



Internal Security as a Guarantee of Personal Data Protection in E-Commerce Systems for Consumers

Merlin Swantamalo Magna^(✉) and Alfayza S. P. Pratama

Department of Demography and Civil Registration, College of Vocational Studies, Universitas
Sebelas Maret, Surakarta, Indonesia
merlinmagna@staff.uns.ac.id

Abstract. The rapid development of information and communication technology, the rapid growth of the economy, with the current globalization altogether has expanded the transaction space to be diverse. One of the innovations in making transactions today is the existence of electronic commerce or commonly referred to as e-commerce. People in different parts of the world can make easier transactions for goods and services just by relying on the internet network. Seeing the increasing number of internet users, of course this makes electronic transactions more attractive to the public because it is considered easier and more practical. However, over time, various complaints arise from consumers who like to make electronic transactions because of the ease of e-commerce, it turns out that the security of personal data of millions of users is under great threat due to weak regulations covering this issue. The research aims to understand the urgency of personal data protection as part of the human rights of e-commerce users and how procedures should be carried out and showcases the effects of strict criminal laws that must be taken to take action in the event of a leak of user data.

Keywords: E-Commerce · Internal Security · Personal Data Protection

1 Introduction

E-commerce is defined as buying and selling transactions made using the internet network, conducting e-commerce transactions for buyers and sellers can save costs and time. Despite providing significant benefits, e-commerce or known in Indonesia's positive laws with commerce through electronic systems still has loopholes against violations of the right to use privacy as a consumer and minimal protection of personal data is a right to privacy. There are no specific regulations regarding the right to privacy or protection of personal data [1]. The right to privacy over personal data is something that must be protected in electronic activities, one of which is e-commerce, because in addition to being everyone's privacy, personal data is also an asset or commodity that has high economic value.

The concept of consumer protection is commonly used to classify measures that seek to ensure that consumers are treated fairly and that their rights are protected in

commercial transactions involving the supply of goods or services. People are worried that their personal data is being leaked and used by irresponsible parties. Reflecting on the current situation and the lack of regulations that support the protection of e-commerce consumers' personal data, this is one reason for authors to research about the legal protection of personal data as a right to privacy of e-commerce consumers.

In this study, the authors will focus on two issues. First, what is the conception of personal data, which is the right to privacy for consumers in e-commerce transactions? Second, how does the legal construction of personal data protection law as the privacy of e-commerce consumers? Given that in Indonesia there is no personal data protection law that specifically regulates and this causes a legal vacuum and also the absence of legal certainty to address legal issues related to the personal data of the Indonesian people. So starting from this issue, the author was moved to examine the legal issue to examine this legal issue in relation to the tendency of legal vacancies regarding compensation for losses suffered by consumers in the event of negligence made by e-commerce platforms, which led to the leakage of consumers' personal data which is a right to privacy. Consumers as users of e-commerce services. The research aims to understand the urgency of personal data protection as part of the human rights of e-commerce users and know the construction of personal data protection laws, which are privacy rights.

2 Research Methods

In line with the description in the introduction, the author uses normative juridical methods, namely by examining library materials or secondary data that includes primary and secondary legal materials. In this study, the authors used the statutory approach, which is an approach used by examining all laws and regulations relating to legal issues or issues to be discussed. In this study, the author used the method of library research by making an inventory of laws and legal literature. Efforts are made to obtain secondary data in the form of primary and secondary legal materials with documentation studies, namely by studying or critically examining legal documents that have relationships with legal issues regarding protection. Laws on personal data, which is the right to privacy of e-commerce consumers.

3 Results of Discussion and Research

3.1 Self-protection of Personal Data Protection for Consumers in E-Commerce Transactions

In online transactions, it is very important to pay attention to the extent to which consumers can be accessed by the protection of personal data. Issues of protecting consumers' personal data will also arise in payment mechanisms in particular: i) how to determine which party is responsible for the use and management of consumer payment information; ii) the identities of the parties should not be able to use anonymous identities; iii) how such payment information should be retained and not disseminated to third parties [2]. In electronic transactions, it is very important to pay attention to the extent to

which consumers can be personally protected because now almost all online transactions always access consumer personal data for marketing and advertising purposes through various ICT advances.

Transaction security is absolutely necessary to ensure the security of consumers' personal data such as information about credit card numbers, password numbers or other personal identities misuse by unauthorized persons. According to the Norton Cyber security Insight Report, the average global lost cyber user is nearly \$358 per person or about a total of \$150 billion a year. Research obtained in 17 countries shows that cyber-crime has increased and Indonesia is one of the most vulnerable cybercrime countries. Different characteristics in the trading system through electronic technology have not been covered, but it is necessary to make legal regulations regarding *cyberlaw* including about *e-commerce* so that the rights of consumers as users of electronic technology in the trade process, especially in conducting *e-commerce* transactions can be guaranteed [3].

Regulation on the protection of personal data in Indonesia in this digital platform is needed because given the progress of the times, where data storage and data processing have used digital systems, there are indeed some laws and regulations that also regulate personal data, but this is just a regular rule, not a special regulation, and also this data protection is in personal regulation number 20 of 2016 on the protection of personal data, However, there is no criminal penalty for individuals who misuse and disseminate Indonesian personal data on digital platforms. In addition, the Indonesian government has also prepared eight priorities in the development of e-commerce in Indonesia in accordance with Presidential Regulation No. 74/2017 on the National Electronic Based Trading System Roadmap [4]. Discussion of personal data protection is one of the priorities related to consumer protection. Many parties are encouraging the government to immediately prepare, the Draft Law on Personal Data Protection, which will become a *lex specialis* for the protection of consumer personal data in Indonesia [5].

3.2 Personal Data Protection Act as a Right to Privacy for E-Commerce Consumers

There are many cases of personal data problems that occur in Indonesia. One real example of a breach of consumer personal data is seen from the case between PT Tokopedia and the Indonesian Consumer Community, which is listed in the list of cases number 235 / Pdt.G / 2020 / PN Jkt. Pst. From the cases that have been mentioned, there is a weak and lack of protection of personal data on digital platforms where the data that must be stored is kept secret by business actors, both private companies and state-owned enterprises. As also mentioned in the Regulation of the Minister of Communication and Informatics of the Republic of Indonesia Number 20 of 2016 on The Protection of Personal Data in Electronic Systems Article 2 paragraph 1 which is titled as follows "Protection of Personal Data in Electronic Systems includes the protection of acquisition, collection, processing, analysis, storage, appearance, announcement, transmission, dissemination and destruction of Personal Data." In addition, the public also has the right to the confidentiality of their personal data. It is contained in Article 26 letter a for the belief of their Personal Data; Then in Article 27 the letter of business actors or parties who use personal data must maintain the confidentiality of personal data from clients or their

people, which states as follows “maintaining the confidentiality of the Personal Data they obtain, collect, process and analyze”.

Regulation of the Minister of Communication and Informatics of the Republic of Indonesia Number 20 of 2016 on Protection of Personal Data in Electronic Systems only states the rights and obligations of personal data owners (people) and users (Business Actors). However, there is no penalty for users who misuse people’s personal data. Data protection can essentially relate specifically to privacy as allan Westin, who for the first time defined privacy as the right of a group or institution’s individual, to Determine whether information about them will be communicated or not to other parties, so it is called *information privacy* because it concerns personal information [6]. Westin’s opinion is understandable that personal data needs to be protected because personal data is part of an individual’s privacy, so that the owner of the personal data itself is determine whether his or her personal data may be accessed and known by others or not.

The Banking Law (Law No. 10/1998), regulates among other things problems related to bank secrecy based on the principle of confidentiality, which requires banks to keep everything related to data and information about customers confidential, both financial situation and personal information. In Article 1 paragraph (28) of the Banking Law, bank secrecy is interpreted as everything related to the deposit of customer information and deposits. Thus, the principles of trust and confidentiality as the basis of the performance of financial institutions are also applied in the relationship between customers and banks. Customers in storing or using other bank products must provide personal data as deemed necessary to the bank. In the context of trade, in addition to talking about electronic transactions, which are regulated by the ITE And PP PSTE Law, personal data protection is also closely related to Law no. 8/1997 on Document Companies, Law no. 8/1999 on Consumer Protection, and Law no. 7/2014 on Trade. Unfortunately, the Consumer Protection Act does not specifically mention the protection of personal data, as part of consumer rights, which must be protected by business actors. The Consumer Protection Act emphasizes the availability of accurate information for consumers (related to goods and services), provided by businesses. Even so, the Trade Law does not specifically regulate the obligation to protect personal data (consumers). However, in the provisions of Article 65 paragraph (3) of the law it is emphasized that in trading using electronic systems (e-commerce), every trade actor must fully refer to the provisions of the applicable ITE Law. This means that the provisions regarding the protection of personal data also bind any trade using electronic systems. Therefore, the establishment of government regulations on trade through electronic systems mandated by Article 66 of the Trade Law must also regulate the protection of consumers’ personal data, with reference to existing laws and regulations, especially the ITE Law and the Consumer Protection Act. Law No. 8 of 1999 is no longer appropriate in providing legal protection in the digital economy and must be updated immediately by implementing a comprehensive regulatory model taking into account the architecture of the digital economy relating to juridical and non-juridical factors.

The Indonesian government is preparing a bill on the protection of personal data, the material of which more or less adopts the principles in *the EU GDPR* described by Berend van der Eijk in his presentation on the principle of transparency: that citizens have the right to access, change and delete their personal data at any given time from

the company's customer data [9]. There are three important principles in privacy: i) *right to be alone*, which is the basic principle of one's privacy; ii) the personal data of a person to which the personal data is written by other people such as medical records, tax information, insurance information and so on; iii) privacy over communications made by someone online, so that under certain conditions Interception of electronic communications can be categorized as a violation of the right to privacy [9].

The principle is tried to be outlined in the PDP Bill consisting of 15 Chapters and 74 Articles, including regulating from general provisions, types of personal data, personal data owners' rights, processing of personal data, obligations of controllers and processors of personal data in the processing of personal data, transfer of personal data, prohibition of the use of personal data, establishment of a code of ethics for personal data controllers, exceptions to protection. Personal Data, Dispute Resolution, International Cooperation, Community Role, Criminal Provisions, Transitional Provisions, and Closing Provisions.

The Indonesian government itself has delivered digital economic growth targets until 2020 and one of the problems that must be set by the government is the protection of consumers in the digital economy by paying attention to government regulations on trade transactions through electronic systems; harmonization of regulations; system of payment of trade and spending of government goods/services through e-commerce; and the gradual development of national payment gateways [11].

Author's Contribution. Merlin Swantamalo Magna, S.H., M.H.

Alfayza Sabila Putri Pratama.

The authors shown in parantheses contribute greatly to the following research tasks: conceived and designed analysis (M.S.M); data collection and analysis (M.S.M., A.S.P.P.), data collection (A.S.P.P.), data analysis and interpretation (M.S.M., A.S.P.P.), writing and revising papers (M.S.M., A.S.P.P.).

Confession. The author would like to thank God Almighty, thanks to His abundant grace this article can be made, to the lecturers of the Faculty of Law of Sebelas Maret University who have provided understanding in compiling this article, and to the Faculty of Vocational School, Universitas Sebelas Maret, in particular.

References

1. Warren, S., & Brandheis, L.D. (1890). Right to privacy. Harvard Law Review (4) 5, 193-220 DOI: <https://doi.org/10.2307/1321160>
2. Rosadi, S.D. (2018). Protecting Privacy on Personal Data in the Digital Economy Era: Indonesia's Legal Framework. Journal of Brawijaya Law (5) 1, 143-157 DOI: <https://doi.org/10.21776/ub.blj.2018.005.01.09>
3. Wulandari, Y.S. (2018). Legal Protection for Consumers against E-Commerce Transactions. ADJUDICATION: Journal of Legal Sciences Vol 2 No. 2, 199–210
4. Djafar, W (2019). Personal Data Protection Law in Indonesia: Landscape, Urgency and Need for Updates. The paper was delivered as material in a public lecture "Legal Challenges in the Era of Big Data Analysis", Post-Graduate Program of the Faculty of Law, Universitas Gadjah Mada, Yogyakarta, August 26, 2019
5. Sukmadilaga, A., & Rosadi, S.D. (2020). Legal Efforts Against Violations of Internet of Things (IoT) Implementation in the Field of Health Services According to Personal Data Protection Provisions, Journal of Voice of Justice, Vol. 2 No. 2 October 2020 Issue, 205–221

6. Westin, Alan F., (1967). *Privacy and Freedom*. London: Atheneum Press.
7. Benuf, K., Mahmudah, S., & Priyono, E. A., (2019). Legal Protection of Financial Technology Consumer Data Security in Indonesia. *Reflection on Law: Journal of Legal Sciences* Vol. 3 No. 2 April 2019 Edition, 145–160
8. Rongiyati, S. (2019). Consumer Protection in E-Commerce. *Journal of The State Of Law: Building The Law For Justice and Welfare* Vol 10 No. 3, 1-25
9. Niffari, H. (2020). Protection of Personal Data as Part of the Human Right to The Protection of Personal Data (A Comparative Review of the Laws and Regulations of Other Countries.) *Juridical Journal* (7) 1, 105–119 DOI: <https://doi.org/10.35586/jjur.v7i1.1846>
10. Priscyllia, F. (2019). Protection of Personal Data Privacy Legal Comparative Perspective . *Jatiswara Jurnal* Vol 34 No. 3 November 2019 Edition, 239–247
11. Pudhail, M., & Baihaqi, I., (2017) *Indonesia's Digital Economy Ecosystem Development Strategy*. Vidya: Scientific Journal Vol. 25 No. 1 June 2017 Issue. 69–85

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

