authentication that will be accepted before validating an account in their service data.

Based on the progressive legal theory, the service provider must comply with the laws and regulations in preventing the misuse of personal data and protection of the users' personal data. If the laws and regulations have not provided a comprehensive legal protection for the owners of the original personal data, the loan service providers and the legal officials must cooperate to produce legal coordination and harmonization in order to create legal products and the implementation of legal protection for the welfare of the community.

Conclusion

Based on the financial technological development, phone numbers, photos, and personal data in any digital forms should also be protected, but the Law Number 24 of 2013 concerning the amendments to the Law Number 23 of 2006 on the population administration, particularly Article 58 paragraph (2), does not state that the data stored in digital forms are categorized as personal data that must be protected. The Regulation of Financial Services Authority Number 77 of 2016 concerning Technology-based Loan Services, particularly Article 26, does not protect personal data since point 5 of Article 26 states that the owner of personal data will be notified if a failure to protect the confidentiality of personal data happens. This article does not provide an explanation of the accountability and the rights of the data owner if there is any failure in protecting the confidentiality of personal data. Article 39 of the Regulation of Financial Services Authority 77/2016 states that *fintech* operators are prohibited from distributing the personal data of the service users to the third parties without any permission given by the data owner. The explanation provided in this article is sufficient to protect the personal data of *fintech* service users. Article 15 of the Law Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions states that those who are responsible for personal data of *fintech* service users are electronic system providers. The protection guidelines are regulated in the Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems.

The users who misuse other people's personal data will be accused of committing criminal act and can be charged according to the provisions of Law number 19 of 2016 concerning ITE for forging the personal data belonging to other people. If these users do not change the data, but misusing the original data for applying for loans through the online loan application, the sanction must be made based on the violation committed. Sanctions can be in the form of criminal and civil sanctions, such as compensations. The original owners whose personal data are used by other people in online loan activities should have the right to legal protection. Thus, the victims must receive restitution as regulated in Article 1 paragraph (5) of the 2008 government regulation number 44.

References

Andini, Gita. *Faktor-Faktor yang Menentukan Keputusan Pemberian Kredit Usaha Mikro Kecil dan Menengah (UMKM) Pada Lembaga Keuangan Mikro Peer to Peer Lending*, Jakarta: Universitas Islam Negeri Syarif Hidayatullah, 2017.

Barger, G.A. *Lost in Cyberspace: Inventors, Computer Piracy and Printed Publications under Section 102 (b) of the Patent Act of 1994 Detroit*, USA : Mercy L. Rev, 1995.

Cita Yustisia Serfiyani, R. Serfianto D. Purnomo dan Iswi Hariyani. *Bisnis Online dan Transaksi Elektronik*. Jakarta: Penerbit PT Gramedia Pustaka Utama,2013.

Departemen Agama Republik Indonesia. *Alquran dan Terjemahnya*. Jakarta: CV Penerbit J-Art, 2004.

Ernama, Budiharto, Hendro S. Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology,Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016, Semarang: *Diponegoro Law Journal*, Vol. 6, No.3, 2017.

Jakarta: Badan Pembinaan Hukum Nasional, 2007.

Maya, Devi, Dwiatmanto. Analisis Pengawasan Kredit Modal Kerja (KMK) Sebagai Upaya Mengantisipasi Terjadinya Kredit Bermasalah (*Jurnal Administrasi Bisnis* (JAB), Studi Pada PT. Bank Tabungan Negara (Persero) Tbk. Vol. 49, No.1, 2017.

Peraturan Kementerian Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi.

Purwanto. Penelitian Tentang Perlindungan Hukum Data Digital.

Rahardjo, Satjipto. Hukum Progresif: Hukum yang Membebaskan. *Jurnal Hukum Progresif, Semarang* : Program Doktor Ilmu Hukum Univ. Diponegoro, Vol. 1/No. 1/April 2005.

Raharjo, Satjipto. *Teori Dasar Ilmu Hukum*. Bandung: PT. Citra Aditya Bakti, 2000.

Ramli, Ahmad Mujahid. C*yber Law dan Haki, Dalam Sistem Hukum Indonesia*. Bandung : PT. Refika Aditama, 2004.

Riduan. *Metode & Teknik Menyusun Tesis*. Bandung: Bina Cipta, 2010.

Riswandi, Budi Agus. *Hukum Dan Internet DI Indonesia*. Yogyakarta : UII Pres, 2003.

Rofiq, Ahmad. *Hukum Islam di Indonesia*. Jakarta: RajaGrafindo Persada. 1998.

Shinta Dewi. *CyberLaw, Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional.* Bandung: Widya Padjajaran, 2009.

Undang-undang Nomor 19 Tahun 2016 Tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.