Legal Regulations on Personal Data Breaches in the Use of Social Media

Ni Komang Sutrisni
Faculty of Law, Universitas Mahasaraswati Denpasar, Denpasar, Indonesia
Kamboja street, No. 11, Denpasar, Bali, Indonesia
komangsutrisnifh@unmas.ac.id

Abdul Kadir Jaelani
Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia
Ir. Sutami street, No. 36 Kentingan, Jebres, Surakarta, Jawa Tengah, Indonesia 57126
jaelaniabdulkadir@staff.uns.ac.id

***Abstract*—In the 5.0 industrial revolution era, there are very efficient and effective changes or transformations in the digital market regarding technology and information. However, this can cause problems regarding personal data protection, especially in the use of social media. Therefore, there is a need for a study to optimize regulations regarding personal data protection for social media users. This research aims to understand the legal regulations on personal data protection for social media users and determine how to optimize personal data protection for social media users. The result of this discussion is, first, Article 26 Paragraph (1) of Law No. 19 of 2016 contains a norm that is unclear in meaning regarding the approval of legal protection for data owners whose data has been leaked. Second, the legal protection of social media users' personal data is not optimal, as evidenced by the numerous cases of leaked personal data. For that reason, there is a need to optimize efforts in personal data protection. The PDP Law mandates the establishment of an institution that serves as the spearhead in the implementation of personal data protection in Indonesia.**

***Keywords*—Legal Regulations; Personal Data; Protection; Social Media.**

I. Introduction

In this era of globalization and digitalization, many things are evolving, from the way humans transact to the communication conducted in cyberspace. The digital revolution has created an innovative capacity to acquire, store, manipulate, and transmit data volumes in real-time, extensively, and complexly.[1] With the numerous innovations present in this digital revolution era, it is seen as an advanced technological development that significantly impacts people's lives. Significant and rapid social changes have transformed human behavior globally due to the boundless nature of information and communication technology.

The evolving information technology makes various aspects of communication more accessible for humans. The rapid development of social media is marked by the emergence of various types of social media, such as Facebook, Twitter, Instagram, Line, and so on.[2] This can trigger a personal data leak. The issue of individual information leaks on the internet is becoming increasingly frequent, and there are various information leaks regarding the giant global industry. Information leaks have also occurred in Indonesia, with several accounts and individual consumer information being leaked through social media to e-commerce platforms. Unfortunately, the strengthening of laws regarding individual information leaks in Indonesia is very weak compared to those in other countries. This situation is at risk of individual information leakage issues repeatedly without legal reinforcement. [3] In 2018, there was a data leak of Facebook users worldwide. In Indonesia, the data breach of Facebook users reached 1,096,666 (one million ninety-six thousand six hundred sixty-six) users, or about 1.26% of the total leaked data. This number is significant, considering that the number of Facebook users in Indonesia is 130,000,000 (one hundred thirty million), or six percent of the total number of users worldwide.[4]

In the Republic of Indonesia, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (from now on referred to as Law No. 19 of 2016) Article 26 Paragraph (1) which regulates "Unless otherwise stipulated by law, the use of any information through electronic media that concerns a person's personal data must be done with the consent of the person concerned." In this article, it can be analyzed that every person who uses information on electronic media and is concerned about their data must have consent before doing so.

However, in the Republic of Indonesia Law Number 27 of 2022 on Personal Data Protection (hereinafter referred to as Law No. 27 of 2022) Article 23, which regulates "Contract clauses containing requests for the

A. K. Jaelani et al. (eds.), *Proceedings of the International Conference on Cultural Policy and Sustainable Development (ICPSD 2024)*,
Advances in Social Science, Education and Humanities Research 869,
https://doi.org/10.2991/978-2-38476-315-3_94

processing of Personal Data that do not include explicit valid consent from the Data Subject are declared null and void by law." This article underscores the need for personal data owners to take responsibility and provide explicit consent, a requirement that can prevent personal data leaks when using social media. With the advancement of technology, legal regulations regarding personal data breaches in the use of social media must be clarified so that personal data owners such as individuals, businesses, and the government clearly understand the laws governing personal data breaches. This falls into the category of normative ambiguity, which means that the norms or legal rules are unclear, ambiguous, or have multiple meanings. Therefore, the author wants to discuss the legal regulations regarding personal data breaches in social media usage, examined through the relevant legislation and literature review conducted by the author.

II. LITERATURE REVIEW

A. Personal Data

Personal data are a part of the data that resides on a computer or mobile device. According to the General Data Protection Regulation (GDPR), personal data are information about an identifiable individual. An identifiable person can be identified, directly or indirectly, by reference to an identification number or one or more factors specific to their physical, physiological, mental, economic, cultural, or other social features. Personal data that can be used directly to identify an individual can be categorized as Personally Identifiable Information (PII). Personally Identifiable Information (PII) may include name, date of birth, home address, gender, race, phone number, email address, political opinions, credit card number, health information, ID cards, IP address, and location data. Hence, personal data are the main asset for social media, because they can be used for business or other developer purposes. Personal data security protects personal data and information from unauthorized access, disclosure, disruption, deletion, corruption, modification, or destruction.[5]

As mentioned by Sylwia Kosznik-Biernacka, personal data should be protected and secured based on the CIA triad:

1. Confidentiality—The required degree of protection of the information against unauthorized access;
2. Integrity—Data and information should be correct, intact, and not be manipulated;
3. Availability—Data are available under the system or user requirements.

Related rules or regulations on personal data security are included in GDPR, a regulation in the European Union law on data protection and privacy in the European Union and the European Economic Area. Though it was initially published for the scope of the European Union and is one of the world's strictest privacy and security laws, the regulation has had influence and become an excellent reference for many organizations and countries worldwide. Some related standards discuss personal data security, such as which provides a way to protect valuable information using the base standard of ISMS (Information Security Management System), established by the ISACA (Information Systems Audit and Control Association), which provides guidance or a framework for managing enterprise information and technology that supports enterprise goal achievement.[6]

On 20th September 2022 in Indonesia, the UU PDP (*Undang-Undang Perlindungan Data Pribadi*), or local personal data protection law, was officially formalized. The UU PDP aims to protect Indonesia's citizens' data and sets a standard for legally processing and maintaining data. The UU PDP was drafted based on the reference to the GDPR.[7]

B. Characteristics of Social Media

Social media is an online medium where users can easily participate, share, and create content, including blogs, social networks, wikis, forums, and virtual worlds. Blogs, social networks, and wikis are the most commonly used forms of social media by people worldwide. Today's rapid development of social media is because everyone can have their own platform. If traditional media such as television, radio, and newspapers require large capital and significant labor, the situation is different with social media today. Social media users can take advantage of the internet network to use social media even if the access is slow, without significant costs, without expensive tools, and can be done independently without staff. Social media users are free to edit, add, and modify text, images, videos, graphics, and various other types of content.[8]

We can easily find many definitions of social media on the internet. However, upon further examination, we can find several common characteristics that a platform must possess to be categorized as a social media platform. The main characteristics that a social media platform must have include:

1. A User-Based Platform Before social media dominated the digital era, content spread on a site was one-way. Any changes or updates depended on one party, commonly known as the webmaster. However, the content spread on social media is entirely controlled by the platform's users.
2. Highly Interactive In every popular social media platform today, interaction between users becomes significant. The intensity of interactions that occur within a piece of content will be discussed in the section on indicators for assessing the success of a piece of content.

3. Users Are Content Creators As a user-based platform, each user controls the content contained within a social media platform. However, the type of content (text, images, videos, or audio) that can be posted on each platform differs.
4. Users Are Free to Determine Their Account Settings The account or page settings provided by each platform allow users to customize the interface and features they want to display.
5. Depending on the relationships between users and the communities that are formed, the more connections established between users on a social media platform, the greater the likelihood of interactions occurring, and the more communities will be formed based on the shared interests of each user.

In addition, social media also provides opportunities for nearly limitless connections. Social media allows users to connect with anyone, anywhere, and anytime. You could connect with an old friend or someone from a country you have never heard of or visited. Anyone can connect with anyone as long as they are connected to the internet.

III. METHOD

The research method used in this study employs a normative legal research type with the use of the Statute Approach, the Conceptual Approach, and the Comparative Law Approach. The sources of legal materials used are primary legal materials, secondary legal materials, and tertiary legal materials. The technique for collecting legal materials uses documentation studies with the snowball technique. The technique for analyzing legal materials uses descriptive, comparative, evaluative, and argumentative techniques.

IV. RESULTS AND DISCUSSION

A. The Ambiguity of Norms in Personal Data Protection Regulations

The rapid development of social media in this digital era, personal data owners who use or store their data on social media are at risk of personal data breaches. Data breaches are a serious issue that can cause financial losses, identity theft, and even further data misuse. The government, companies, and individuals need to raise awareness about data security and take appropriate preventive measures to protect personal data. The development of personal data protection laws has evolved alongside the advancement of technology itself, mainly information and communication technology. It cannot be denied that the rapid development of technology in the digital era today brings many positive impacts. However, behind all those advantages, people believe negative aspects accompany certain things. On one hand, technology can provide an extraordinary speed of information dissemination.[9]

However, on the other hand, the development of information technology has evolved into cybercrime. Data leaks have become one of the cybercrimes that have occurred in Indonesia. This can trigger a personal data leak. In 2018, there was a data breach of Facebook users worldwide. In Indonesia, this data breach affected 1,096,666 (one million ninety-six thousand six hundred sixty-six) users, or about 1.26% of the total leaked data. This number is significant, considering that the number of Facebook users in Indonesia is 130,000,000 (one hundred thirty million), or six percent of the total Facebook users worldwide. The Facebook data leak can result in criminal penalties. This issue arises because, in this case, Facebook tracks its users' activities and web activities.

In Indonesia, in the Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (from now on referred to as Law No. 19 of 2016), Article 26 Paragraph (1) regulates that "Unless otherwise stipulated by law, the use of any information through electronic media concerning a person's personal data must be done with the consent of the person concerned." In this article, it can be analyzed that every person who uses information on electronic media concerning their data must have consent before doing so. However, this article does not specify in what form the consent should be, whether written or unwritten. Therefore, this article can be considered a vague norm, which means there is ambiguity or lack of clarity in the legal norm or rule governing a matter because the article needs to specify the form of an agreement made when using information through electronic media. The form of an agreement can be categorized into two types: written and oral. The parties involved make a written agreement, which can serve as evidence of the agreement. In contrast, an oral agreement is made verbally by the parties, and it is more difficult to prove its legal strength if it is only made orally because there is no binding force on the parties if one party breaches the agreement.

If viewed from the Republic of Indonesia Law Number 27 of 2022 on Personal Data Protection (from now on referred to as Law No. 27 of 2022), Article 23, which regulates "Contract clauses that contain requests for the processing of Personal Data without the explicit valid consent of the Data Subject are declared null and void by law." So, this article states that the owner of a personal data needs explicit consent. That can invite personal data leaks when using social media. According to the Great Dictionary of the Indonesian Language, "explicit means clear, firm, straightforward, not convoluted (so that people can easily grasp the meaning and

do not have a vague or incorrect understanding of news, decisions, speeches, etc.); stated." So, in that article, the personal data owner needs explicit consent, but not all agreements in electronic media, including social media, can be made explicitly.

Furthermore, in Article 23 of Law No. 27 of 2022, the phrase "does not contain explicit valid consent" means that this article requires explicit valid consent from the personal data owner if they wish to agree. The Personal Data Subject is declared null and void by law without explicit valid consent. However, the author says this can invite personal data leaks when using social media. The explicit word that has meaning, which is stated, makes the personal data owner fill in, store, or share their data. We do not know whether electronic or social media will store the data well or use it for evil purposes, causing personal data leaks. This can invite personal data leaks when using social media.

So, from the author's analysis of Article 26 Paragraph (1) of Law No. 19 of 2016, it was found that the word "approval" in that article falls into the category of normative ambiguity with unclear meaning because this article does not specify in what form the approval should be, whether in written or unwritten form. If written, it can be used as evidence to obtain protection for leaked personal data, but what if the consent is not written? Indeed, the leaked personal data owner cannot claim their right to legal protection. It would be better if the person or authority responsible for amending the law could further clarify the meaning of the written approval in that article.

In this article, it can be analyzed that every person who uses information on electronic media and involves their data must have consent before doing so. However, this article does not specify in what form the consent should be, whether written or unwritten. Therefore, this article can be considered a vague norm, which means there is ambiguity or lack of clarity in the legal norms or rules governing a matter because the article does not specify the form of an agreement made when using information through electronic media.

B. Legal protection of personal data breaches for social media users

In line with the regulation of personal data protection in a specific law, namely the Republic of Indonesia Law No. 27 of 2022 on Personal Data Protection, it can be observed that there are several progressive aspects regarding personal data in Indonesia. It can be viewed from the perspective of legal politics, definitions, information, personal data processors, personal data controllers, and personal data subjects who are individuals and companies/legal entities. Thus, the legal politics in this regulation are evident in the government's active role, starting from regulation, storage, processing, and transfer to handling both preventively and repressively. It should also be noted that this is a regulation regarding personal data protection governed at the statutory level, so it is undoubtedly appropriate to immediately strive for its implementing regulations so that the protection mechanism becomes efficient.[10]

Substantively, one thing to pay attention to is the imposition of sanctions on specific activities that violate a person's right to personal data protection. This is outlined in Chapter XIII of the Personal Data Protection Law. However, upon observation, the type (offense) of the crime has yet to be specified in the sanction, whether it is a public offense or a complaint offense. It is logical to regulate explicitly in the law or its implementing regulations so that law enforcement agencies are evident later in their application. It can indeed be noted that this is closely related to the legal structure section, which will be discussed in the next section. Complaints or ordinary offenses deserve regulation, considering that personal data tends to be private, so it would be risky if they were regulated like ordinary offenses are for individuals or legal entities such as companies. A series of efforts aimed at providing understanding so that in the enforcement of this law, there is no fallacy of mind, even in actions.[10]

So far, regulations regarding personal data protection have been sectoral and governed in various fields related to implementing electronic systems. However, in this PDP Law, the parties involved in processing personal data are beginning to be identified, namely the data controller and the data processor. The data controller is any person, public body, or international organization that acts individually or jointly to determine the purposes and control personal data processing. Meanwhile, the data processor is any person, public body, or international organization that acts individually or jointly in processing personal data on behalf of the data controller. As part of the efforts in personal data protection, the PDP Law regulates every requirement that the personal data controller must fulfil. Among them, as regulated in Article 20, the personal data controller must have a basis for processing personal data. The controller must also process personal data in a limited and specific manner, legally and transparently, as regulated in Article 27. Article 36 regulates the obligation to maintain confidentiality, and Article 37 mandates supervision of every party involved in processing personal data under the control of the personal data controller.[11]

To optimize efforts in personal data protection, the PDP Law mandates the establishment of an institution that serves as the spearhead in implementing personal data protection in Indonesia. The institution is established and directly accountable to the president. This institution has the following duties: 1. Formulating

and establishing policies and strategies for personal data protection that serve as guidelines for personal data subjects, controllers, and processors; 2. Supervising the implementation of personal data protection; 3. Enforcing administrative law against violations of this law; 4. It is facilitating the resolution of disputes outside of court. In principle, the PDP Law aims to provide new hope for personal data security in Indonesia. The PDP Law has a stronger position than existing regulations that govern personal data protection, which are still sectoral and have a lower legal standing than laws. The PDP Law also provides a legal basis for broader personal data protection.

V. Conclusion

From the discussion that has been explained, it can be concluded that, first, Article 26 Paragraph (1) of Law No. 19 of 2016 contains a norm that is unclear in meaning regarding the approval of legal protection for data owners whose data has been leaked. Second, the legal protection of social media users' personal data is not optimal, as evidenced by the numerous cases of leaked personal data. For that reason, there is a need to optimize efforts in personal data protection. The PDP Law mandates the establishment of an institution that serves as the spearhead in the implementation of personal data protection in Indonesia.

REFERENCES

[1] N. P. N. Suharyanti, "Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat," *Pros. Semin. Nas. Fak. Huk. Univ. Mahasaraswati Denpasar*, vol. 1, no. 1, p. 122, 2020.

[2] L. K. Saragih and D. Budhijanto, "Perlindungan Hukum data Pribadi Terhadap Penyalahgunaan Data Pribadi Pada Platform Media Sosial," *J. Huk. De'rechtsstaat*, vol. 6, no. 2, p. 126, 2020.

[3] A. K. Sari, "Aspek Hukum Perlindungan Data Pribadi Sebagai Hak Privasi Pengguna Media Sosial," *J. Rectum*, vol. 5, no. Vol 5 No 1 (2023): EDISI BULAN JANUARI, 2023, doi: http://dx.doi.org/10.46930/jurnalrectum.v5i1.2856.

[4] M. B. Satrio and M. W. Widiatno, "Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Dara Pengguna Facebook di Indonesia)," *JCA LAW*, vol. 1, no. 1, pp. 49–50, 2020.

[5] N. Tskhovrebashvili, "Economic and Social Exchange of Personal Data and the Risks of Their Protection," *Vectors Soc. Sci.*, vol. 1, pp. 53–68, 2021.

[6] S. Kosznik-Biernack, "The Analysis of Risks to Personal Data Security," *Dimens*, vol. 34, pp. 256–267, 2020.

[7] Y. Kurniawan, S. I. S. R. R. W. N. Anwar, G. Bhutkar, and E. Halim, "Analysis of Higher Education Students' Awareness in Indonesia on Personal Data Security in Social Media," *Sustainability*, vol. 15, no. 4, 2023, doi: 10.3390/su15043814.

[8] T. H. Telaumbanua, D. Soeikromo, and D. S. S. Lumintang, "Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut Hukum Positif," *Lex Priv.*, vol. 131, no. Vol. 13 No. 1 (2024): Lex Privatum, 2024.

[9] K. R. A. Suari and I. M. Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," *J. Anal. Huk.*, vol. 6, no. 1, p. 134, 2023.

[10] M. Rifqy, H. Arham, and M. C. Risal, "Perlindungan Data Pribadi Bagi Pengguna Media Sosial," *J. Al Tasyri'iyyah*, vol. 3, no. 2, p. 109, 2023, doi: https://doi.org/10.24252/jat.vi.44108.

[11] B. K. Arrasuli and K. Fahmi, "Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi," *UNES J. Swara Justisia*, vol. 7, no. 2, p. 369, 2023, doi: 10.31933/ujsj.v7i2.351.