



Personal Data Protection in Indonesia: Legal Perspective

Andriyanto Adhi Nugroho; Atik Winanti; Surahmad

Faculty of Law, UPN Veteran Jakarta, Indonesia

<http://dx.doi.org/10.18415/ijmmu.v7i7.1773>

Abstract

The arrangement of personal data protection in national law is stipulated explicitly in the regulation of the Minister of the Ministry of communication and Information No. 20 of 2016 on the protection of personal data. In Indonesia, there are no rules that accommodate the protection of personal data on financial technology. That can be hazardous when the economic response of technology is not limited to its use. The case of personal data is not contained in the case of a Such hazard that may arise. The case from the theft of personal data, damage to the system that may allow the occurrence of data breaches, misuse of personal data that has been the business ruled itself, or other parties who may access personal consumer data (such as government). The need to set this up is important because private data is a person's privacy right. Still, it can fundamentally be economically valuable for a third party who is about to take advantage of it.

Keywords: *Data Protection; Personal Data; Financial Technology*

Introduction

Data protection logically and historically entwined with privacy, and disentangling their substance has proven to be a daunting task. (Lorenzo Dalla Corte, 2020), the relevant changes in the light of the legal vacuum where mobile wallet issuers were operating before. The obligations to apply enhanced security measures and strong consumer authentication ought to result in increased security of mobile payments. (Johan Peeters, 2020). Under the General Data Protection Regulation (GDPR), transparency of information becomes an obligation aimed at creating an ecosystem where data subjects understand and control what happens to their data. (Rossi & Palmirani, 2020). Concept of personal data and the future of EU data protection law. (Purtova, 2018). Data protection legislation generates an enforceable framework for guarding against informational privacy harms (Tamò-Larrieux A, 2018). Comparison brought to light which type of protection is best suited to protect the investment in database creation (Derclaye, 2007).

The startup movement in Indonesia can be said to continue to develop rapidly. This type of startup divided into two, namely, e-commerce and financial technology (Fintech). E-commerce is a company that provides online buying and selling platform. At the same time, Fintech is more focused on companies that innovate in the field of financial services with the touch of modern technology (Yuking,

2018). Simply, Fintech can be construed as the utilization of information technology to improve services in the financial industry. Another definition is the variation of business models and technological developments that have the potential to improve the financial services industry (Departemen Perlindungan Konsumen, 2017).

In a juridical sense, Fintech is found in the Bank Indonesia Regulation (PBI) Number 19/12/PBI/2017 About organizing Financial technology. Organizing Financial technology declares that financial technology is the use of technology in the financial system. That generates new products, services, technology, and/or business models and can impact monetary stability, financial system stability, and/or efficiency, smoothness, safety, and reliability of the payment system.

E-commerce has become an essential means for small, medium, and large scale businesses around the world. Not only sell goods and raw materials from sales to buyers but involve the interaction of the parties. In 2012 the sales by E-Commerce in The world reached 1 trillion US dollars (Renouw,2017). E-commerce based on the World Trade Organization (WTO), covering the field of production, distribution, marketing, sale, and delivery of goods and/or services through electronics. At the same time, the OECD (*Organization for Economic Cooperation and Development*) explains that e-commerce is a process based on electronic data transitions and processes. Apart from these two international institutions, the *Alliance for Global Business*, a prominent field of trade, means another about E-commerce, i.e., all value transactions involving the transfer of information, products, services, or payments through electronic networks as media (Renouw,2017).

Currently, the scope of the Internet has covered almost all over the world. In 1998 it was estimated that there are over one hundred million people who use the Internet and by the year 1999 the number has reached twice. Data Monitor 125 estimated in 2005, more than 300 million people (Sitompul, 2004). Once the Internet is open to the broader community, the Internet also used for trading purposes. There are at least two things that encourage trading activities concerning technological advances that are increasing demand for the product's technology and the ease of conducting trade transactions (Rahardjo, 2001). The development of the technology world is overgrowing in the world no exception Indonesia by reaching the third rank in Asia for the number of Internet users. It has recorded 44.6 million Facebook users and as many as 19.5 million Twitter users in Indonesia. Indonesia is the fifth largest country of Twitter users under the UK and other major countries. From 245 million Indonesians, Internet users in Indonesia reach 55 million people or control Asia by 22.4% after Japan(<http://kominfo.go.id>).

While the laws and regulations of E-commerce or electronic transactions in the State of Republic of Indonesia, Singapore, and Australia vary. However, the same is the same as referring to the UNCITRAL Model Law of the United Nations. Each country has a difference in legal needs for its people. In the Republic of Indonesia, E-commerce began to be governed by more cyber violations occurred so that the government established law No. 11 the year 2008 on electronic information and transactions for online trading. It contains several articles that also govern the certification body to supervise goods or services issued by business actors to circulate the market through the Internet. This institution is further governed by government regulation No. 82 the year 2012 on the implementation of electronic transactions and systems (Renouw, 2017). As for the total value of the Indonesian e-commerce market in 2014 predicted by Vela Asia, and Google will reach USD 8 billion and predicted to increase to reach USD 24 billion. Visa estimates online shopping in Indonesia will grow 40% this year and 53% next year, from 23% last year. Given the rapid growth of e-commerce, e-commerce related rules have been widely regulated in the Law (UU) No. 7 of 2014 on trade. E-Commerce setting is Trust ACT No. 7 years 2014 about trading (<http://www.pajak.go.id>).

The presence of e-commerce gives a remarkable comforting to consumers because consumers do not need to go out shopping besides the choice of goods/services that vary with a relatively lower price. It is a positive and negative challenge. It is said to be positive because the condition can provide benefits for

consumers to choose the goods/services it wants freely. Consumers have the freedom to determine the type and quality of goods/services according to their needs. It is said to be negative because the condition causes the customer to become weaker than the position of the business that can lead to disappointment and loss (Susanto, 2008).

The growing progress of the Internet is one of the driving factors of the development of e-commerce in Indonesia. The growth of e-commerce is governed by law No. 19 of 2016 concerning information and electronic transactions abbreviated to the ITE law. As a consumer, we must be observant in buying an item. In e-commerce, it is also necessary to bind the agreement between consumers and e-commerce in conducting personal data. In other words, every what has become the owner of consumers an e-commerce Party to analyze personal data that becomes a confidential owner of the personal data. The will of parties manifested in the agreement is the basis of binding an agreement, the will can be expressed in various ways both oral and written and binding on the parties with all the consequences of the law (Suharnoko, 2004).

In e-commerce transactions created more practical business transactions paperless and in e-commerce transactions can not meet directly to parties who conduct transactions. So it can be said e-commerce to be a new economic movement in the field of technology. In general trade, e-commerce transactions create an alliance between parties to provide an achievement as an example in the agreement between the parties to provide a prestige as an example in the coalition or buy and sell agreements. In this agreement arise rights, and obligations filled by the parties involved. But in law No. 11 of 2008 on information and electronic transactions, in addition to regulating the utilization of information technology, also handles electronic transactions. Electronic transactions are legal acts made using computers, computer networks, and/or other media. Application of law No. 11 of 2008 on information and electronic transactions is still facing technical constraints.

The number of human needs and desires, according to Nathan Roscoe Pound, the means of serving and fulfilling human needs and desires are limited. The risk is a conflict of interest, so it becomes a legal right or a right through the law, the interests and passions of the community, as can be protected by the law (Renouw, 2017).

Personal Data is data that is in the form of someone's identity, code, symbol, letter, or figure. Each country uses different terminology between personal information and personal data. However, the terms have almost the same understanding that the two terms often used interchangeably. The United States, Canada, and Australia use the terms of personal information, whereas the EU and Indonesian countries themselves in the Electronic Information and Transactions (ITE) act use personal data terms. Currently, there are several legal provisions related to the protection of personal data consisting of the general to the Special. The essential purpose of the privacy policy in e-commerce activities is that in addition to providing legal certainty to consumer's personal information. That has been input and or preferences made in the movement of electronic transactions is not abused and kept confidential because it is related to the human rights of consumers. Also related to the efforts of the provider of e-commerce services and online marketplace system to avoid violations of the security and comfort and dignity of the consumer itself (Indriyani et al., 2017).

However, it can be conveyed that personal data is essential to be protected. The personal data protection important because there have been many leaks associated with personal data, in an application system all cover all data related to the address, residence, and document documents relating to the data required in completing an account in any form relating to the e-commerce infringements of privacy. This crime aimed at the information of someone who is very personal and confidential. This crime usually addressed to the personal information of someone stored on the personal data form stored in

computerized. Which is known by others, can harm the victim materially or immaterial, such as identity, credit card number, credit card PIN (Ketaren, 2016).

Results and Discussion

Personal Data

Personal Data is certain individual data that is stored, cared for, and safeguarded and protected by confidentiality. Certain individual data is any reliable and tangible information that is inherent and identifiable, whether direct or indirect, in each individual whose utilization is following the provisions of the laws and regulations. So it can be said that the identity in conducting a loan agreement in the Fintech included in the personal data, which is owned by the owner of the private data, which is the individual to whom the particular individual data attached. Privacy or if it merely translates "personal freedom," closely with the issue of how the personal data of the community is getting adequate protection so that no more misuse of personal data. The development of society united fretted with the phenomenon of "data leakage," which causes the discovery, SMS credit offers, Pictures/videos, credit card numbers, data/confidential company information. Personal Data today is a valuable asset for businesses and organizations that continually collect, exchange, process, store, and even sell personal data as a commodity, especially with regards to consumers.

Personal Data in National Law

The protection of personal data since 2016 has had the rules as stipulated in the Minister of Communication and Information Regulation No. 20 of 2016 on personal Data protection in electronic systems. This regulation was born weighing the need for official rules regarding the protection of personal data to enforce the provisions of article 15 paragraph (3) of Government Regulation No. 82 year 2012, on the implementation of electronic systems and transactions.

The arrangement of personal data protection has not stipulated in the law of Indonesia which governs the legal protection of personal data in the law explicitly; however, there are at least Indonesian legislation that we can use to retain our data in electronic media that is regulation of the Minister of Government No. 20 year 2016 on personal Data protection in electronic systems.

Personal data protection arrangements governed by some articles in the electronic information and transaction act. This act does not yet contain strict and comprehensive personal data protection rules. However, this act indirectly gives rise to a new understanding of the protection of the existence of data or electronic information of both public and personal that specifically in the Electronic media. This personal data contained in article 26 paragraph 1 ITE Act, stating that "unless otherwise specified by statutory regulations, the use of any information through electronic media regarding the personal data of a person must do with the consent of the person concerned."

The personal data in the electronic media contained in article 26 of the ITE Act remains unclear and not described in detail. For example, when compared to article 84 of Act No. 23 of the years 2006 of the population Administration governing the protection of personal data of residents registered with E-Resident Card. In article 26 of ITE Act. It is described in detail the personal data of residents who must be protected including family card number, population registration number, date of birth, information on physical and or mental disability, population registration number of the biological mother, population registration number fathers, and some critical event record contents.

In addition to the stipulated in article 26 of ITE Act and regulated in the government regulation number 82 the year 2012. This set about the protection of unauthorized data use protection by electronic system organizers, protection from information access, Protection of Intervening illegal.

The Urgency of Personal Data Protection in Financial Technology

According to the Minister of Communication and Information Regulation No. 20 of 2016, electronic systems that can be used in the process of protecting personal data are electronic systems. That system has been certified and has internal rules on the protection of personal data that must pay attention to aspects of the application of technology, human resources, methods, and costs.

According to Minister of Communication and Information Regulation No. 20 the year 2016, has the right to the confidentiality of its data; The right to file a complaint to complete the personal data; Entitled to gain access to personal historical data; and reserves the right to request the destruction of certain individual data in electronic systems. This right related matter is governed in article 26 of the Minister of Communication and Information Regulation No. 20, the year 2016.

Any electronic system will be obliged to notify the personal data owner in the event of a failure of confidential protection of personal data. The information that must be submitted include:

- a. Reasons or causes of secret security of personal data may be carried out electronically,
- b. have been accepted by the personal data owner if such failure contains any potential loss to the concerned
- c. Written notice is sent to the owner of the personal data no later than 14 (fourteen) days from the date of failure.,

In addition to administrative sanctions, following Act No. 11 of 2008, Jo. Act No. 19 of 2016, if there is proved to be a violation of personal data misuse by third parties and fulfilling. The criminal element of the use of personal data information and causing losses, it can be sentenced to imprisonment for a maximum of 12 (twelve) years and/or a fine of Rp 12.000.000.000 (twelve billion rupiah).

The Fintech industry is essentially utilizing information technology in the financial system that produces new products, services, technologies, and/or business models. This new capital business needs to be supported by the government because it is very profitable to increase Indonesia's economy both in terms of business and society as consumers. However, it is also worth noting that the use of information technology for two-eyed knives. Technology, if used properly, can help human life. Still, technology can also be hazardous if it is not limited to use, as in the case of not being contained personal data because there is no obligation in the positive law that in detail govern and sanctioned against violations. Such hazards may arise from:

- a. the theft of personal data
- b. damage to the system that may allow the occurrence of data breaches (including personal data)
- c. misuse of personal data that has been ruled business itself, or other parties who may access personal consumer data (such as government).

The need to set this up is important because private data is a person's privacy right. Still, it can fundamentally be economically valuable for a third party who is about to take advantage of it. It is contrary to the concept of martial arts in attitudes and behaviours of citizens that are outlawed by his love for unitary State of Republic of Indonesia based on Pancasila and the Indonesian Constitution 1945 in establishing the survival of the nation and the whole nation.

The danger of the legal absence void on the personal data protection will be very detrimental to consumers, because of threats from the breach in addition to the negligence. That can be caused by the lack of a personal data protection system initiated by the fintech sector business or threats from the alleged business people or workforce in the fintech business sector who intend to break personal data for particular interests. These risks can make Fintech in Indonesia get the insufficient predicate of countries that already have more capable personal data protection regulations and from consumers and prospective consumers of fintech services.

The most prominent and first deeds must be governed by the Parties Agreement (consent) relating to the submission of data. To fulfil the principle of consensually in all the necessary alliance settings about it as the most fundamental payload material. It must be determined that the personal data that has been taken from the consumer. The personal data must first be preceded by a deal that should be made in written form, explicitly stated, and made a digital signature or signature as a means of proof that the consumer has knowingly approved his data to be processed by business actors. The authors assess it to make it easier to prove the dispute later. The agreement must also clearly determine the purpose for which the personal data has been provided so that it can only be used or allowed to be limited to a mutually agreed-upon goal and not for any other purpose. In other words, the use is solely for the purpose that directly relates to the function of the employee and the processing of such data only. The agreement must also contain clauses stating and binding the perpetrators not to provide or sell the personal data of fintech consumers to other businesses, or other third parties is prohibited.

Conclusion

The arrangement of personal data protection in national law is regulated explicitly in the regulation of the Minister of Communication and Information Regulation number 20 the year 2016, and which in any case was born to weigh the need for official rules regarding the protection of personal data to enforce. The provisions of article 15 paragraph (3) Government regulation number 82 the year 2012, where it was only based on ITE Act that is still unclear and not information regarding the protection of personal data in electronic commerce.

References

- Chalton, Simon. 2001, *A Specially Commissioned Report the Legal Protection of Databases*, Thorogood, London
- Corte, L.D. (2020). *A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection*. In D. Hallinan, R. Leenes, S. Gutwirth & P. De Hert (Eds.). *Data Protection and Privacy: Data Protection and Democracy (Computers, Privacy and Data Protection)*, pp. 27–58). Oxford: Hart Publishing. Retrieved May 21, 2020
- Davison, Mark J. 2003, *The Legal Protection of Databases*, Cambridge University Press, New York
- Departemen Perlindungan Konsumen. 2017, *Perlindungan Konsumen Pada Fintech Kajian Perlindungan Konsumen Sektor Jasa Keuangan*, Departemen Perlindungan Konsumen. Jakarta.

- Derclaye, Estelle. 2007, *The Legal Protection of Databases a Comparative Analysis*, Edward Elgar Publishing Limited, USA
- Hallinan, D. *Data Protection without Data: Could Data Protection Law Apply without Personal Data Being Processed?* European Data Protection Law Review Volume 5, Issue 3 (2019), pp. 293 – 299
- Indriyani, Masitoh et al., *Perlindungan Privasi Dan Data Pribadi Konsumen Daring Pada Online Marketplace System*, Justitia Jurnal Hukum Volume 1 No.2, Oktober 2017
- Ketaren, Eliasta. 2016, *Cybercrime, Cyber Space, Dan Cyber Law*, Jurnal TIMES, Vol. V No 2: 35-42
- Peeters, J. *Data Protection in Mobile Wallets*, European Data Protection Law Review, Volume 6, Issue 1 (2020), pp. 56 – 65
- Purtova, N., *The law of everything. Broad concept of personal data and future of EU data protection law*, Law, Innovation and Technology Volume 10, Issue 1, 2 January 2018, pp. 40-81
- Raharjo, Agus, 2001 *Cybercrime; Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Cetakan I, PT Citra Aditya Bakti, Bandung
- Renouw, Dian Mega Erianti, 2017, *Perlindungan hukum e-commerce: perlindungan hukum pelaku e-commerce di Indonesia, Singapura, dan Australia*, Yayasan Taman Pustaka
- Rossi, A., & Palmirani, M. (2020). *What's in an Icon? Promises and Pitfalls of Data Protection Iconography*. In D. Hallinan, R. Leenes, S. Gutwirth & P. De Hert (Eds.). *Data Protection and Privacy: Data Protection and Democracy (Computers, Privacy and Data Protection)*, pp. 59–92). Oxford: Hart Publishing. Retrieved May 21, 2020
- Sitompul, Asril, 2004, *Hukum Internet (Pengenal Mengenai Masalah Hukum di Cyberspace)*, Cetakan II, PT. Citra Aditya Bakti, Bandung
- Suharnoko, 2004, *Hukum Perjanjian: Teori dan Analisa Kasus*, Kencana, Jakarta
- Susanto, Happy, 2008, *Hak-Hak Konsumen Jika Dirugikan*, Visi Media, Yogyakarta
- Tamò-Larrioux A. (2018) *Privacy and Data Protection Regulation in Europe*. In: *Designing for Privacy and its Legal Framework*. Law, Governance and Technology Series, vol 40. Springer, Cham
- Widodo, Suwarno, *Implementasi Bela Negara Untuk Mewujudkan Nasionalisme*, Jurnal Ilmiah CIVIS, Volume I, No 1, Januari 2011
- Yuking, Ana Sofa. 2018, *Urgensi Peraturan Perlindungan Data Pribadi dalam Era Bisnis Fintech*, Jurnal Hukum dan Pasar Modal.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).