Journal Equity of Law and Governance
Vol. 2, No. 1, April 2022, 31-35
P ISSN: 2775-9512
https://www.ejournal.warmadewa.ac.id/index.php/elg

Legal Protection on Data Transmission Through the Digital Short Message Platform

Evelyn Angelita Pinondang Manurung*
Eka Ayu Purnama Lestari
Institut Bisnis Dan Teknologi Indonesia
***inboxevelyn@gmail.com**

Published: 01/04/2022

Manurung, E. A. P. & Lestari, E. A. P. (2022). Legal Protection on Data Transmission Through the Digital Short Message Platform. *Journal Equity of Law and Governance*, *2*(1), 31-35.

ABSTRACT - Digital media is currently utilized by the entire community because it has provided its own space digitally for its users to move in terms of communication and various activities. Especially in terms of communication today people prefer digital media / platforms in sending short messages for information or data delivery activities. The ability to send fast, easy and equipped with service features as per the needs of its users becomes an effective choice for the public in using digital short message platforms. The use of digital messaging platforms today also makes people begin to realize the importance of security in data transmission. The high activity of people who send personal data through digital platforms must also be balanced with the level of security and confidentiality of data on the platform. This research aims to find out the legal protection arrangements in the delivery of data through digital messaging platforms so that the wider community understands security and data protection. This research uses normative juridical research methods using the legal sources of literature. The wider community today sees the number of cases of data violations / misuse through digital messaging platforms is clear evidence that personal data is a human right of digital platform users that must be protected. Therefore, it is necessary to have legal tools that can accommodate the form of laws to ensure the security and protection of personal data.

Keywords: digital media, data transmission, legal protection, digital message platform

I. INTRODUCTION

The development of technology has had a very significant impact on social life, especially on the speed of internet connectivity. This also has implications for accessibility related to the technological advances that raise questions about the right of individuals to maintain the confidentiality of some information. Easy and fast dissemination of information through technology creates a threat to privacy by providing big opportunities for those who access personal information (Mangku et al., 2021).

The use of digital short message platforms that are rife today certainly changes people's communication patterns in sending information. The use of the internet with digital platforms by the people of Indonesia is felt almost all sectors of community activities, especially in sending messages in the form of data or information that has an effect on the smoothness of community activities. According to the results of a survey of internet users in Indonesia in 2020 reached 78.18 percent, the growth of internet use in households was followed by the growth of the population using mobile phones in 2020 reached 62.84 percent (*bps.go.id*, 2020).

Privacy and personal data are important in digital transactions. Privacy and personal data are important because users in the network will not make a digital transaction if they feel the security of their privacy and personal data is threatened (Rosadi & Pratama, 2018). In line with the openness of digital platforms in accessing data and information, the protection of data and information is also something that needs to be realized and protected. Here are some understandings of data including:

1. Data is any information processed through a functioning device that automatically responds to instructions given for its purpose and stored with a view to being processable (UK Data Protection Act 2018).
2. According to webster New World Dictionary, data is things known or assumed, which means that the data of something is known or considered (Situmorang et al., 2010).
3. Personal Data is certain individual data that is stored, maintained, and maintained by truth and protected confidentiality (Regulation of the Minister of Communication and Informatics Number 20 of 2016 Article 1 paragraph 1).

In the development of technology and personal data information consisting of names, residential addresses, electronic mail addresses, mobile phone numbers are very valuable data because there is economic value obtained in the business world with that data. The use of data through the delivery of digital short messages is of particular concern. Many data breaches occur due to poor implementation or lack of security controls both among users and even third parties. Many countries are trying to improve security requirements and implement them in their laws. However, most security frameworks are reactive and do not address relevant threats (Park & et. al., 2018).

II. METHODS

The issues that will be discussed in this study related to the title of the study then this research is carried out using normative legal research methods using normative juridical approach methods. Normative legal research is one type of legal research methodology that bases its analysis on applicable and relevant laws and regulations. Normative juridical approach method is an approach that refers to applicable laws and regulations (Sunggono, 2003).

III. RESULT AND DISCUSSION

3.1. Data as a Right to Privacy

The digital era as a sign of technological progress in parts of the world has given rise to the growth of the use of digital platforms for almost all urban communities. One of the habits of urban society is to communicate with digital platforms that rely on internet networks. From the habits of urban communities that prioritize effectiveness and time efficiency, their communication patterns are formed on digital short message platforms. The platform is used as the most effective and efficient means of communication. WhatsApp, Telegram, Messenger or digital social media platforms that provide short message features such as Facebook, Instagram, and others are some examples of digital messaging platforms that have become an important part of the digital activities of the global community lately. Not only messages sent through the digital platform, but personal data is not infrequently sent to fellow users of digital platforms.

Utilization of technology and information can be felt the benefits related to the development of science, science and so forth that can easily be accessed, so that information can be received quickly. In the field of work, the management of a lot of data can be managed properly, quickly, effectively and efficiently and minimize errors. In the field of economy, promotions and potentials in improving the welfare of the community are carried out quickly without restrictions on places or regions and reach all levels of society both nationally and internationally. However, the development of technology and information not only provides benefits but also causes problems that can harm society, such as data misuse, theft of personal data, sale of personal data, fraud and others (Situmeang, 2021).

According to Law Number 11 of 2008 on Information and Electronic Transactions, Article 26 paragraph (1) in general, personal data is defined as highly personal information stored for

oneself, or at least only known to people on a limited basis. Personal data itself is part of a person's right to oversee access to information about his personal life and data.

The pace of development of the technology industry today makes the public more sensitive to the importance of maintaining the confidentiality of their personal data/information from various threats of data breaches and misuse. Today data is an important element about a person's identity that is a major need in activities in digital media. Call it the function of data is in the registration process to get digital platform services by filling in a personal identity that unwitting data controllers or digital service providers may not be able to guarantee the security of personal data. It is almost inevitable that digital platforms have become an important medium in the routine activities of the wider community.

The protection of data privacy as part of respect for the right of privacy must be started by providing legal certainty. Guarantees for the protection of privacy data must be placed in the highest legal instrument that has the highest power, namely the constitution, because the Constitution is the highest legal instrument in a country. Legal certainty (the principle of legality) is necessary and cannot be ruled out in the framework of law enforcement by each country. The state's step in providing legal certainty is to establish and guarantee these rights in the constitution, then through the instrument the character of a state will be able to be seen about what is put forward, what legal system is used and how the regulation of its government will be seen (Natamiharja & Mindoria, 2019). Each individual is entitled to his or her or her personal rights including data. As an inherent right to the person, the debate over the importance of protecting the right to one's privacy first surfaced in court rulings in the United Kingdom and later in the United States (Djafar, 2019).

3.2. Protection Regulations in Data Transmission

The urgency of data/information protection should be the main legal protection related to the data/personal information of individuals or groups of individuals transmitted through digital platforms. In Indonesia in the constitution of the Constitution of the Republic of Indonesia 1945 actually recognizes the right to the personal self-protection of its citizens which is stated in Article 28 letter G, namely "*Everyone is entitled to the protection of personal self, family, honor, dignity, and property under his control, and entitled to a sense of security and protection from the threat of fear to do or not do something that is a human right*". The article affirms that the state guarantees the right and protection of the privacy of its citizens.

The emergence of cases of data breaches or misuse in various countries triggers many countries to create security regulations to protect the personal data/information of their citizens. With the disquiet of various countries in Europe about the protection of citizens' data, countries that are members of the European Union make a regulation on data protection called *The EU General Data Protection Regulation* (*The EU GDPR*). The EU GDPR is to protect the human rights of citizens in today's digital age. GDPR is seen as a solution to the protection of public data on the internet, thus encouraging data controllers (such as social media) to be more vigilant in protecting data belonging to data subjects (Tommy Kurnia, 2018). Here are some of the rules contained in The EU GDPR that state protection against the transmission of user data: (a) Chapter II Article 9 (1): "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*"; (b) Chapter III Section 3 Article 17: "*The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies*"; (c) Chapter III Section 5 Article 23 number 2 (d): "*the safeguards to prevent abuse or unlawful access or transfe*r".

The article affirms the prohibition on disclosing all data/information related to the identity of race, ethnicity, religion, beliefs, biometric data, data or health data of the data owner. The owner of the data/information must be asked for prior approval if the data/information is to be processed. In line with that in article 17 of The EU GDPR, the data owner is entitled to his data to be deleted in its entirety without delay by the data controller (digital service provider).

If the owner of the data deposits his data on a site platform (digital service provider), then the platform is obliged to delete all user data. Thus, the service provider or digital platform can not store the data of users who no longer use the digital service. The data owner also has the right to get confirmation of his data history/information. As the purpose of data management in regulations is the case if user data is sent to third parties or international organizations, then the data owner is entitled to information.

As a country with a society that is active in digital activities, Singapore has regulations regarding data protection listed in the *Personal Data Protection Act* (PDPA). The regulation or law becomes the legal umbrella for data protection in the private sector. The PDPA regulates the parties involved to comply with the Act in the management and processing of data. In the PDPA explained about the protection in the transmission of personal data to other parties, namely contained in Chapter VI of Personal Data Protection: Article 24. *An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent: a. unauthorised access, collection, use, disclosure, copying, modification ordisposal, or similar risks; and b. the loss of any storage medium or device on which personal data is stored*. The article affirms that there is a definite security guarantee to prevent unauthorized access to collection/copying. Likewise, in Article 26 (1) i.e. *An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act*. The article states a prohibition on transferring any personal data to territories outside Singapore to ensure the existence of standards of protection against personal data transferred as stipulated in the Act.

If compared with in Indonesia that in Indonesia there are regulations that generally regulate data protection in the process of sending/transferring/transmitting data including The Minister of Communication and Informatics Regulation No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems: (a) Article 2 verse 1. *Protection of Personal Data in Electronic Systems includes protection against the acquisition, collection, processing, analysis, storage, appearance, announcement, delivery, dissemination, and destruction of Personal Data*; (b) Article 2 paragraph 2 letter; (b) *Personal Data is confidential in accordance with the consent and/or based on the provisions of the laws and regulations*; (c) Article 21 paragraph 1 letter a. *Displaying, announcing, sending, disseminating, and/or opening access to Personal Data in electronic systems may only be done with consent unless otherwise specified by the provisions of the laws and regulations*. In the above articles it is explained that the process of sending data/information is protected or protected but has not specifically emphasized the protection of individual privacy and there is no certainty of consent if the data is transmitted or disseminated to third parties. Likewise, with the consent given by the rightful owner of personal data regarding the correctness of the personal data in his possession. Digital platforms as digital service providers are also considered to have an obligation to store and manage a person's personal data as it relates to the confidentiality and security of every citizen.

Considering the above it is appropriate for Indonesia to have a Law on data protection to ensure the security, convenience and rights of users of digital messaging platforms in carrying out their activities. Looking at the current situation in Indonesia, the regulation of data protection is still in the form of a Draft Law on Personal Data Protection where arrangements regarding the protection of data transmission by users of digital messaging platforms and digital service providers are seen to have been regulated in such a way, including: (a) Article 4. *The Owner of Personal Data reserves the right to request information about the clarity of identity, the basis of legal interests, the purpose of the request and use of Personal Data, and the accountability of the party requesting the Personal Data*; (b) Article 13. *The Owner of the Personal Data has the right to sue and receive compensation for the breach of his Personal Data in accordance with the provisions of the laws and regulations*; (c) Article 47. *Personal Data Controllers who transfer Personal Data and who receive transfers of Personal Data are obliged to protect Personal Data as referred to in this Act*; (d) *Article 48 paragraph 3. In the event that the Controller of Personal Data in the form of a legal entity dissolves or dissolves,*

the storage, transfer, deletion, or destruction of Personal Data is carried out in accordance with the provisions of the laws and regulations; (e) Article 48 paragraph 4. *Storage, transfer, deletion or destruction of Personal Data as referred to in paragraph (3) notified to the Owner of personal data*.

Some of the above articles state that personal data transmitted to data controllers is protected by the Act as well as the data management arrangements received by data controllers. If the Bill on Data Protection should be considered, the government should respond quickly that Indonesia must immediately have binding and comprehensive regulations on the protection of personal data.

Legal protection of security and confidentiality in the transmission of data through digital messaging platforms is very important because if misused or found to be a violation by a digital service provider or data controller or third party, it does not protect a person's right to a sense of security to his or her personal data/information. The fact that many cases of data breach or misuse through digital messaging platforms is part of the exploitation of personal data. Then it should also be followed by a legal umbrella to minimize violations, prevent misuse of data such as data leaks and can accommodate the digital activities and activities of Indonesian people.

IV. CONCLUSION

In Indonesia, the legal protection of data is not optimal, because it can be seen with the number of found misuse of personal data of someone who is transmitted/disseminated without knowing from the owner because there is no security and supervision system from the users or data managers. The absence of comprehensive regulation regarding data protection in the process of digital data transmission in Indonesia is the main reason for the many data breaches and abuses in this digital era. Likewise, the low knowledge/understanding of the wider community regarding privacy and protection of personal data. Similarly, regulations on data protection in Indonesia are still weak and still general because data protection arrangements are scattered in some regulations, which only describe the concept of personal data protection in general in PERMEN KOMINFO. Until now Indonesia still does not have a law on the protection of personal data, because the arrangement is still a draft of the Personal Data Protection Bill. Considering the many countries that already have and implement the Law on the protection of personal data, especially those governing data transmission, it is appropriate for Indonesia to also authorize and implement it, considering that Indonesians have mostly used digital platforms.

REFERENCES

Djafar, W. (2019). Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan. *ELSAM: Referensi HAM*.

Mangku, D. G. S., Yuliartini, N. P. R., Suastika, I. N., & Wirawan, I. G. M. A. S. (2021). The Personal Data Protection of Internet Users in Indonesia. *Journal of Southwest Jiaotong University*, *56*(1).

Natamiharja, R., & Mindoria, S. (2019). *Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN*. Project Report. Aura.

Park, S., & et. al. (2018). A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. *DFRWS 2018 Europe-Proceedings of the Fifth Annual DFRWS Europe*, *24*(Supplement), S93–S100.

Rosadi, S. D., & Pratama, G. G. (2018). Urgensi Perlindungan Data Privasi Dalam Era Ekonomi Digital di Indonesia. *Veritas et Justitia*, *4*(1), 88–110.

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*, *27*(1), 38–52.

Situmorang, S. H., Muda, I., Doli, M., & F.S., F. (2010). *Analisis Data Untuk Riset Manajemen Dan Bisnis*. Medan: USU Press.

Sunggono, B. (2003). *Metode Penelitian Hukum*. Jakarta: PT Raja Grafindo Persada.

