International Journal of Arts and Social Science www.ijassjournal.com
ISSN: 2581-7922
Volume 5 Issue 6, June 2022.

The Concept of Personal Data Protection in Law Number 19 of 2016concerning Amandments to Lawno. 11 of 2008 Concerning Information and Electronic Transaction

Nabih Amer, Nur Mohamad Kasim, Mohamad Syafri Pautina

Faculty of Law, Universitas Negeri Gorontalo, Indonesia)

ABSTRACT *:The digital penetration caused by the current of digitization gives birth to new capacities to acquire, store, manipulate and transmit data in real time, extensive and complex. Providing protection for the right to privacy means providing protection for the right to freedom of speech. That is, the right to privacy guarantees protection from the threat of fear to do or not to do something which is a human right. The problems that are wanted in this journal, are as follows: 1).What is the meaning of personal data protection in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions?, 2).Are the provisions contained in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions adequate in providing protection for people's personal data?This study uses a normative legal method through a statutory approach and this journal analysis uses a qualitative method. The results of this study indicate that the current protection of personal data in Indonesia is still not sufficient to protect the Indonesian people as a whole. The current concept still has many weaknesses in several parts, such as the lack of accommodation for "consent" and the government's classification of forms of cyber crime which still seem abstract..*

Keywords : *Personal Data Protection, Privacy, Consent*

I. INTRODUCTION

Protection of personal data in Indonesia in general has been contained in the 1945 Constitution of the Republic of Indonesia.In particular, Article 28 G paragraph 1 states that "Everyone has the right to personal protection, family, honor, dignity and property under his control, and has the right to a sense of security and protection from the threat of fear to do or not do something which is the right basic". [1]

The digital penetration caused by the current of digitization gives birth to new capacities to acquire, store, manipulate and transmit data in real time, extensive and complex. This triggers the collection of various data, no longer depending on the consideration of what data might be useful in the future.

Personal data is one of the most widely circulated in the electronic world due to its use by almost all software used by society today. Examples of this use we can find on social media platforms (such as Meta, Instragram, Tiktok, Twitter, and others) that are commonly used by the community, where as a condition for using this service, each individual must include relatively complete personal data.Personal information such as full name, place and date of birth, telephone number, etc. This poses a threat of massive and sporadic circulation of personal information.

The lack of regulations related to the protection of personal data, causes the security of users of these digital platforms to be vulnerable. Indonesia has actually regulated the protection of personal data, but these regulations are still incomplete and the existing rules only explain the protection of personal data in general.

Providing protection for the right to privacy means providing protection for the right to freedom of speech. That is, the right to privacy guarantees protection from the threat of fear to do or not to do something which is a human right. Indonesia has now entered the era of the Industrial Revolution 4.0. Everything can be controlled from anywhere through the internet and connected devices.The implications of this can be seen clearly in people's daily lives, for example in increasing work productivity, building socio-economic relations, and helping to make things easier. These conveniences come with new threats in the form of eavesdropping, misuse, illegal sale of personal data and various other cyber crimes.[2]

As explained above, the regulation of personal data in Indonesia is still very minimal in providing regulations regarding the protection of personal data, and it causes many problems in the cyber world. The emergence of many cases of misuse of personal data has forced the government to immediately form special regulations regarding this matter. The Personal Data Protection Bill (PDP) itself has actually been discussed since 2012. This regulation regulates starting from the definition, type, ownership rights, processing, transmission, and the authorized institution that regulates personal data to the sanctions that will be imposed.

Regarding the prevention of personal data theft through penal facilities, namely by giving rewards to perpetrators of using or exploiting personal data without permission. Article 26 of the ITE Law requires that any use of personal data on an electronic platform must first obtain the approval of the owner of the data concerned. Anyone who violates this provision can be sued for the losses caused. The provisions of Article 26 of the ITE Law are as follows:[3]

1. Unless otherwise stipulated by laws and regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned..
2. Any person whose rights are violated as referred to in paragraph 1 may file a lawsuit for the losses incurred under this law.
3. Each electronic system operator is obliged to delete irrelevant electronic information and/or electronic documents that are under his control at the request of the person concerned based on a court order..
4. Each electronic system operator must provide a mechanism for deleting irrelevant electronic information and/or electronic documents in accordance with the provisions of laws and regulations. 5. Provisions regarding procedures for deleting electronic information and/or electronic documents as referred to in clause (3) and (4) are regulated in government regulations.

In connection with the above, it appears that the regulation regarding personal data contained in the ITE Law is not yet complete. Especially regarding what personal data should be protected, what personal data is considered sensitive data. This is further complicated by the evidentiary process in the courts in Indonesia, which makes it difficult for data owners to legally question allegations of theft of personal data or leakage of personal data.

Furthermore, the ITE Law itself does not have a special content that regulates personal data. With the misuse of personal data, it appears the weakness of the current system, lack of supervision, so that personal data can be misused and result in losses for the owner of the data. Wiretapping, theft, illegal sale of personal data is a violation of the law in the field of information technology and can also be categorized as a violation of the law in the field of information technology and can also be categorized as a violation of human rights, because personal data is part of human rights that must be protected.[4]In this regard, there are several examples of cases of misuse of personal data, including:

1. Copying of customer's ATM card data and information (skimming), where skimming perpetrators withdraw customer funds freely.

2. Illegal data sales carried out by irresponsible websites.
3. Protection against data leakage that has not been maximized from digital service providers.

Based on the problems above, the researcher wants to study about "The Concept Of Personal Data Protection In Law Number 19 Of 2016ConcerningAmendmentsTo Law No. 11 Of2008 ConcerningInformationAndElectronicTransaction".

II. RESEARCH QUESTION

Based on the explanation above, the formulation of the problem set by the author is as follows:

1. What is the meaning of personal data protection in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions?
2. Are the provisions contained in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions sufficient in providing protection for the public's personal data?

III. RESEARCH METHOD

This study uses a normative legal method through a statutory approach. So that it can include research on systematics, level of synchronization, history, and comparison of legal materials in the form of laws and regulations as basic reference material in this research. This journal analysis method uses qualitative methods that refer to legal norms contained in legislation and court decisions as well as norms that live and develop in society.

IV. DISCUSSION

Protection Of Personal Data In Law No. 19 of 2016 Concerning Amendments To Law No. 11 of 2008 Concerning Information And Electronic Transactions.

Protection of personal data in Article 26 clause (1) of Law no. 19 of 2016 is one part of personal rights (privacy rights). It is further explained that personal rights have the following meanings:[5]

a. Personal rights are the rights to enjoy a private life and be free from all kinds of interference.
b. Personal rights are the rights to be able to communicate with other people without spying.
c. Privacy rights are the rights to monitor access to information about a person's personal life and data.

Based on the principles described above, in Article 26 of Law No. 19 of 2016 the government has put in place the basis for protecting the public's personal data, as follows:[6]

(1) Unless otherwise stipulated by laws and regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned..
(2) Any person whose rights are violated as referred to in paragraph (1) may file a lawsuit for the losses incurred under this Law.
(3) Each Electronic System Operator is required to delete irrelevant Electronic Information and/or Electronic Documents under its control at the request of the Person concerned based on a court order.
(4) Every Electronic System Operator is required to provide a mechanism for deleting Electronic Information and/or Electronic Documents that are no longer relevant in accordance with the provisions of the legislation.
(5) Provisions regarding the procedure for deleting Electronic Information and/or Electronic Documents as referred to in paragraph (3) and paragraph (4) shall be regulated in a government regulation.

Based on what has been explained above, it appears that the protection of personal data is not yet maximal and capable. This can be seen in Article 26 paragraph 3 of Law no. 19 of 2016 which still requires each individual to request that their data be deleted by an electronic service provider company must attach a court

order. Meanwhile, according to Erna, the concept of data protection implies that individuals have the right to determine whether they will share or exchange their personal data or not.[7]Thus, should matters relating to personal data, each individual must have free control over their own personal data without requiring approval from other parties regarding what they want with their own data.

Regarding the above, Elettra also argues that: *"the notion of consent is tradittionally linked with the idea that is the data subject should be in control of the use that is being made of hisdata".*[8] Which means that each individual must know in full about everything that is done by the digital service provider to his personal data. When a digital service provider asks for an individual's consent, it aims to give the individual a will over his/her personal data, as well as give a will to the data management practice of the digital service provider.

Furthermore, oriented to the United Kingdom General Data Protection Regulation (UK-GDPR) defines consent as follows:"*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*Furthermore, Article 5 Paragraph (1) of the UK-GDPR stipulates five (5) principles of eligibility for how personal data should be processed, including: a). Legitimacy, fairness and transparency; b). Goal limitation; c). Data Minimization; d). Accuracy; e). Storage Limits; f). Integrity and confidentiality (security); g). Accountability.[9]

Based on what has been said above, these principles are then further elaborated, as follows:[10]

a) Processed lawfully, fairly and transparently in relation to individuals;
b) Collected for a specific, explicit and legal purpose and not further processed in a way that is inconsistent with that purpose; further processing for archival purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be deemed incompatible with the original purpose;
c) Adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;
d) Accurate and, if necessary, continuously updated; every reasonable step should be taken to ensure that inaccurate personal data, taking into account the purpose for which it was processed, is deleted or corrected without delay;
e) Kept in a form that permits identification of the data subject no longer than is necessary for the purpose of processing personal data; personal data may be retained for a longer period to the extent that personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes subject to the application of appropriate technical and organizational measures required by the GDPR to protect individual rights and freedoms;
f) Processed in a manner that ensures the appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Thus, regarding the protection of personal data "consent" is something that is inherent and absolute and is accompanied by clear and accountable real protection. In addition, protection must also be provided by providing limitations for digital service providers to process the personal data of each individual. This is because consent is something that is common sense or there must be something about personal data protection. This shows that in this case the concept of legal protection in Indonesia currently does not place this as an important matter by attributing other parties to the freedom to use each individual's personal data.

Provisions In Law Number 19 of 2016 Concerning Amendments To Law Number 11 of 2008 Concerning Information And Electronic Transactions In Providing Protection For Public Personal Data.

In order to create a safe digital environment for the people of Indonesia, the government has actually tried to formulate steps to make this happen. This is reflected in Article 31 of Law no. 19 of 2016, as follows:[11]

(1) Any person intentionally and without rights or against the law intercepts or intercepts Electronic Information and/or Electronic Documents in a certain Computer and/or Electronic System belonging to another person.
(2) Every Person intentionally and without rights or against the law intercepts the transmission of Electronic Information and/or Electronic Documents that are not public from, to, and within a certain Computer and/or Electronic System belonging to another Person, whether not cause any changes or cause changes, removal, and/or termination of Electronic Information and/or Electronic Documents that are being transmitted.
(3) The provisions as referred to in paragraph (1) and paragraph (2) do not apply to intercepts or wiretapping carried out in the context of law enforcement at the request of the police, prosecutors, or other institutions whose authorities are determined by law..
(4) Further provisions regarding the interception procedure as referred to in paragraph (3) shall be regulated by law.

Furthermore, Article 40 of Law No. 19 of 2016 also provides obligations for the government in more detail regarding the protection of people's personal data, as follows:[12]

(1) The government shall facilitate the utilization of Information Technology and Electronic Transactions in accordance with the provisions of the laws and regulations.
(2) The government protects the public interest from all kinds of disturbances as a result of the misuse of Information and Electronic Transactions that disrupt public order, in accordance with the provisions of laws and regulations.

(2a)The government is obliged to prevent the dissemination and use of Electronic Information and/or Electronic Documents. invitation.

(2b)In carrying out the prevention as referred to in paragraph (2a), the Government is authorized to terminate access and/or instruct the Electronic System Operator to terminate access to Electronic Information and/or Electronic Documents which have unlawful contents.

(3) The government stipulates agencies or institutions that have strategic electronic data that must be protected.
(4) The agency or institution as referred to in (3) must make Electronic Documents and electronic backup records and connect them to certain data centers for data security purposes..
(5) Institutions or other institutions other than those stipulated in clause (3) make Electronic Documents and electronic back-up records in accordance with their data protection needs.
(6) Further provisions regarding the role of the Government as referred to in clause (1), clause (2), clause (2a), clause (2b), and clause (3) shall be regulated in a government regulation.

Based on what has been explained above, the current regulations provide an explanation regarding the things that must be done to protect people's personal data circulating in the cyber world. However, this does not specifically regulate more specific cases. As in Article 40 clause (2) where government protection is related to the misuse of information and electronic transactions that disturb public order, where the phrase disturbing public order does not have a clear classification of what is considered disturbing public order.

In addition, in an effort to protect personal data, the government should also accommodate matters relating to a person's personal interests. In fact, the majority of things related to personal data security breaches often intersect with someone's security. Therefore, more emphasis should be placed on protecting the interests of an individual. According to Acquisti:"*In an information society the self is expressed, defined, and affected through and by information and information technology. The boundaries between private and public become blurred. Privacy has therefore become more a class of multifaceted interests than a single, unambiguous concept.*"[13]Therefore, privacy has become more of a diverse interest class than a single,

unambiguous concept. So that in protecting personal data, the government as a regulator who is responsible for the people he leads must be able to provide clear boundaries regarding the boundaries between things that are private and public. This is to establish clearer and stronger protection for the community.

V. CONCLUSION

The current protection of personal data in Indonesia is still not sufficient to protect the Indonesian people as a whole. The current concept still has many weaknesses in several parts, such as the lack of accommodation for "consent" and the government's classification of forms of cyber crime which still seem abstract.

RECOMMENDATION

The government should pay more attention to important details in the protection of personal data. Strengthening the "consent" of individuals in the digital world, as well as a clear classification of electronic crimes. This is important in order to create a safer cyber environment for every community and can create a safety net for the community.

REFERENCE

Journal Papers:

[1] Saragih, L. K., Budhijanto, D., & Somawijaya, S. (2020). *Perlindungan hukum data pribadi terhadap penyalahgunaan data pribadi pada platform media sosial berdasarkan undang-undang republik indonesia nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elek. De rechtsstaat, 6(2),* 125-142.

[2] Hadita, C., Glugur Darat, I. I., Timur, M., & Medan, K. (2018). *Registrasi Data Pribadi melalui Kartu Prabayar dalam Perspektif Hak Asasi Manusia. Jurnal HAM Vol, 9(2),* 191-204.

[4] Kesuma, A. N. D. H., Budiartha, I. N. P., & Wesna, P. A. S. (2021). *Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial Dalam Transaksi Elektronik. Jurnal Preferensi Hukum, 2(2),* 411-416.

[7] Priliasari, E. (2019). *Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online*. *Majalah Hukum Nasional, 49(2),* 1-27.

[8] Bietti, E. (2020). The Discourse Of Control And Consent Over Data In Eu Data Protection Law And Beyond.

[13] Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (pp. 21-29).

Legal Product

[3] Undang-undang Nomor. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

[5][6][11][12] Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

[9][10] UK-GDPR