PROTECTING PERSONAL DATA IN FINANCIAL TECHNOLOGY IN INDONESIA

I Made Mulyawan Subawa

ABSTRACT

Consumers have the obligation to send personal data to access fintech. This condition gave birth to the legal obligation of fintech companies to provide personal data protection. Unfortunately, there are cases where the personal data of consumers is misused by fintech companies, even the personal data is sold to third parties. Indonesia has not yet had a law on personal data protection. Regulations regarding the protection of personal data are still scattered in several statutory and policy regulations. The purpose of this research is to analyze and find out the protection of personal data as a protection of privacy, the potential risk of violation of personal data, and the existence of a law regarding personal data protection. The protection of personal data is the protection of privacy rights, in which the right to privacy is a human right. By law, businesses have a legal obligation to protect personal data of consumers, but this business has the potential to cause violations of personal data both committed by the fintech itself and by the third parties. The provisions for protecting personal data in Indonesia are only regulated in Minister of Communications, Bank Indonesia, and Financial Services Authority (OJK) Regulation. These provisions provide administrative sanctions for businesses that violate the use of personal data. The protection of personal data has not been regulated in the law. Consequently, the protection of personal data has not been carried out optimally.

Keywords: Protection, personal data, financial technology.

INTRODUCTION

Goods and Services Tax (GST) is a consumption tax imposed on the sale of goods and services. In some countries it is also called Value Added Tax (VAT). It is a new tax instrument introduced by the Malaysian government soon, estimated in 2012 would be the soonest year of implementation (Customs Department, 2010). The introduction of GST in Malaysia has called many arguments from various parties including academics, professionals and the nation (would become the taxpayers) on how GST affect goods prices-increase or decrease. The onus of GST is to replace the current Sales Tax and Service Tax in line with the government policy of conforming policies of AFTA.

The internet has been developing so rapidly as a culture of modern society. It is said as a culture because through the internet, various *cyber* community activities such as thinking, creating, and acting can be expressed in it whenever and wherever internet users are located. Its presence has shaped its own world known as cyberspace or the pseudo world, which is a world of computer-based communication that offers a new reality in the form of virtual (indirect and not real).[1] The rapid development of the internet has implications for the financial system. The financial system is basically the order in a country's economy that has a role, especially in providing financial services facilities by financial institutions and other supporting institutions.[2]

Technological advancements have changed the global financial services sector. Various business model innovations are developing rapidly in various parts of the world, including Indonesia..[3] Previously, the financial system was played by conventional banks. Now, banks must compete with the presence of financial technology (fintech). Fintech is a financial service innovation that is the use of technology in the financial services sector.

Fintech is the implementation and use of technology to improve banking and financial services. Fintech is used by startup companies by utilizing the latest software, internet, communication and computing technology. This concept is adapting technological developments combined with the financial sector, so that it can present a more practical, secure and modern financial transaction process. The basic forms of fintech include payments (digital wallets, p2p payments), credit facilities), investments (equity crowdfunding, peer to peer lending), cross-processing (big data analysis, predictive modelling), financing (crowdfunding, micro-loans, insurance (risk management), and infrastructure (security).[4] According to Bank Indonesia Regulation Number 19/12 / PBI / 2017 Regarding Financial Technology Implementation (hereinafter referred to as Bank Indonesia Regulation 2017):

> Financial Technology is the use of technology in the financial system that produces new products, services, technology, and / or business models and can have an impact on stability monetary, financial system stability, and / or efficiency, smoothness, security and reliability of payment systems. Financial Technology is categorized into: (a) payment system, (b) market support, (c) investment and risk management, (d) loans, financing and capital provision, and (e) other financial services.

The development of fintech provides greater and easier access for people to access finance, but it must be recognized that the presence of fintech still poses potential risks. The Fintech's business has at least two potential risks, namely the risk of consumer data security and the risk of errors in the transaction process. The security of personal data is an issue that always accompanies fintech. Billing is not only done to the borrower, but it is also done to all phone contacts stored in the borrower's phone. If the borrower does not make payments on time, then the officer of the online loan application will create a WhatsApp group whose

[1] Agus Rahardjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: PT.Citra Aditya Bakti, 2002), 20.
[2] Djoni S. Gazali, Rachmadi Usman, *Hukum Perbankan* (Jakarta: Sinar Grafika, 2016), 39.
[3] Abubakar, Lastuti, and Tri Handayani. "Financial technology: Legal challenges for Indonesia financial sector." In*IOP Conference Series: Earth and Environmental Science*, 175, no. 1, p. 012204. IOP Publishing, 2018.
[4] Nofie Iman, *Financial Technology dan Lembaga Keuangan* (Yogyakarta: Gathering Mitra Linkage Bank Syariah Mandiri, 2016), 6-7.

contents are the telephone contact list of the borrower. In this group, the officer in the online loan application will distribute the photo of the borrower's *Kartu Tanda Penduduk* (ID card) accompanied by the sentence that the person is borrowing money in this amount.[5] This shouldn't happened. The billing should be sent to the borrower only not everyone in the contacts lists of the borrower.

Fintech marketing is done through websites, social media, SMS, and telephone calls by telemarketer on duty. Telemarketing basically has a good goal which is to present and introduce brands, products, and services to the potential prospects of consumers or buyers clearly and honestly. The high target burden imposed by the company on telemarketers is the reason why telemarketers are trying to get as many consumers as possible. Telemarketing contacts potential customers, even though consumers themselves never provide telephone numbers and allow telemarketer to contact potential customers. This condition has certainly ignored the right of consumers to protect their personal data.

Indonesia has not yet had a law on personal data. The Ministry of Communication and Information states that the draft Revision of the Personal Data Protection Act is still being discussed with the relevant ministries. Provisions regarding the protection of personal data are still regulated separatedly in the law on Information and Electronic Transactions, Financial Services Authority Regulations, Financial Services Authority Circular, and in the Minister of Communication and Information Regulations of the Republic of Indonesia.[6] Related to the protection of personal data, the problem of personal data is not only a legal problem, but also the protection of privacy data. Judges in examining cases must look at various dimensions, including social dimensions. Regarding this phenomenon. Alessandro Mantelero states:

Existing case and regulations are inadequate to address the potential risks and issues related to this change of paradigm in social investigation. This is due to the fact that both the right to privacy and the more recent right to data protection are protected as individual rights. The social dimension of these rights has been taken into account by courts and policymakers in various countries. Nevertheless, the rights holder has always been the data subject and the rights related to informational privacy have mainly been exercised by individuals.[7]

Malaysia already has a law on data protection. Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on June 2, 2010 and came into force on November 15, 2013. The Personal Data Protection Act 2010 has at least regulated personal data protection principles, registration, user forum data and code of practice, rights of data subject, exemption, ppointment, functions and powers of commissioner, personal data protection fund, personal data protection advisory committee, appeal tribunal, inspection, complaint and investigation, enforcement, miscellaneous, savings and transitional provisions. Personal data includes any sensitive personal data or expression of opinion about the data subject. Personal data does not include any information that is processed for the purpose of a business credit reporting agency carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.[8]

Consumers can be the object of business activity to get the maximum profit from business actors. This phenomenon causes the position of consumers is not balanced with business actors, and is in a weak position.[9] Protection of personal data in the fintech business needs to be regulated by appropriate regulations that must be implemented in good faith by the fintech business actors. This research will discuss the protection of personal data as protection of privacy, the potential risk of violation of personal data, and the existence of the law regarding personal data protection.

METODOLOGY

This research is a normative juridical study which examines the legal vacuum in Indonesia which regulates the protection of personal data. Indonesia does not have a personal data law, although several Ministerial regulations and state institutions have been issued. The legal materials used in this study are primary legal materials and secondary legal materials. Primary legal material, namely the Republic of Indonesia Law No. 19 of 2016 concerning Amendments to the Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions, the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 Year 2016 Regarding Protection of Personal Data in Electronic Data Holders , 12 / PBI / 2017 Regarding the Implementation of Financial Technology, and Regulation of the Financial Services Authority Number 77 /POJK.01/2016 Concerning Information Technology Lending and Borrowing Services. Secondary legal materials used are

[5] Ambaranie Nadia Kemala Movanita. "Dugaan Pelanggaran Fintech: Bocorkan Data Pribadi hingga Pelecehan Seksual." Accessed January 3, 2020. https://ekonomi.kompas.com/read/2018/12/10/063800526/dugaan-pelanggaran-fintech-bocorkan-data-pribadi-hingga-pelecehan-seksual.

[6] These provisions include the Republic of Indonesia Law No. 19 of 2016 concerning Amendments to the Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transaction, the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 Year 2016 Regarding Protection of Personal Data in Electronic Data Holders, 12 / PBI / 2017 Regarding the Implementation of Financial Technology, and Regulation of the Financial Services Authority Number 77 /POJK.01/2016 Concerning Information Technology Lending and Borrowing Services.

[7] Alessandro Mantelero, "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection."*Computer law & security review* 32, no. 2 (2016): 238-255.

[8] 'Personal data' means any information in respect of commercial transactions that is:
Being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose
Recorded with the intention that it should wholly or partly be processed by means of such equipment, or
Recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, and, in each case
...that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user.
DLA Piper. "Data Protection Laws of The World; Malaysia." Accessed January 3, 2020.https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=14&ved=2ahUKEwj4lI7NvuvmAhWQbn0KHWVQB3sQFjANegQIBhAC&url=https%3A%2F%2Fwww.dlapiperdataprotection.com%2Fsystem%2Fmodules%2Fza.co.heliosdesign.dla.lotw.data_protection%2Ffunctions%2Fhandbook.pdf%3Fcountry-1%3DMY&usg=AOvVaw0PlhEKRwCP9w4_F9bBM0VA

Indosentius Samsul, *Perlindungan Konsumen, Kemungkinan Penerapan Tanggung Jawab Mutlak* (Jakarta: Universitas Indonesia, 2004), 2.

journals, books and electronic articles that discuss legal issues in this research. Researchers also used The Regulation (EU) 2016/679 (General Data Protection Regulation) and the Malaysian Personal Data Protection Act 2010. Legal material was collected through a literature study. The analysis of this research was carried out qualitatively.

PERSONAL DATA PROTECTION AS PRIVACY PROTECTION

The transformation of the form of society into an information society has implications for the use of information technology in all fields of human life. Advances in information technology have made the public have more room to move. Human activities that were originally national are turned into international. Events that occur in one country within seconds can already be known in other countries.[10] The information technology revolution created increasingly sophisticated information technology tools and information systems networks that were increasingly complex and reliable and were able to meet the demands of all levels of society.[11]

Mastery of information becomes important in the era of globalization. Information is the core of globalization, especially for countries with ambitions to develop and realize change.[12] Gordon B. Davis defines information as 'data that has been processed into a form that is meaningful to the recipient and is used of real or perceived value in current or prospective actions or decisions."[13] Shanon and Weaver state that information is "the amount of uncertainty that is reduced when received. "[14] The characteristics of good information will be determined by the following criterias:

a. Pertinence, i.e. the information must be relevant and can provide added value;
b. Timeliness, i.e. the information must be available when needed;
c. Accuracy, i.e. the information must be accurate in accordance with the context and intensity of its intended use;
d. Reduced uncertainty, i.e. the information must approach absolute certainty;
e. Element of surprise, that information must be something actual.[15]

Mastery of information will be limited in protecting privacy. Acquisition of information must not violate someone's privacy. Warren and Brandheis said that technological development and progress raises a public awareness that there is a person's right to enjoy life. The right to enjoy life is interpreted as a person's right not to be disturbed on his personal life either by someone else, or by the state, therefore the law must recognize and protect that right to privacy.[16] There are a number of reasons why privacy must be protected because in establishing relationships with others, a person must close a portion of his personal life so that he can maintain his position at a certain level Someone in his life needs time to be alone (*solitude*) so privacy is needed by someone. Privacy is a right that stands alone and does not depend on anything else but this right will be lost if the person publishes things that are private to the public. Privacy also includes the right of a person to have domestic relations including how a person builds a marriage, fostering his family and other people may not know the personal relationship.

Protection of privacy is a protection of human rights. Article 12 Universal Declaration of Human Right states "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." In Indonesia, right to privacy is a constitutional right. This right is provided or mentioned in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia which states that "Every person has the right to protection of personal, family, honor, dignity, and property under his authority, and is entitled to a sense of security and protection from the threat of fear of doing or not doing something that is a human right." The Article protects personal or individual right which may also include protection of personal data.

In the use of Information Technology, protecting personal data is one part of personal rights (privacy rights). Personal rights in the Elucidation of Article 26 of Law Number 19 of 2016 2016 concerning Amendments to the Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions contains the following meanings:

a. Personal rights are the right to enjoy personal life and are free from all kinds of disturbances.

b. Personal rights are the right to be able to communicate with others without spying.

c. Personal rights are the right to supervise access to information about one's personal life and data.

Edmon Makarim summarizes three aspects of *privacy*, namely privacy of a person, privacy of data about a person, and privacy of person's communications. The three aspects of privacy can be detailed as follows:

1. Privacy of a person

This right to privacy is based on the general principle that everyone has the right to be let alone. In general, there are four types of violations of personal privacy, namely:

[10] Dikdik M. Arief Mansur dan Elisatris Gultom, C*yber Law: Aspek Hukum Teknologi Informasi* (Bandung: Refika Aditama, 2005), 29.
[11] Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta: PT RajaGrafindo Persada, 2004), 27
[12] Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Bandung: Refika Aditama, 2005), 5.
[13] Davis Gordon B and Margareth Olson, *Management Information System: Conceptual Foundations, Structure and Development* (New York: McGraw-Hill, 1987), 5.
[14] David Kroenke, *Management Information System, International Edition California* (Singapore: Mitchell McGraw-Hill, 1993), 3.
[15]Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta: Raja Grafindo Persada, 2003). 31-32.
[16] Shinta Dewi, *CyberLaw: Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional* (Bandung: Widya Padjajaran, 2009), 10.

- Publications that place someone in the wrong place. For example, by using a photo of a woman as an illustration of an article about a mother who abandoned her child.
- Incorrect use of a person's name or preference for commercial purposes.
- Disclosure of embarrassing personal facts to the public.
- Disturbs someone's solitude.

2. Privacy of data about a person

Privacy rights can also bind to information about someone that is collected and used by others. This includes, for example, information about a person's habits, medical records, religion and membership in political parties, tax records, employee data, insurance records, criminal records and so on. Misuse of information collected on members of an organization / institution or on customers of a company is included in violations of one's privacy rights.

3. Privacy of person's communications

In certain situations, the right to privacy may also include online communication. In certain cases, monitoring and disclosure of the contents of electronic communications by others not by the sender or the person sent can be a violation of someone's privacy.[17]

The Regulation (EU) 2016/679 (General Data Protection Regulation) defines 'personal data' as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The General Data Protection Regulation further describes the Principles relating to processing of personal data, as follows:

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods of information as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

Financial Services Authority Circular Letter Number 18 / SEOJK.02/2017 regarding Information Technology Risk Management and Management in Information Technology Based Lending and Borrowing Services, states that "Providers are prohibited from sharing data and personal information about users to other parties. Personal data and information include at least:

<table>
<tr><td colspan="5">Types of personal data</td></tr>
<tr><td colspan="2">Data and information that is inherent and identifiable:</td><td>Material non-public</td><td>Data and information Data and information related to financial transactions; and</td><td>Data and information related to contracts / agreements.</td></tr>
<tr><td>Individual</td><td>Corporate:</td><td></td><td></td><td></td></tr>
<tr><td>a. name;
b. Residence address;</td><td>a. corporation name;
b. address;
c. phone number;
d. composition of directors and</td><td>a. financial statements;
b. business performance;
c. Management decision;</td><td></td><td></td></tr>
</table>

[17] Edmon Makarim II, *Op.Cit.*, 146-147.

c. identity card (KTP, SIM, Passport); d. Taxpayer Identification Number (NPWP); e. date of birth and / or age; f. email address; g. IP address; h. phone number; i. account number; j. biological mother's name; k. credit card number; l. digital identity (Biometrics); m. signature; n. educational background; o. Job Experiences; p. current account; q. register of assets; r. data and other related information;	commissioners including documents e. identity in the form of identity card / Passport / residence permit; f. board of director; g. account number; h. current account; i. asset register; j. company document; k. data and other related information;	d. number of customers; e. data and other related information;		

POTENTIAL RISK OF PERSONAL DATA VIOLATION

The use of personal data in fintech is necessary to enter into a loan agreement between the borrower and the lender, and between the organizer and the lender. Personal data in this case is related to the identity of the parties. Of course, data may not necessarily be accepted. There needs to be verification in advance of the parties concerned. This verification is intended to prevent misuse of personal data.[18] In fintech, organisers and users do not meet directly or face to face. Therefore, the truth of personal data and access to personal data is the only guarantee for fintech to know the personality of prospective consumers, especially for the delivery of electronic loans and loan services in providing credit analysis.

Fintech has a legal obligation to maintain the confidentiality, integrity and availability of personal data, transaction data, and financial data that it manages from the time the data is obtained until the data is destroyed. Utilization of user data and information obtained by fintech companies must obtain approval from users. Fintech is obliged to convey restrictions on the use of data and information to users, convey any changes in the purpose of using data and information to users in the event that there is a change in the purpose of using data and information, media and methods used in obtaining data and information guaranteed confidentiality, security, and integrity as outlined on electronic contracts.[19]

Personal data in the fintech business is indeed vulnerable to various risks. Misuse of personal data is a risk in protecting personal data. Fintech has a legal obligation to maintain the confidentiality of personal data, prevent employees from committing personal data breaches, and maintain the security of personal data from cyber-attacks. Regarding this matter, Anugerah, Dian Purnama, and Masitoh Indriani analyze the potential risks to personal data as follows:

The risk on how the data should be treated can be seen that the centralized authority, in this regards is a Fintech services provider, in several steps as collecting, processing and analyzing. Even though the technology used in Fintech such as Blockchain technology is able to encrypt some actions on the web, there is still a potential threat in cyberspace. The cyber risk and cyber security is the main issue concerning consumer's data protection; cyber-attacks can be the potential threat of a system or data confidentiality, integrity and availability. Moreover, those potential cyber-attacks are becoming more frequent and more costly for more broadly societies. And this financial sector is one of the prime targets of cyber-attacks because it represents where the money is or be a symbol of capitalism that leads to cyber-attacks that might have some politically motivation.[20]

[18] Dimas Hutomo. "Perlindungan Data Pribadi dalam Penyelenggaraan Fintech." Accessed January 3, 2020. https://www.hukumonline.com/klinik/detail/lt5c498fb94dc87/perlindungan-data-pribadi-dalam-penyelenggaraan-fintech/

[19] Kornelius Benuf, Siti Mahmudah, and Ery Agus Priyono. "Perlindungan hukum terhadap keamanan data konsumen financial technology di Indonesia."*Refleksi Hukum: Jurnal Ilmu Hukum*3.2 (2019): 145-160.

[20] Anugerah, Dian Purnama, and Masitoh Indriani. "Data Protection in Financial Technology Services: Indonesian Legal Perspective." In*IOP Conference Series: Earth and Environmental Science*, vol. 175, no. 1, p. 012188. IOP Publishing, 2018.

Misuse of personal data certainly harms consumers who use fintech services. Victims are consumers of fintech service users whose personal data are violated. The loss suffered is difficult to assess in which the loss is felt far greater than the physical loss, because it has disrupted his personal life so that if there is a loss suffered, the victim have a right to receive compensation.[21] Damage to one's reputation because of the spread of personal data is certainly difficult to be valued in money. This loss lasts for a long period.

THE PRESENT LEGAL POLICIES AND REGULATIONS ON PERSONAL DATA PROTECTION

The development of the fintech industry is increasing. Various financial services provided to consumers only by using applications on phones that are connected to the internet. The issue of consumer protection is one part that is closely related to fintech, especially since the industry began to develop in Indonesia in the last five years. In the financial services sector, regulation of fintech consumer personal data is still not too strict compared to other industries such as banking, insurance and capital markets. Seeing this condition, it is necessary to have rules in the form of a law as a legal basis for protecting the personal data of the public.[22]
Data protection is a phrase that is quite difficult to define. This term implies that data requires a comprehensive protection mechanism.[23] The mechanism is set forth in policies aimed at protecting personal data. Government policy in the field of telematics has three objectives, namely:

a. Achieving economic growth and competitiveness (economic growth and competitiveness)
b. Achieving an increase in the quality of life of the people; and
c. Achievement of national defense and defense stability.[24]

Regulations regarding the protection of personal data in Indonesia have not yet been regulated in specific laws, but rather regulated in technical policies. The technical policy was issued by ministries and state institutions, such as the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 Year 2016 Regarding Protection of Personal Data in Electronic Data Holders, 12 / PBI / 2017 Regarding the Implementation of Financial Technology, and Regulation of the Financial Services Authority Number 77 /POJK.01/2016 Concerning Information Technology Lending and Borrowing Services.

Article 1 number 1 of the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in the Electronic System (hereinafter referred to as the Ministerial Regulation 2016) states "Personal Data is certain personal data that is stored, maintained, and kept truthful and protected by confidentiality." In providing personal data protection, Article 21 of the 2016 Ministerial Regulation stipulates that the act of displaying, announcing, sending, distributing, and / or opening access to Personal Data in the Electronic System can only be carried out with the Agreement unless otherwise stipulated by statutory provisions; and after verification of the accuracy and suitability of the purpose for the acquisition and collection of the Personal Data. Related to the protection of personal data, Article 26 of the 2016 Ministerial Regulation states that the Data Owner is entitled to:

a. the confidentiality of his Personal Data;
b. file a complaint in the context of resolving Personal Data disputes over the failure of protecting the confidentiality of his Personal Data by the Electronic System Provider to the Minister;
c. get access or opportunity to change or update his Personal Data without disrupting the management system of Personal Data, unless otherwise specified by statutory provisions;
d. get access or opportunity to obtain historical Personal Data that has been submitted to the Electronic System Provider as long as it is still in accordance with the provisions of the legislation; and
e. request the destruction of his Specific Individual Data in the Electronic System which is managed by the Electronic System Provider, unless otherwise stipulated by statutory provisions.

Owners of personal data are individuals who are attached to certain personal data. Electronic system users, hereinafter referred to as users, are any person, state administrator, business entity, and community who use goods, services, facilities, or information provided by the electronic system operator. Protection of personal data in an electronic system is carried out in the process of acquisition and collection; processing and analyzing; storage; appearance, announcement, delivery, distribution and / or opening of access; and extermination. The Ministerial Regulation 2016 regulates the legal obligations for users to protect personal data. Users as referred to in the Ministerial Regulation 2016 are all people, state administrators, business entities, and the public who use goods, services, facilities, or information provided by electronic system providers. Article 27 of the 2016 Ministerial Regulation states, Users must:

a. maintain the confidentiality of Personal Data obtained, collected, processed and analyzed;
b. use Personal Data in accordance with User needs only;
c. protect Personal Data and documents containing Personal Data from misuse; and
d. be responsible for the Personal Data contained in his control, both the organizational control of his authority and individuals, if there is an act of abuse.

[21] Shinta Dewi, *Op.Cit.*, 11.
[22] Mochamad Januar Rizki. "Perlindungan Data Konsumen Harus Jadi Prioritas Industri Fintech." Accessed January 3, 2020. https://www.hukumonline.com/berita/baca/lt5d887b1ba7f91/perlindungan-data-konsumen-harus-jadi-prioritas-industri-fintech/
[23] Schaar, Peter. "Data protection empowerment." In *Cyber Security. Simply. Make it Happen.*, pp. 21-26. Springer, Cham, 2017.

[24] Dikdik M. Arief Mansur dan Elisatris Gultom. *Cyber Law: Aspek Hukum Teknologi Informasi*, (Bandung: Refika Aditama, 2005), 126.

Article 36 Ministerial Regulation 2016 regulates administrative sanctions for unlawful use of personal data. Every person who obtains, collects, processes, analyzes, stores, displays, announces, sends, and / or disseminates Personal Data without rights or does not comply with the provisions in this Ministerial Regulation or other laws and regulations is subjected to administrative sanctions in accordance with statutory provisions regulations in the form of:

1. verbal warnings;
2. written warning;
3. temporary suspension of activities; and / or announcements on online sites (online websites).

Bank Indonesia Regulation 2017 is issued with the consideration that the development of technology and information systems continues to produce various innovations related to financial technology. The development of financial technology brings benefits, but on the other hand has the potential risk. The potential risks referred to include the existence of regulations that have not yet reached the development of fintech, theft and misuse of personal data, and protection of personal data from cyber-attacks. The financial technology ecosystem needs to be continuously monitored and developed to support the creation of monetary stability, financial system stability, and payment systems that are efficient, smooth, safe, and reliable to support sustainable and inclusive national economic growth. The implementation of financial technology must apply the principles of consumer protection and risk management and prudence. Bank Indonesia's policy response to the development of financial technology must remain synchronous, harmonious, and integrated with other policies issued by Bank Indonesia.

Protection of personal data is also regulated in the 2017 Bank Indonesia Regulation. Article 8 of the 2017 Bank Indonesia Regulation states:

(1) Providers of Financial Technology that have been registered with Bank Indonesia must:

1. apply consumer protection principles in accordance with products, services, technology, and / or business models that are run;
2. maintain the confidentiality of consumer data and / or information including transaction data and / or information;
3. applying the principles of risk management and prudence;
4. use rupiah in every transaction made in the territory of the Unitary Republic of Indonesia in accordance with the provisions of the legislation governing currency;
5. apply the principle of anti money laundering and prevention of terrorism financing in accordance with the provisions of the legislation governing anti money laundering and prevention of financing of terrorism; and
6. fulfill the provisions of other laws and regulations.
7.

(2) In addition to the obligations referred to in paragraph (1), Providers of Financial Technology are prohibited from conducting payment system activities using virtual currency.

Article 20 paragraph (2) of the 2017 Bank Indonesia Regulation states that the Provider of Financial Technology violating the provisions referred to in Article 8 paragraph (1), Article 8 paragraph (2), Article 8 paragraph (3), Article 12 paragraph (3), Article 12 paragraph (4) and / or Article 16 paragraph (2) shall be liable to administrative sanctions in the form of a written warning; and / or deletion from the list of Financial Technology Providers at Bank Indonesia.

The government established an oversight body in the financial services sector in Indonesia, the Financial Services Authority (*Otoritas Jasa Keuangan*) . The Financial Services Authority is an institution that is independent and free from interference from other parties, which has the functions, duties and authority to regulate, supervise, examine and investigate. The Financial Services Authority was formed with the aim that all financial service activities within the financial services sector can be carried out in an orderly, fair, transparent and accountable manner, and be able to realize a financial system that grows in a sustainable and stable manner, and be able to protect the interests of consumers and society.[25]

In protecting the interests of consumers in the financial services sector, the Financial Services Authority issued a regulation namely Regulation of the Financial Services Authority Number: 1 / POJK.07 / 2013 Concerning Consumer Protection in the Financial Services Sector (hereinafter referred to as the Financial Services Authority Regulation 2013) and Financial Services Authority Regulation Number 77 /POJK.01/2016 About Information Technology-Based Lending and Borrowing Services (hereinafter referred to as the 2016 Financial Services Authority Regulation).

Consumers according to the 2013 Financial Services Authority Regulations are parties who place their funds and / or utilize services available at Financial Services Institutions including customers in Banks, investors in the Capital Market, policyholders in insurance, and participants in Pension Funds, based on legislation regulations in the financial services sector. According to Article 2 of the 2013 Financial Services Authority Regulation, Consumer Protection applies the principle of transparency; fair treatment; reliability; confidentiality and security of Consumer data / information; and handling complaints and resolving Consumer disputes in a simple, fast, and affordable manner. Regarding the protection of personal data, Article 31 of the 2013 Financial Services Authority Regulation stipulates the following:

(1) Financial Service Providers are prohibited in any way from providing data and / or information about their Customers to the third parties.

[25] See General Explanation of the Law of the Republic of Indonesia Number 21 of 2011 concerning the Financial Services Authority.

(2) Prohibition as referred to in paragraph (1) is excluded in terms of:
a. The consumer gives written approval; and / or
b. Required by statutory regulations.

(3) In the event that a Financial Services Business Actor obtains personal data and / or information of a person and / or group of people from other parties and the Financial Services Business Actor will use the data and / or information to carry out its activities, the Financial Services Business Actors must have a written statement that the other party concerned has obtained written approval from a person and / or group of such people to provide the personal data and / or information to any party, including Financial Services Business Actors.

(4) The cancellation or amendment of part of the agreement on the disclosure of data and or information as referred to in paragraph (2) letter a is made in the written form of statement by the consumer.

Regulations issued by the Financial Services Authority only contain administrative sanctions for business actors who violate the provisions of personal data protection. These provisions are contained in Article 53 of the 2013 Financial Services Authority Regulation which states as follows:

(1) Financial Service Business Actors and / or parties who violate the provisions of this Financial Services Authority Regulation are subject to administrative sanctions, including but not limited to:

a. Written warning;
b. Fines that are obligations to pay a certain amount of money;
c. Limitation of business activities;
d. Suspension of business; and
e. Revocation of business activity permit.

(2) Sanctions as referred to in paragraph (1) letter b, letter c, letter d, or letter e may be imposed with or without prior imposition of written warning sanctions as referred to in paragraph (1) letter a.
(3) Penal sanctions as referred to in paragraph (1) letter b may be imposed separately or jointly with the imposition of sanctions as referred to in paragraph (1) letter c, letter d, or letter e.
(4) The amount of financial sanctions as referred to in paragraph (1) letter b shall be determined by the Financial Services Authority based on the provisions on administrative sanctions in the form of fines that apply to each financial service sector.
(5) The Financial Services Authority can announce the imposition of administrative sanctions as referred to in paragraph (1) to the public.

The implementation of fintech business in the field of online loan providers is bound by the provisions of the 2016 Financial Services Authority Regulation. Article 1 paragraph (3) of the 2016 Financial Services Authority Regulation states Information Technology Based Money Lending and Borrowing Services is the organization of financial services to bring together lenders and loan recipients in the framework of entering into loan and loan agreements in rupiah directly through the electronic system using the internet network.

The regulation regarding personal data protection in information technology based lending and borrowing services are regulated in Article 26 of the 2016 Financial Services Authority Regulation. The provision regulation that the Operator is required:

a. maintain the confidentiality, integrity, and availability of personal data, transaction data, and financial data that it manages since the data was obtained until the data is destroyed;
b. ensure the availability of authentication, verification, and validation processes that support the discrepancy in accessing, processing and executing personal, transaction, and financial data that it manages;
c. guarantee that the acquisition, use, utilization and disclosure of personal, transaction, and financial data obtained by the Operator is based on the agreement of the owner of personal, transaction, and financial data, unless otherwise stipulated by statutory provisions;
d. provide other communication media in addition to the Information Technology-Based Lending and Borrowing Services Electronic Money System to ensure the continuity of customer services that can be in the form of electronic mail, call centers, or other communication media; and
f. Notify the owner of personal, transaction, and financial data in written way if there is a failure in protecting the confidentiality of personal, transaction, and financial data under management.

In protecting personal data from consumers, service providers must provide a security system. Article 28 of the Financial Services Authority Regulation 2016 states as follows:

(1) Providers are required to safeguard information technology system components by owning and carrying out procedures and facilities for securing Information Technology Based Money Lending and Borrowing Services in order to avoid disruption, failure and loss.
(2) The Operator is obliged to provide a security system that includes procedures, prevention systems, and countermeasures for threats and attacks that cause interference, failure, and loss.
(3) Providers must participate in managing information technology security loopholes in supporting information security in the information technology-based financial services industry.
(4) Providers are required to re-display Electronic Documents fully in accordance with the format and retention period determined in accordance with statutory provisions.

Article 39 of the 2016 Financial Services Authority Regulation stipulates that administrators are prohibited in any way from providing data and / or information about Users to the third parties. Prohibitions are excluded in the event that the user gives consent electronically; and / or required by statutory provisions. Cancellation or amendment of part of the agreement on the disclosure of data and / or information is done electronically by the User in the form of Electronic Documents. The 2016 Financial Services Authority Regulation provides a legal umbrella for consumer protection against personal data violations in the form of administrative sanctions. Article 47 of the 2016 Financial Services Authority Regulation determines the following:

(1) For violating obligations and prohibitions in this OJK regulation, OJK is authorized to impose administrative sanctions on the Operator in the form of:
   a. written warning;
   b. fines, namely the obligation to pay a certain amount of money;
   c. restrictions on business activities; and
   d. revocation of permission.
(2) Administrative sanctions as referred to in paragraph (1) letter b through letter d, may be imposed with or without prior imposition of administrative sanctions in the form of written warnings as referred to in paragraph (1) letter a.
(3) Administrative sanctions in the form of fines as referred to in paragraph (1) letter b may be imposed separately or jointly with the imposition of administrative sanctions as referred to in paragraph (1) letter c and letter d.

The presence of information technology based lending and borrowing services make Indonesian consumers do have many choices about products and services in accordance with their wants, needs, and purchasing power. But on the other hand, for consumers who are less critical, it will still have the potential that results in losses due to the use of goods and / or services.[26] Article 37 of the 2016 Service Authority Regulation states "Providers are responsible for User losses arising from errors and / or negligence of the Directors, and / or Operator employees." Article 38 further states "Operators are required to have standard operating procedures in serving Users contained in Electronic Documents."

Indonesia basically does not have specific laws regarding personal data. Provisions regarding the protection of personal data are only contained in one article in the Republic of Indonesia Law No. 19 of 2016 concerning Amendments to the Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions. In fact, the law on the protection of personal data should be the legal umbrella of various technical policies regarding the protection of personal data. Article 26 of the Republic of Indonesia Law No. 19 of 2016 concerning Amendments to the Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions states:

(1) Unless otherwise stipulated by legislation, the use of any information through electronic media that involves a person's personal data must be done with the approval of the person concerned.
(2) Any person whose rights have been violated as referred to in paragraph (1) may file a claim for damages incurred under this Law.

Breaches of personal data by Fintech as a business actors are categorized as unlawful acts/ tort. The legal basis for the claim for compensation is regulated in Article 1365 of the Civil Code which states that "Any act that violates the law, which brings harm to another person, obliges the person who is because of his mistake to issue the loss, compensates for the loss."
Article 32 of the Republic of Indonesia Law No. 11/2008 concerning Electronic Information and Transactions (hereinafter referred to as the Electronic Information and Transaction Act 2008) regulates criminal provisions for violations of personal data. Article 32 states as follows:

(1) Every person intentionally and without rights or against the law in any way alters, adds, subtracts, transmits, damages, removes, transfers, hides an Electronic Information and / or Electronic Documents belonging to another person or public property.
(2) Every person intentionally and without rights or against the law in any way transfers Electronic Information and / or Electronic Documents to the Electronic System of other unauthorized persons.
(3) Regarding acts as referred to in paragraph (1) which results in the disclosure of confidential Electronic Information and / or Electronic Documents that can be accessed by the public with inappropriate data integrity.

Provisions in Article 32 of the Law of the Republic of Indonesia Number 11 Year 2008 regarding Information and Electronic Transactions provide a clear description that telephone numbers may not be given to anyone without permission from the owner of the telephone number. However, this practice is still ongoing and there is no law enforcement for violations.[27] Consumers who want to access fintech, must provide approval for fintech to access personal data on the cellular phone used. If approval is not given, the application will stop, so that inevitably, the consumer must give consent. Permits granted by consumers can be said to be "forced", which if not done, then consumers can not take advantage of the fintech application. The prohibition of exceptions that allow access to personal data is a loophole for businesses to obtain consumer personal data and provide it to third parties.

CONCLUSION

Protection of personal data is protection of privacy rights. The development of the fintech business has the potential to pose risks to the violation of consumer personal data. Consumer personal data has the potential to be used unlawfully that could cause damage

[26] Zulham, *Hukum Perlindungan Konsumen* (Jakarta: Kencana, 2013), 3.
[27] Buana, A. P., Ma'ruf, T. A., & Aswari, A. (2019). Harmonisasi Peraturan Perundang-undangan Terhadap Bentuk Perjanjian Melalui Telemarketing. *Pleno Jure*, *9*(2), 47-59.

to someone's reputation, or be given to the third parties through agreements that are "forced" to be done by the consumers. Indonesia has not yet had a specific law on personal data protection. The regulation of personal data is disaggregated into statutory regulations in juridical technical policies such as the Minister of Communications Regulation, Bank Indonesia Regulation and Financial Services Authority Regulations. This condition causes a phenomenon in which personal data is not optimally protected. Formulations regarding the protection of personal data in the future are formulated into the Personal Data Protection Act.

REFERENCES

Abubakar, L., and Tri Handayani. "Financial technology: Legal challenges for Indonesia financial sector." In*IOP Conference Series: Earth and Environmental Science*, 175, no. 1, p. 012204. IOP Publishing, 2018.

Anugerah, Dian Purnama, and Masitoh Indriani. "Data Protection in Financial Technology Services: Indonesian Legal Perspective." In*IOP Conference Series: Earth and Environmental Science*, vol. 175, no. 1, p. 012188. IOP Publishing, 2018.

Benuf, K., Siti Mahmudah, and Ery Agus Priyono. "Perlindungan hukum terhadap keamanan data konsumen financial technology di Indonesia."*Refleksi Hukum: Jurnal Ilmu Hukum*3.2 (2019): 145-160.

Buana, A. P., Ma'ruf, T. A., & Aswari, A. (2019). Harmonisasi Peraturan Perundang-undangan Terhadap Bentuk Perjanjian Melalui Telemarketing. *Pleno Jure*, *9*(2), 47-59.

Dewi, S., *CyberLaw: Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional* (Bandung: Widya Padjajaran, 2009), 10.

Gazali, Djoni S. Rachmadi Usman, *Hukum Perbankan* (Jakarta: Sinar Grafika, 2016), 39.

Gordon B., D. and Margareth Olson, *Management Information System: Conceptual Foundations, Structure and Development* (New York: McGraw-Hill, 1987), 5.

Hutomo, D. "Perlindungan Data Pribadi dalam Penyelenggaraan Fintech." Accessed January 3, 2020. https://www.hukumonline.com/klinik/detail/lt5c498fb94dc87/perlindungan-data-pribadi-dalam-penyelenggaraan-fintech/

Iman, N*Financial Technology dan Lembaga Keuangan* (Yogyakarta: Gathering Mitra Linkage Bank Syariah Mandiri, 2016), 6-7.

Kroenke, D., *Management Information System, International Edition California* (Singapore: Mitchell McGraw-Hill, 1993), 3.

Makarim, E., *Kompilasi Hukum Telematika* (Jakarta: PT RajaGrafindo Persada, 2004), 27

Makarim, E., *Kompilasi Hukum Telematika* (Jakarta: Raja Grafindo Persada, 2003). 31-32.

Mansur, D.M.A. & Elisatris Gultom. *Cyber Law: Aspek Hukum Teknologi Informasi*, (Bandung: Refika Aditama, 2005), 126.

Mantelero, A., "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection."*Computer law & security review* 32, no. 2 (2016): 238-255.

Movanita, A.N.K., "Dugaan Pelanggaran Fintech: Bocorkan Data Pribadi hingga Pelecehan Seksual." Accessed January 3, 2020. https://ekonomi.kompas.com/read/2018/12/10/063800526/dugaan-pelanggaran-fintech-bocorkan-data-pribadi-hingga-pelecehan-seksual.

Piper. "Data Protection Laws of The World; Malaysia." Accessed January 3, 2020. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=14&ved=2ahUKEwj4lI7NvuvmAhWQbn0KHWVQB3sQFjANegQIBhAC&url=https%3A%2F%2Fwww.dlapiperdataprotection.com%2Fsystem%2Fmodules%2Fza.co.heliosdesign.dla.lotw.data_protection%2Ffunctions%2Fhandbook.pdf%3Fcountry-1%3DMY&usg=AOvVaw0PlhEKRwCP9w4_F9bBM0VA

Rahardjo, A. *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: PT.Citra Aditya Bakti, 2002).

Rizki, M.J., "Perlindungan Data Konsumen Harus Jadi Prioritas Industri Fintech." Accessed January 3, 2020. https://www.hukumonline.com/berita/baca/lt5d887b1ba7f91/perlindungan-data-konsumen-harus-jadi-prioritas-industri-fintech/

Samsul, I., *Perlindungan Konsumen, Kemungkinan Penerapan Tanggung Jawab Mutlak* (Jakarta: Universitas Indonesia, 2004), 2.

Schaar, P., "Data protection empowerment." In *Cyber Security. Simply. Make it Happen.*, pp. 21-26. Springer, Cham, 2017.

Wahib, A. & Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Bandung: Refika Aditama, 2005), 5.

Zulham, *Hukum Perlindungan Konsumen* (Jakarta: Kencana, 2013), 3.

I Made Mulyawan Subawa
PhD of Law
Udayana University, Denpasar, Bali, Indonesia
Email: mulyawansubawa@gmail.com