Advances in Economics, Business and Management Research, volume 130
3rd International Conference on Law and Governance (ICLAVE 2019)

The Urgency of Establishing Personal Data Protection Act and Financial Technology Act in Digital Era in order to Protect and Control the Privacy in Indonesia

Ira Apriyanti[1*]

[1]*Faculty of Law, Universitas Indonesia, Depok, Jawa Barat 16424, Indonesia*
[*]*Corresponding author. Email: ira.apriyanti23@gmail.com*

ABSTRACT
Expeditious of technological developments are now hand in hand with the problems that occur, especially relating to personal data, a prodigious remarkable asset. Recently, a problem that is humid in the digital era is regarding Fintech which attacks personal data that causing a lot of harm. Also at this time, Indonesia does not yet have firm and well-established rules to regulate personal data protection. In fact, the Constitution of the Republic of Indonesia contains respect for human rights values to privacy and personal data. On Article 28 G of the 1945 Constitution of the Republic of Indonesia which regulates the right to protection of personal, family, honor, dignity, and property under his authority. In addition, many other countries have regulated data protection law and Fintech. Hence this research aims to provide some views and recommendation for the government to immediately make and ratify the Personal Data Protection Act and the Financial Technology Act to ensure the protection of civilians data. This study will use a juridical normative-empirical method that uses secondary legal materials such as literature studies and regulation.
Keywords: *privacy, data protection, legal basis, Financial Technology, regulation*

1. INTRODUCTION

In the era of the industrial revolution 4.0, digital innovations and technology-enabled business model innovations are developing very rapidly. This is supported by the potential of Indonesia's large digital economy and continues to rapidly increase. Based on data released by the Indonesian Internet Service Providers Association (APJII) mention that in 2019, the number of internet users in Indonesia is growing by 10.12% per year and internet users are in the range of 52%, most of them accessing the internet on mobile for 4 hours per day. (APJII, 2019). Everything that supports human daily life is now integrated through digital technology, ranging from consumption, transportation, entertainment, education, shopping, banking, even to being able to get credit loans through the Fintech application. Fintech growth has continued to accelerate in the last three years. Data presented by the Otoritas Jasa Keuangan (OJK) shows that in 2017, the realization of Fintech loans ranged from 2.256 trillion rupiah. But in the following year, the realization of loans increased sharply to touch 786% to 22.67 trillion rupiah. In 2019, funding provided through Fintech could double from the previous year to reach 40 trillion rupiah. It is estimated that this phenomenon will continue to increase every year along with the rapid innovation in the world of digital innovations. (OJK, 2019).

Fintech growth has continued to accelerate in the last three years. Data presented by the Otoritas Jasa Keuangan (OJK) shows that in 2017, the realization of Fintech loans ranged from 2.256 trillion rupiah. But in the following year, the realization of loans increased sharply to touch 786% to 22.67 trillion rupiah. In 2019, funding provided through Fintech could double from the previous year to reach 40 trillion rupiah. It is estimated that this phenomenon will continue to increase every year along with the rapid innovation in the world of digital innovations. (OJK, 2019).

Fintech lending comes with many features and convenience in getting loan funds. Fintech can be accessed through an online application that everyone can download for free. The lending process is very easy and fast. The data is filled in through the application to complete and within a few hours, the loan funds will be immediately disbursed. The process of disbursing loan funds which takes a maximum of 2-3 days causes Fintech to be able to answer the problems that exist in the community in providing loan funds. Unlike the case with loans from banks or Unsecured Loans (KTA), the process includes 1) meetings between creditors and debtors; 2) survey of debtor's ability to pay debts; 3) the process of disbursing funds is quite long. This is undoubtedly

one of the factors causing Fintech to continue to grow every year. With the offer of ease of borrowing and the fast disbursement process, many people have taken this path without regard to the consequences borne in the future. The ease and speed of obtaining money is one factor why online lending or peer-to-peer (P2P) lending services are increasingly developing in Indonesia.

But behind the brilliance of the development of the digital money lending industry, there are many problems that occur in the Fintech industry today. These problems include 1) protection of customers' personal data; 2) high loan interest; 3) the maturity period is short; 4) billing procedures carried out by the Fintech application to the customer when the loan is due. When the borrower is unable to pay the due date, the company of the application will bill through the debt collector or 'Debt Collector' by terrorizing obscene words through short messages on cell phones and social media. In fact, this debt collector does not only terrorize the borrower's cell phone numbers that are heavily in debt but also addresses the cell phone numbers of his relatives so that many of the borrowers feel humiliated and feel insecure. Even sadder, this billing caused casualties. A taxi driver committed suicide because he was unable to bear the weight of the debt burden through the Fintech application he used. Through a will, he advised the government to eradicate the Fintech application which he dubbed as a demon trap. This raises the urgency, especially regarding the protection of users' personal data from being misused.

Privacy on personal data issues in Indonesia has recently emerged and become an increasing concern due to the way the government and private companies collect and process privacy on personal data. The problems that arise in Indonesia comprise among others: 1) the emergence of complaints raised by either individuals or groups or organizations against violations of personal information regarding disruption of the privacy on personal data through both print and electronic media; 2) the emergence of complaints from the public because their identity and privacy on personal data are not properly kept, for example in the banking industry, financial industry, or more specifically in the credit card industry, where customer's privacy on personal data can be accessed, disseminated, and shared between banks and their agencies without the knowledge of the customer. Similarly with other privacy on personal data, causing great concern in Indonesia relates to e-identity card programs where the government compiles privacy on personal data. Thus, problems that often occur in this era must be immediately followed up with the presence of the Personal Data Protection Act and the Financial Technology Act to answer any problems that occur in this digital age.

2. LEGAL MATERIAL AND METHODS

This research uses the juridical normative-empirical method to explain the legal framework in the protection of personal data in the Fintech application by linking the problems that occur in lending funds in Peer to Peer Lending with the regulations regarding the protection of current personal data of customers. Comparison with other states that already have regulations regarding the protection of personal data and conducted to hand over suggestions for law on the protection of personal data in Indonesia. Various legal materials ranging from secondary legal materials are used. Such legal materials include the following legal instruments as well as other journal articles relevant to the topic:

a. POJK No. 77/POJK.01/2016
b. POJK No. 13/POJK.02/2018
c. POJK No. 37/POJK.04/2018
d. Bank Indonesia Regulation No. 19/12/PBI/2017
e. General Data Protection Regulation (GDPR) of European Union (EU)
f. The Personal Data Protection Act 2010 (PDPA) in Malaysia
g. The Information Technology (Amendment) Act 2008 in India

3. DISCUSSION AND RESULTS

3.1 Illegal Fintech Set of Problems

The Otoritas Jasa Keuangan (OJK) have closed 133 illegal peer-to-peer lending Fintech entities in October 2019. The total number of entities handled by the Investment Alert Task Force has reached 1,477 entities since 2018. Of these, there are private pawn services total are 52 entities, illegal investment offering activities total are 27 entities, 11 illegal forex trading, 8 illegal cryptocurrency investments, 2 illegal Multi-Level Marketing (MLM), 1 illegal Umrah travel, 5 other illegal investments, and the rest holding the most entities are illegal Fintech. This closure was carried out by the Otoritas Jasa Keuangan (OJK) to protect online loan service users against problematic illegal Fintech. The reason is, this illegal Fintech often misuse user data if the customer does not pay the loan until the specified number of maturities. Debt collectors from illegal Fintech use several methods of billing such as 1) threatening with verbal violence; 2) threatening to send a Debt Collector to the customer's home; 3) contact everyone in the customer's contact, collect and then embarrass the customer; 4) disseminating data and customer information through social media and contacts in the contact list and WhatsApp; 5) sending messages by spreading slander to all contacts on the contact list as if running away company money; 6) short maturity period; 7) large flowers; 8) high potential administration costs; 9) have a daily fine if the customer does not pay off the debt when it is due.

Various kinds of violations were carried out in this illegal Fintech billing activity, ranging from pressure to sexual harassment. Armed with customers' personal data, the Fintech application collects debts to customers in various ways. The Fintech application usually puts pressure on customers such as contacting relatives or friends of victims through phone numbers

whose data can be accessed by the application on the victim's phone. Not infrequently, the application also often contacts the employer of the place where the victim works. In some cases, there are victims who are fired from their jobs because the application always contacts the employer's employer in collecting debts.

The Jakarta Legal Aid Institute (LBH) notes, as of June 2019 there were 4,500 complaints regarding Fintech lending. That number jumped compared to last year which reached a total of 1,330 complaints. There are at least 14 violations of law and human rights experienced by victims of illegal Fintech applications. The violations are as follows:

1. High and unlimited interest;
2. Billing which is not only done by the borrower or emergency contact included by the borrower;
3. Threats, libel, fraud and sexual harassment;
4. Dissemination of personal data;
5. Distribution of photos and loan information to contacts in the borrower's device;
6. Taking almost all access to the borrower's device;
7. Unclear contact and office location of the online loan application provider;
8. Unclear admin fees;
9. The application changes its name without notification to the borrower, while the interest on the loan continues to grow;
10. The borrower has paid the loan, but the loan has not been written off on the grounds of not entering the system;
11. The application cannot be opened and even disappears from the Appstore/Playstore when the loan repayment is due;
12. Billing is carried out by different people;
13. KTP data is used by providers of online loan applications to apply for loans in different applications;
14. Virtual Account refunds are incorrect, so interest continues to grow and intimidating billing continues.

Interest charged to users is also very high. Based on data from several peer-to-peer lending companies, there are Fintech that provides loans of Rp.800,000 to Rp1,500,000 with a tenor of up to 14 days. The total interest applied to the loan reaches 1% per day. The breakdown of interest is 0.05% per day, risk assessment is 0.2% per day, risk mitigation is 0.25% per day, returns are 0.15% per day, billing is 0.2% per day, and legal risk is 0, 15% per day. Based on the interest breakdown, the total interest, and principal to be paid after maturity for 14 days reaches Rp912,000 to Rp1,710,000. These details do not explain how much the fines are imposed if the customer is late paying. The amount of interest and short maturity causes many problems in billing. In addition to the burdensome economic burden of having to pay high interest and fines, many debtors experience depression due to terrorism by Debt Collector from Fintech Illegal. This billing practice has been complained about by a number of customers. The problem is, this illegal Fintech is not within the scope of supervision of the Otoritas Jasa Keuangan (OJK). Even though it has been closed, it does not make the illegal Fintech application disappear, this illegal peer-to-peer always disguises itself by using another identity so that many people are entangled. (OJK, 2019).

Data requested by this Fintech application includes very personal data. To get a loan of money, the customer must upload an ID card to the application and fill in the customer's address, bank account, and telephone number. In conducting customer verification, there is a need for approval from the customer so that the contacts on his smartphone can be accessed without being known by the customer the destination of the contact access. This has the potential to be misused by illegal Fintech both for commercial purposes and even to inhumane billing. The protection of personal data is a major problem in Fintech services. This is because POJK No.77 / 01/2016 does not provide criminal sanctions against perpetrators when distributing customers' personal data. In Article 47 POJK No.77 / 01/2016 only provides administrative sanctions in the form of written warnings to revocation of permits. These sanctions are only given to Fintech companies. While the personal liability of the person who spreads the customer's personal data cannot be reached. Matters regulated by the Financial Services Authority regarding Fintech include the following:

OJK and Bank Indonesia Regulation Related to Fintech		
1.	POJK No.77/POJK.01/2016	Information Technology Based Lending and Borrowing Services
2.	POJK No.13/POJK.02/2018	Digital Financial Innovations in the Financial Services Sector
3.	POJK No.37/POJK.04/2018	Urun Dana Fund Services through Equity Crowdfunding
4.	Bank Indonesia Regulation No.19/12/PBI/2017	Implementation of Financial Technology

Table 1. OJK and Bank Indonesia Fintech Regulation

Each of the above regulations only contains administrative sanctions and there is no strong legal basis to protect users from illegal lending practices as we can examine below.

3.1.1 POJK No.77/POJK.01/2016

In Chapter VI Part II governs the Confidentiality of User ata. In Article 26 POJK No.77/POJK.01/2016, Provider must:

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 data, transaction data, and financial data that it manages;

c. Ensure that the acquisition, use, utilization and disclosure of personal data, transaction data and financial data obtained by the Operator is based on the agreement of the owner of personal data, transaction data and financial data obtained by the Operator based on the approval of the owner of personal data, transaction data and data financial, unless otherwise specified by statutory provisions;
d. Providing other communication media besides the Electronic Information Technology-Based Lending and Borrowing Service System to ensure continuity of customer services that can be in the form of electronic mail, call centers, or other communication media; and
e. Notifying the owner of personal data, transaction data and financial data in writing if there is a failure in protecting the confidentiality of personal data, transaction data and financial data under management.

Regarding the prohibition set forth in Article 39 which stipulates that the Operator is prohibited in any way, providing data and/or information about Users to third parties. The sanctions imposed if violating Article 39 only in the form of administrative sanctions as stated in Article 47 paragraph (1) which reads:

For violating the obligations and prohibitions in these OJK regulations, OJK has the authority to impose administrative sanctions on the Provider in the form of:

a. Written warning;
b. Fines, namely the obligation to pay a certain amount of money;
c. Limitation of business activities; and
d. Revocation of permission.

3.1.2 POJK No.13/POJK.02/2018

In Chapter X concerning Data Protection and Confidentiality, Article 30 POJK No.13/ POJK.02/2018 states that:

1) The Operator is obliged to maintain the confidentiality, integrity, and availability of personal data, transaction data, and financial data that it manages since the data is obtained until the data is destroyed;
2) Provisions on the use of data and user information obtained by the Operator must meet the following requirements:
    a. Obtain consent from the user;
    b. Conveying limits on the use of data and information to users;
    c. Deliver any changes in the purpose of using data and information to the user in the event of a change in the purpose of using data and information; and
    d. The media and methods used in obtaining data and information are guaranteed confidentiality, security, and integrity.

This regulation also regulates the prohibition in Article 38 paragraph (1) which states that the Provider is prohibited from providing data and / or information about consumers to third parties. Sanctions given to Organizers that violate this article are only in the form of administrative sanctions regulated in Article 39 in the form of:

a. Written warning;
b. Fines, namely the obligation to pay a certain amount of money;
c. Cancellation of approval; and/or
d. Cancellation of registration.

3.1.3 POJK No.37/POJK.04/2018

In Chapter VII Part Two concerning Data Confidentiality regulated in Article 48, states that the Provider must:

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 data, transaction data, and financial data that it manages;
c. Guarantee that the acquisition, use, utilization and disclosure of personal data, transaction data and financial data obtained by the Operator is based on the agreement of the owner of personal data, transaction data and financial data, unless otherwise stipulated by statutory provisions;
d. Providing other communication media besides Electronic Funding Services through Equity Crowdfunding to ensure the continuity of Investor services that can be in the form of electronic mail, call centers, or other communication media; and
e. Give written notification to the owner of personal data, transaction data and financial data, if there is a failure in protecting the confidentiality of personal data, transaction data, and financial data that it manages.

The prohibition itself is regulated in Article 38 paragraph (1) which states that the Provider is prohibited from providing and / or information about consumers to third parties. The sanctions given are the same as the previous regulation which is still in the form of administrative sanctions as regulated in Article 39 POJK No.37 / POJK.04 / 2018, particularly:

a. Addressed warning;
b. Penalties, namely the obligation to pay a certain amount of money;
c. Cancellation of approval; and/o
d. Cancellation of registration

3.1.4 Bank Indonesia Regulation No.19/12/PBI/2017

In Bank Indonesia Regulation No.19 / 12 / PBI / 2017 regulates the obligations of Registered Financial Technology Providers for:

a. Apply the principle of consumer protection;
b. Preserve the confidentiality of data and / or consumer information including data and/or transaction information;
c. Apply the principles of risk management and prudence;
d. Using rupiah in every transaction made in the Republic of Indonesia;
e. Apply APU and PPT principles;
f. Meet other statutory provisions.

Of the four regulations owned by 2 financial institutions in Indonesia, there is no strongest and highest legal basis, namely the law to protect personal data from practices carried out by illegal Fintech. Regulations made by the Financial Services Authority (OJK) only regulate registered Fintech, so the sanctions stipulated in the above regulations are only imposed on registered Fintech companies. Whereas illegal Fintech does not yet have strong rules to ensnare them. In fact, if Indonesia has a legal umbrella for personal data protection and technological financial laws, there is strict law enforcement from the authorities who can crackdown on illegal Fintech and are not officially registered at the Otoritas Jasa Keuangan (OJK). So that the existence of a personal data protection law and technology financial law can prevent the misuse of personal data of users who are increasingly vulnerable to this era of highly developed digital innovation.

3.1.5 What around of the Information and Electronic Transactions Act?

The rules regarding personal data in Act Number 19 of 2016 concerning Amendments to the ITE Law in Article 26 paragraph (1) are regulated regarding personal data which reads, "Unless otherwise stipulated by legislation, the use of any information through electronic media involving personal data a person must be carried out with the consent of the person concerned. "The criminal sanctions provided for in Law Number 19 of 2016 only regulate the following: 1) people who intentionally and without the right to send information that violates decency; 2) people who intentionally and without the right to send information that has a gambling content; 3) people who intentionally and without the right to insult and / or defame; 4) people who intentionally and without the right to carry out extortion and / or threats; 5) people who spread false and misleading news that result in consumer losses in Electronic Transactions; 6) people who spread information intended to incite hatred or hostility of certain individuals and / or groups of people based on ethnicity, religion, race and intergroup (SARA); 7) people who spread information with the aim of causing hatred or hostility of certain individuals and/or groups of society. Prohibition regulated in Law No. 19 of 2016 does not include violations of the law committed by illegal Fintech so there is a need for special laws governing financial technology and protecting personal data. (Sinta Dewi Rosadi, 2018).

3.1.6 The Importance of Personal Data Protection Act

Privacy is one of the biggest problems in this new electronic age. Digital data that contains a person's personal information is a remarkable prodigious asset. It is a tempt gold mine for organizers who have explored the digital business world in the 4.0 industrial revolution. As the life of e-commerce, these data can be used in the framework of planning and decision making that are useful in developing business in the digital world. Personal data is a type of data that includes a population identity such as full name, date of birth, residence, to someone's status. Article 6 paragraph (3) of the Draft Act on the Protection of Personal Data regulates what is meant by personal data which includes beliefs, health data, biometrics, genetics, sex life, political views, criminal records, child data, personal financial data, information about disability physical and mental. The definition of personal data gives a clear picture of one's preferences. Data can be used to design marketing strategies. This can help the company to avoid various mistakes that might occur. For example, a bag company assumes that backpacks are being sought after by many people and continuously produce backpacks. But apparently the facts on the ground are different, tote bags are actually in demand, the potential for consumers to buy company products will be quite small. This will be detrimental to the company so having consumer data is incredibly important to know trends that are of concern right now. Corporate awareness of the importance of data is increasing. In 2017, the revenue of the large data technology business along with its analysis (big data analytic/BDA) globally reached 150.8 billion US dollars (around Rp2000 trillion). The thing that should be the focus in this era of big data is how to protect user data from crime and misuse of that data. If not anticipated, it will increasingly lead to complex problems. So that regulations regarding the protection of personal data become a necessity in this digital era because until now Indonesia does not yet have its rules so user data in companies are vulnerable to be misused and traded.

Technology has advanced the importance of this kind of privacy as it is especially the ability to communicate without being in the same physical

place that makes privacy invasions possible. The invention of the telephone is a good example of this phenomenon. It is evident that on line communication today is a major field for privacy protection. All personal data may be viewed as private that may lead to an invasion of privacy. Some personal data is categorized as sensitive implying that misuse regardless of the factual situation constitutes an infringement of privacy while other data is viewed as ordinary and for this reason usage of this data may not always violate privacy. In general privacy law this will depend on the situation while in data protection law all personal data as a starting point is protected. Data protection provides in this sense a more extensive regulation and seen from the legal perspective, this is a main difference between the two concepts. Privacy also relates to communication as it protects the right to communicate in confidentiality and without surveillance. (James Waldo, et al, 2007). The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others. Provisions on the protection of privacy data and personal data are mandates Protection of personal data is one form of privacy protection that is mandated directly by the Constitution of the Republic of Indonesia which contains respect for human rights values and equality values and respect for individual rights so it needs to be given a foundation the law to provide more privacy and personal data security to ensure a conducive business climate. Article 28 G of the 1945 Constitution of the Republic of Indonesia which regulates the right to protection of personal, family, honor, dignity, and property under his authority. Privacy is recognized internationally in Article 12 of the Universal Declaration of Human Rights (UDHR) that proclaims: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. Everyone has the right to the protection of the law against such interference or attacks.” In 1998, UN Human Rights Committee recognized the need for data protection laws to safeguard the fundamental right to privacy by Article 17 of the ICCPR: “The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination. (Sinta Dewi Rosadi, 2018). In December 2016, the UN General Assembly passed a resolution on the Right to Privacy in the Digital Age, GA Res. 71/199, which reaffirmed previous General Assembly resolutions on the subject, emphasizing that: “States must respect international human rights obligations regarding the right to privacy when they require disclosure of personal data from third parties, including private companies.

Warren and Brandeis in his work entitled The Right to Privacy states that privacy is the right to enjoy life and the right to be respected by his feelings and thoughts. (Warren, Samuel D., & Louis Brandeis, 1890). This is confirmed by Allan Westin where privacy protection is closely related to the fulfillment of personal data rights. He defines privacy as the right of individuals, groups, or institutions to determine whether information about them will be communicated or not to other parties. (Alan Westin, 1967). Personal data is data that relates to an individual. Individuals need tools to protect their right to privacy and protect themselves and their data from abuse. It is about safeguarding human fundamental right to privacy by regulating the process of personal data by providing the individual rights over their data, and setting up systems of accountability and clear obligations for those who control or undertake the processing of the data. (Alan Charles Raul, 2007). Individuals have the right to view their data and amend it as needed; the right to be notified when and to whom individually identifiable data has been disclosed; and the right to request restricted access of their data to different entities. (Fred H. Cate, et al, 2014). In relation to citizenship, the information contained in the ID card is the thing to get the protection of privacy and personal data. Because population data is personal data that if this leaks will threaten the privacy of its owner because population data includes but is not limited to the person's birth month, address, information about physical and/or mental disability and some contents of important event records. Every citizen has the right to obtain protection for privacy and personal data and compensation and restoration of good name as a result of errors in Population Registration and Civil Registration as well as misuse of personal data by implementing agencies. Thus the Implementing Agency has an obligation to guarantee the confidentiality and security of population data. This obligation is a consequence of the state as a welfare state that is flexible to the times to protect the right to privacy of its citizens.

There are two main reasons that the government must make a comprehensive data protection legal basis: 1) the law must be able to overcome problems that occur in accordance with the times. Currently, the community has entered the era of industrial revolution 4.0 where data is a valuable asset. The current value of a data mine exceeds that of gold, silver, and gem. Activities undertaken by the community have now been integrated through the online system so that a lot

of data has been collected through these activities. In many countries, rules regarding the protection of privacy and personal data already exist and remain important to help protect people's information and human rights; 2) corporate and self-regulation are not too working to protect our data. (Malecki, Edward J., & Bruno Moriset, 2009). As in cases that occur in the community due to illegal Fintech, companies and other entities that collect people's data have long advocated for regulation of privacy and data protection not through binding frameworks but rather through self or co-regulation mechanisms that offer them greater versatility. Indonesia currently has a Personal Data Protection Bill. The draft law aims to incorporate privacy arrangements for personal data that are spread into a separate law. The protection of personal data is important for Indonesia to provide privacy and personal data protection that is on par with other countries. The arrangement drawn up in this Draft Law is expected to place Indonesia on a level with countries that are already aware of the protection of privacy and personal data. Below are countries that have adopted personal data protection laws that govern each of the following:

3.1.5.1 European Union

The protection of personal data and privacy in the European Union has been recognized as a fundamental right in the European Union Charter of Fundamental Rights. As a derivative of the Charter, the European Union has a personal data protection legislation in 2016 that is used to protect personal data in the digital age known as The General Data Protection Regulation (GDPR) based on Regulation 2016/679. This regulation is essentially a step to strengthen the fulfillment of the basic rights of European Union people in the Digital Age and will directly encourage more conducive business development. The European Union also established The Police Directive based on Directive 2016/680 which protects individuals in processing personal data that has an element of the criminal offense as well as the application of criminal sanctions for violations of personal data committed against data subjects. Some of the key privacy and data protection requirements of the GDPR include:

a. Requiring the consent of subjects for data processing;
b. Anonymizing collected data to protect privacy;
c. Providing data breach notifications;
d. Safely handling the transfer of data across borders;
e. Requiring certain companies to appoint a data protection officer to oversee GDPR compliance.

The GDPR itself contains 11 chapters and 91 articles. The following are some of the chapters and articles that have the greatest potential impact on security operations:

Articles 17 & 18
Articles 17 and 18 of the GDPR give data subjects more control over personal data that is processed automatically. The result is that data subjects may transfer their personal data between service providers more easily (also called the “right to portability”), and they may direct a controller to erase their personal data under certain circumstances (also called the “right to erasure”).

Articles 23 & 30
Articles 23 and 30 require companies to implement reasonable data protection measures to protect consumers’ personal data and privacy against loss or exposure.

Articles 31 & 32
Data breach notifications play a large role in the GDPR text. Article 31 specifies requirements for single data breaches: controllers must notify Supervising Authorities (SA)s of a personal data breach within 72 hours of learning of the breach and must provide specific details of the breach such as the nature of it and the approximate number of data subjects affected. Article 32 requires data controllers to notify data subjects as quickly as possible of breaches when the breaches place their rights and freedoms at high risk.

Articles 33 & 33a
Articles 33 and 33a require companies to perform Data Protection Impact Assessments to identify risks to consumer data and Data Protection Compliance Reviews to ensure those risks are addressed.

Article 35
Article 35 requires that certain companies appoint data protection officers. Specifically, any company that processes data revealing a subject’s genetic data, health, racial or ethnic origin, religious beliefs, etc. must designate a data protection officer; these officers serve to advise companies about compliance with the regulation and act as a point of contact with SAs. Some companies may be subjected to this aspect of the GDPR simply because they collect personal information about their employees as part of human resources processes.

Articles 36 & 37
Articles 36 and 37 outline the data protection officer position and its responsibilities in ensuring GDPR compliance as well as reporting to Supervisory Authorities and data subjects.

Article 45
Article 45 extends data protection requirements to international companies that collect or process EU citizens’ personal data, subjecting them to the same requirements and penalties as EU-based companies.

Article 79
Article 79 outlines the penalties for GDPR non-compliance, which can be up to 4% of the violating company's global annual revenue depending on the nature of the violation.

The GDPR has increased penalties for non-compliance. SAs or 'lead authority' have more authority than in the previous legislation because the GDPR sets a standard across the EU for all companies that handle EU citizens' personal data. SAs hold investigative and corrective powers and may issue warnings for non-compliance, perform audits to ensure compliance, require companies to make specified improvements by prescribed deadlines, order data to be erased, and block companies from transferring data to other countries. Data controllers and processors are subject to the SAs' powers and penalties. The GDPR also allows SAs to issue larger fines than the Data Protection Directive; fines are determined based on the circumstances of each case and the SA may choose whether to impose their corrective powers with or without fines. For companies that fail to comply with certain GDPR requirements, fines may be up to 2% or 4% of total global annual turnover or €10m or €20m, whichever is greater. (European Union, 2016).

3.1.5.2 Malaysia

Malaysia has regulations on privacy protection and personal data called The Personal Data Protection Act 2010 (the PDPA) that covers relevant legislation and competent authorities, territorial scope, key principles, individual rights, registration formalities, appointments of a data protection officer and processor in 42 jurisdictions. In these rules, there are 3 major matters regulated namely: 1) banking and financial sector; 2) communications sector; 3) the healthcare sector. The definitions regulated in this regulation include:

1) Personal Data
   Personal data means any information in respect of commercial transactions which:
   a. Is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
   b. Is recorded with the intention that it should wholly or partly be processed by means or such equipment; or
   c. Is recorded as part of a relevant filling system or with the intention that it should form part of a relevant filling system

   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, including any sensitive personal data and expression of opinion about the data subject, but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

2) Processing
   a. In relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including: The organization, adaption or alteration of personal data;
   b. The retrieval, consultation or use of personal data;
   c. The disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or
   d. The alignment, combination, correction, erasure or destruction of personal data.

3) Controller
   The term used in Malaysia is data user. A data user is defined as a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor.

4) Processor
   Means any person, other than employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.

5) Data Subject
   Means an individual who is the subject of the personal data.

6) Sensitive Personal Data
   Means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as may be determined by the Minister of Communications and Multimedia.

7) Data Breach
   Is not defined in the PDPA

8) Commercial Transactions
   Are defined as any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010. Sections 9 about Security Principle of the PDPA provides that data users must take practical steps to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, by deployment of the necessary technical or organizational security measures to protect personal data. Besides that, the PDPA has

individual rights in relation to the processing of their personal data which include:

a. Right to access to data/copies of data;
b. Right to rectification of errors;
c. Right to deletion or right to be forgotten;
d. Right to object to processing;
e. Right to restrict processing;
f. Right to data portability;
g. Right to withdraw consent
h. Right to object to marketing
i. Right to complain to the relevant data protection authority (ies). (The Personal Data Protection Act, 2010).

3.1.5.3 India

India has The Personal Data Protection Bill in 2018 that regulates the privacy protection of citizen-state. This regulation is concern about sensitive personal data, genetic data, and health data. Besides that, this regulation has security guards and its penalties. Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioral characteristics, physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. Beside of that, health data means data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services. In article 31 govern about security safeguard that states:

1) Having regard to the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, the data fiduciary and the data processor shall implement appropriate security safeguards including:
   (a) use of methods such as de-identification and encryption;
   (b) steps necessary to protect the integrity of personal data;
   (c) and steps necessary to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data.
2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically as may be specified and may take appropriate measures accordingly.

India also authenticate Data Protection Authority of India to establish for the purpose of this Act that shall be a body corporate by the name preceding, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued. The Authority may, with the prior approval of the Central Government, establish its offices at other places in India. The unique one is on Article 60 subsection (1), (2), and (3) that regulate power and functions of that authority which includes:

1) It shall be the duty of the Authority to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness of data protection.
2) Without prejudice to the generality of the foregoing and other functions set out under this Act, the functions of the Authority shall include:
   a. monitoring and enforcing application of the provisions of this Act;
   b. specifying reasonable purposes for which personal data may be processed under section 17 of this Act;
   c. specifying residuary categories of sensitive personal data under section 22 of this Act;
   d. taking prompt and appropriate action in response to a data security breach in accordance with the provisions of this Act;
   e. specifying the circumstances where a data protection impact assessment may be required to be undertaken in accordance with section 33 of this Act;
   f. maintaining a database on its website containing names of significant data fiduciaries along with a rating in the form of a data trust score indicating compliance with the obligations of this Act by such fiduciaries;
   g. specifying the criteria for assigning a rating in the form of a data trust score by a data auditor having regard to the factors mentioned in sub-section (2) of section 35;
   h. examination of any data audit reports submitted under section 35 of this Act and taking any action pursuant thereto in accordance with the provisions of this Act;
   i. issuance of a certificate of registration to data auditors and renewal, modification, withdrawal, suspension or cancellation thereof and maintaining a database on its website of such registered data auditors and specifying the requisite qualifications, code of conduct, practical training and functions to be performed by such data auditors;
   j. categorization and issuance of certificate of registration to significant data fiduciaries and renewal, modification, withdrawal, suspension or cancellation thereof under section 38;
   k. monitoring cross-border transfer of personal data undersection 41 of this Act;
   l. issuing codes of practice in accordance with section 61 of this Act and publishing such codes on its website;
   m. promoting public awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal

data, including issuance of any public statement setting out trends in, or specific instances of, contravention of the provisions of this Act by a data fiduciary or a class of data fiduciaries, as the case may be;

n. promoting awareness among data fiduciaries of their obligations and duties under this Act;
o. monitoring technological developments and commercial practices that may affect protection of personal data;
p. promoting measures and undertaking research for innovation in the field of protection of personal data;
q. advising Parliament, Central Government, State Government and any regulatory or statutory authority on measures that must be undertaken to promote protection of personal data and ensuring consistency of application and enforcement of this Act;
r. issuing guidance on any provision under this Act either on its own or in response to any query received from a data fiduciary where the Authority considers it necessary, subject always to the provisions of this Act;
s. advising the Central Government on the acceptance of any relevant international instrument relating to protection of personal data;
t. specifying fees and other charges for carrying out the purposes of this Act; (u) receiving and handling complaints under the provisions of this Act;
u. calling for information from, conducting inspections and inquiries into the affairs of data fiduciaries in accordance with the provisions of this Act;
v. preparation and publication of reports setting out the result of any inspection or inquiry and any other comments that the Authority deems to be in public interest; and
w. performing such other functions, including maintaining, updating and submitting any records, documents, books, registers or any other data, as may be prescribed.

3) Notwithstanding anything contained in any other law for the time being in force, while exercising the powers under clause (v) of sub-section (2), the Authority shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a suit, in respect of the following matters, namely:
   a. the discovery and production of books of account and other documents, at such place and at such time as may be specified;
   b. summoning and enforcing the attendance of persons and examining them on oath;
   c. inspection of any book, document, register or record of any data fiduciary;
   d. issuing commissions for the examination of witnesses or documents;
   e. any other matter which may be prescribed.

India also has an Appellate Tribunal regulated in Article 79 subsection (1) which states that:

(1) The Central Government shall, by notification, establish an Appellate Tribunal to:
   a. hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 39;
   b. hear and dispose of any appeal from an order of the Authority under sub-section (2) of section 65;
   c. hear and dispose of an application under sub-section (9) of section 66;
   d. hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 74; and
   e. hear and dispose of any appeal from an order of an Adjudicating Officer under subsection (7) of section 75. (The Information Technology (Amandment) 2008).

Many countries establish laws that deal with this matter, but there is no law in Indonesia regulating this matter. The development of digital technology, globalization, and the power of data have created the need for privacy on personal data. Privacy on personal data terms as a human right has become more and more important in the era of information and communication technology (ICT). Taking into account the above mentioned development, Indonesia should develop a specific legislation on privacy on personal data. In formulating a good concept of regulation, the initial process starts with the good goal setting. Law is not only the rules and principles that govern human life in society, but also covers institutions and processes to realize that law in the reality.

The state has a big role to play in establishing regulations regarding financial technology and the Data Protection Act. A good concept of regulation should cover: principles, rules, processes, and institutions. If it is associated with the concept of privacy on personal data regulation, then such regulation should include:

1. The principle to be the basis in establishing a regulation should consider both national and international developments. The principles of information privacy on personal data regulation should be based on the 1945 Constitution wherein Article 28 (G) has clearly recognized that the right to privacy on personal data must be protected;
2. In addition to the basic principles, the concept of regulation must also consider the so called principles of fair use of information (fair information principles) which calls for standards of practices required to ensure that entities that collect and use personal data provide adequate protection. These standards that have been internationally recognized and as such adopted by many countries such as: the principles of the OECD Guidelines in 1980, the EU General Directive 1995, and the APEC Framework 2004, these include the following principles: (European Union Agency for Fundamental Rights and Council of Europe, 2016)

a. Principle of limitation in the collection of information. The information obtained, processed and disseminated should be limited only to lawful and fair purposes and should be upon the knowledge and consent of the information owner;
b. Principle concerning the quality of information. Personal information must be obtained in accordance with the intent and purpose of its collection. Quality of information must be maintained in terms of its accuracy, completeness and updates;
c. Principle of the objective. Personal information may only be opened in accordance with its intended use;
d. Principle of retention. The retention of information for a particular purpose should not be longer than the necessary period of time;
e. Principle of maximum security on personal information. Personal information shall be protected by adequate security system in order to avoid the risk of losing or unlawful act such as access, destruction, use, modification or disclosure of such information by other parties;
f. Principle of transparency. The management of information must take necessary steps so that the information owners can learn about the kinds of personal information held by the data manager;
g. Principle of individual participation of information subject. Information's owners shall have the right to access their personal information maintained by the data manager, including the right to make corrections to their personal information;
h. The principle of accountability. Information manager is fully responsible to implement the above mentioned principles.
3. There must be clear definitions of the substantial terms to be mentioned in the regulation;
4. Scope of regulation must be clear;
5. The subject to be regulated by the law must be determined;
6. Legislation should also regulates exceptions in order for personal information to be disclosed for special cases;
7. Institution
   In achieving a good concept of regulation, involvement of both institution and process is a must. In the law making process, the institution has an obligation to be able to carry out its duties properly and must always be accountable for all of his duties to the public;
8. Has criminal sanction. (Sinta Dewi Rosadi, 2018).

4. CONCLUSIONS

In order to become a developed country in line with technological developments and succeed in organizing the industrial revolution 4.0, the government as the organizer should be able to intervene in providing protection to the community. in this case the protection provided is in the form of personal data protection. because as explained earlier, it can be concluded that in the future problems related to the digital world that cover various sectors will experience complex problems so that strict rules are needed to ensure the creation of certainty, justice and the benefit of law for citizens. Therefore, the government as a rule-maker needs to immediately establish rules regarding personal data protection and Fintech.

The personal data protection law and the financial technology law, as well as the above mentioned, must cover a number of things. First, regulate the controller or organizer that collects digital and consular data or third-party organizers who work with the first organizer. The GDPR regulated by a strict controller of the provision of personal data to third parties. Second, the clarity of the relevance of data use. Third, the data accessed has a time limit for existence, so it cannot be stored forever. Fourth, easy to access and easy to delete personal data, meaning the platform must make it easy for users to delete their data that has been given to the platform.

REFERENCES

[1] Cate, Fred.H., et al. *Data Protection Principles for the 21st Century.* Indiana: Indiana University, 2014.

[2] European Union Agency for Fundamental Rights and Council of Europe. *Handbook on Eurepoean Data Protection Law*. Belgium: European Union Agency, 2014.

[3] Malecki, Edward J., & Bruno Moriset. *The Digital Economy: Business organization, production processes, and regional developments.* London & New York: Routledge, 2009.

[4] Raul, Alan Charles. *The Privacy, Data Protection and Cybersecurity Law Review 4th Edition.* Derbyshire: Encompass Print Solutions, 2017.

[5] Rosadi, Sinta Dewi. *Aspek Perlindungan Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*. Bandung: Refika, 2015.

[6] Waldo, James, et al. *Enganging Privacy and Information Technology In A Digital Age.* Washington: The National Academy of Science Press, 2007).

[7] Westin, Alan. *Privacy and Freedom.* London: Athenum, 1967.

[8] Gellert, Raphael. "Understanding Data Protection As Risk Regulation." Journal of Internet Law, Vol.18, No.11, (May 2015). [Accessed at 1 October 2019].

[9] Rosadi, Sinta Dewi. "Protecting Privacy On Personal Data In Digital Economic Era: Legal Framework in Indonesia." Brawijaya Law Journal, Vol. 5, No.1, (April 2018). [Accessed at 1 October 2019].

[10] Warren, Samuel D., & Louis Brandeis. "*The Right to Privacy*." Cambridge: Harvard Law Review, No.193, (December, 1890).

[11] European Union, *General Data Protection Regulation (GDPR)*. 679/2016.

[12] India, The Information Technology (Amendment) Act 2008.

[13] Indonesia, *Digital Financial Innovations in the Financial Services Sector*. POJK No.13/POJK.02/2018.

[14] Indonesia, *Information Technology Based Lending and Borrowing Services*. POJK No.77/POJK.01/2016.

[15] Indonesia, *Implementation of Financial Technology*.

Bank Indonesia Regulation No.19/12/PBI/2017.

[16] Indonesia, *Information and Electronical Transaction.* Law No. 19 of 2016. State Gazette. No. 58 of 2008, Supplementary to the State Gazette No. 4843.

[17] Indonesia, *Urun Dana Fund Services through Equity Crowdfunding*. POJK No.37/POJK.04/2018.

[18] Malaysia, The Personal Data Protection Act. 709/2010.

[19] Congressional Research Service. *Data Protection Law: An Overview*. March 2019.

[20] European Data Protection Supervisor. *Guidelines on the protection of personal data in IT governance and IT management of EU institutions.* March 2018.

[21] Privacy International. *A Guide for Policy Engangement on Data Protection: The Keys to Data Protection.* London: Privacy International, 2018.

[22] World Vision. *Data Protection, Privacy, and Security for Humanitarian & Development Programs.* Discussion Paper.

[23] AntaraNews. "*UU Fintech dan Perlindungan data Pribadi Solusi Jerat Fintech Illegal.*" https://www.antaranews.com/berita/1102548/uu fintech-dan-perlindungan-data-pribadi-solusi jerat-fintech-ilegal (accesses 4 October 2019).

[24] Geotimes. "*Jerat Hutang Fintech.*" https://geotimes.co.id/op-ed/jerat-hutang-fintech/ (accesses 1 October 2019).

[25] Kompas.com. "*Per Juni 2019, LBH Jakarta terima 4.500 Aduan Fintech.*" https://money.kompas.com/read/2019/07/29/1547005 26/per-juni-2019-lbh-jakarta-terima-4.500-aduan-soal-pinjaman-fintech (accesses 3 October 2019).

[26] The Jakarta Post. "*Fintech companies need to protect customers from frauds and data misuse: Observers.*" https://www.thejakartapost.com/news/2019/09/27/fintech-companies-need-to-protect-customers-from-frauds-and-data-misuse-observers.html (accesses 3 October 2019)