Legal Implications of Indonesia's Kominfo Data Leak Between Government Responsibility and Consumer Rights Protection

Ni Luh Wayan Yasmiati[1], I Dewa Gede Herman Yudiawan[2] Putu Fairnanda Sastra Devi[3], Jessica Carina Baptista Ferreira[4], Ni Nyoman Ayu Hari Savitri[5]

wayan.yasmiati@undiksha.ac.id[1] , idewa.gede.hermanyudiawan@undiksha.ac.id[2] fairnanda@student.undiksha.ac.id[3] jessica@student.undiksha.ac.id[4], ayu.hari@student.undiksha.ac.id [5]

Universitas Pendidikan Ganesha, Indonesia[1,2,3,4,5]

Abstract. The data leak of the Ministry of Communication and Telecommunication (Kominfo) inIndonesia has raised deep concerns regarding personal data protection and the government's responsibility in managing sensitive information. This issue is important to study because it hasa broad impact on public trust and data security in the digital era. This study aims to explore the legal implications of the Kominfo data leak, with a focus on government responsibility and consumer rights protection. The method used in this study is a qualitative normative method witha comparative approach. This study compares data protection regulations in Indonesia with the General Data Protection Regulation (GDPR) in the European Union, which is one of the strictestdata protection legal frameworks in the world. The GDPR provides high standards for personal data protection, including strong rights for individuals and strict obligations for data managers. This comparison aims to identify weaknesses in the Indonesian legal framework and provide recommendations for improving personal data protection in the country. The research findings show that the legal framework in Indonesia still has significant weaknesses in terms of data security and consumer rights protection. The implementation of stricter standards, such as those set by the GDPR, will help improve personal data protection and rebuild public trust. This studymakes an important contribution to understanding the challenges and opportunities in improvingpersonal data protection in Indonesia. It is hoped that the recommendations produced will help policymakers in formulating better regulations to protect consumer rights and ensure governmentaccountability in managing personal data.

Keywords: legal implications, data leaks, consumer rights protection, government accountability.

1 Introduction

Personal data security is an increasingly crucial issue in this digital era. The rapid developmentof information and communication technology has had a significant impact on everyday life, including in terms of storing and processing personal data. However, this progress is also accompanied by various challenges, one of which is the problem of data leakage. Data leakage not only harms individuals but has a broad impact on institutions and governments. In Indonesia, data leakage from the Ministry of Communication and Informatics (Kominfo) has become a serious public concern because it concerns the personal data of the wider community.

ICLSSE 2024, October 17, Singaraja, Indonesia

DOI 10.4108/eai.17-10-2024.2353731

The Kominfo data leak is not an issue that can be ignored, considering the role of Kominfo asan institution responsible for data and information management in Indonesia. This leak raises concerns about the extent to which the government can be trusted to protect the personal data of its citizens. From the research context, the legal responsibility of the Indonesian government in handling the Kominfo data leak becomes very important to analyze. This is because the data leak covers complex legal aspects, including aspects of personal data protection, public trust, and responsibility of government institutions to protecting sensitive information.

The government's legal responsibility includes a series of regulations and policies designed toprotect and ensure the privacy personal data of citizens. However, the data leak case involving the Kominfo shows weaknesses in the data security system, as well as the government's unpreparednessin handling such incidents. In recent years, a number of data leak incidents involving government institutions and private companies in Indonesia have revealed gaps in the data protection system, resulting in millions of Indonesians' personal data being exposed and vulnerable to misuse. The nomenclature regarding privacy can basically be found in the Criminal Code (KUHP) which contains several articles related to criminal acts, especially regarding privacy, such as the prohibitionon opening letters [1] and a ban on entering private land/property [2]. In this case of Kominfo data leak, the government is faced with the challenge of taking appropriate steps to address the issue, including identifying the cause of the leak, improving the data security system, and ensuring that similar incidents do not recur. In addition, it is important to review existing policies and regulations,and consider implementing stricter data security standards. This is closely related to the question ofhow the Indonesian government is legally responsible for handling the Kominfo data leak and to what extent such responsibility can be legally accounted for.

On the other hand, the issue of data leakage also touches from aspect all consumer rights protection. Especially in the economic sector, many business actors have started opening their businesses on the internet with all types of buying and selling transactions carried out online. With the presence of the internet and technological advances, it has encouraged the formation of e- commerce. E-commerce, according to Laudon J. and Laudon C, is defined as "a process of buying and selling products electronically by consumers from one of company to other company with computers as intermediaries for business transactions." [3]. However, it is also necessary to be awareof data security when conducting online transactions because data hacking crimes are very high. Consumers whose data is leaked experience losses that cannot be ignored, ranging from potential identity theft, misuse of data for illegal activities, to loss of privacy. Therefore, legal protection provided to consumers affected by data leaks is an equally important issue. The public has the rightto adequate legal protection to ensure that their rights are not violated and that they receive proper compensation for the losses they experience. In this context, it is necessary to evaluate the current legal protection mechanisms and the extent to which they are effective in providing protection to consumers.

The Personal Data Protection Law that has been implemented in various countries provides a good example of how to protect of personal data can be managed effectively. In Indonesia, regulations related to protect personal data are still in the development stage, and the Kominfo dataleak incident shows the importance of accelerating the implementation of stricter regulations. This is not only to protect consumer rights, but also to increase public trust in the government and institutions responsible for data management.

In addressing data leakage, a holistic approach is required, involving cooperation between governments, regulatory agencies, and private entities. This cooperation is essential to

make a safety environmental for personal data and ensure that data leakage does not become a persistent threat. The government needs to take initiatives to strengthen the legal framework, implement strict sanctions for violations, and raise awareness of the importance of data protection among the publicand companies. In addition, transparency in handling data leakage incidents is also important to rebuild public trust [4].

As the issue of the Kominfo data breach in Indonesia opens up an important discussion on thegovernment's legal responsibility and consumer rights protection, this paper will further examine thegovernment's legal accountability in the context of the Kominfo data breach and evaluate the legal protections provided to affected consumers. By understanding these two aspects, it is hoped that more effective policy recommendations can be developed to enhance data security and protect consumer rights in Indonesia.

2 Research Method

This research used normative qualitative method, which refers to legal principles and legislation related to consumer protection and data protection, as well as a comparison of regulations, including those that have been enacted and those that have not. In this research used problem approach includes a comparative approach that compares the existence of one or more variables in two different samples, as well as a case study approach. Data collection was carried out using the library research method.

3 Result and Discussion

3.1 The Legal Responsibility of the Indonesian Government

In fact, many victims in Indonesia have experienced cases related to personal data leakage. The confiscated personal data makes consumers worried, because it can be used by the perpetrators as a field of cyber crime. It is no wonder that the performance of (Kominfo), which is considered the most responsible for personal data leaks, has begun tobe questioned. The Indonesian government is obliged to ensure that all data management processes must adhere to security standards set by law, making it legally accountable in theevent of a data breach that harms consumers. This accountability includes the duty to safeguard personal data, take corrective action if a breach occurs, and enforce legal penalties against any parties found negligent or violating data protection regulations. In thisregard, the Ministry of Communication and Informatics (Kominfo), as a governmental body, is classified as a personal data controller in the category of public institutions. Thus,Kominfo bears significant responsibility to ensure the collection, storage, use, and deletionof personal data are conducted in strict accordance with the provisions outlined in Article 16 of the (PDP Law) [5]. As a controller of personal data, the Ministry of Communication and Information Technology must comply with data protection principles, such as transparency, security, and individuals' rights to their data, and is responsible for protecting the personal data it manages from misuse or violation of the law.

The Ministry of (Kominfo) is responsible for safeguarding consumers' personal data in Indonesia. Kominfo's obligations as the overseeing institution are outlined in Law Number 27 of 2022 on PDP. Article 58, paragraph 1, specifies that the Government has a role in enforcing Personal Data Protection in line with this law’s provisions [6]. This articlehighlights the government’s duty to ensure that personal data protection is implemented according to legal regulations. The government is responsible for setting policies, monitoring data protection practices, securing citizens’ personal data against misuse or unauthorized access,

addressing any violations, and raising public awareness on theimportance of personal data protection [7].

The government has the right and obligation to take action in the event of a violation related to consumer data leaks, such as personal data leaks in the Ministry of Communications, as the protection and control of personal data, the Ministry of Communications has the obligation and responsibility to immediately take appropriate action and in accordance with the provisions of the PDP Law Number 27 of 2022, the Ministry of Communications must also take steps to stop the leak and minimize its impact.Kominfo is also required by law to notify data subjects affected by data breach incidents and report them to the personal data protection authority (in this case, the PDP supervisoryauthority) within the legally specified time period as regulated in the PDP Law Number 27of 2022 in article 48 paragraph 1 states that what is meant by "notification" is to the Personal Data Subject or general notification through media, both electronic and non- electronic[8]. In the notification, whether through media or in writing, the data controller must include information about the type of data breached, the potential consequences, andthe steps taken to address the breach. Additionally, an investigation must be conducted to determine the reason behind the data breach and to put measures in place to avoid similar incidents in the future. If the investigation reveals that the breach was due to negligence ora violation of security procedures, Kominfo may be subject to administrative, civil, or criminal sanction in accordance with the provisions of the (UU PDP).

Such as Kemkominfo, fails to safeguard personal data, it may face sanctions depending on the severity of the violation and its impact. According to the (PDP) Law Number 27 of 2022, Article 57 paragraph 2, administrative sanctions in paragraph (1) may include: a) written warnings; b) temporary suspension of personal data processing activities; c) deletion or destruction of personal data; and/or d) administrative fines. In cases of data breaches in Indonesia, individuals responsible for data leaks may face criminal sanctions under relevant laws and regulations, particularly those regarding personal data protection. The main regulations governing criminal sanctions for data breach offenders include Article 67 paragraph (3) of the PDP Law, which states that anyone who deliberately creates false personal data or falsifies it for personal or others' benefit, potentially causing harm to others, can be sentenced to up to 6 years in prison and/or fined up to Rp. 6,000,000,000 (six billion rupiah) [9]. Additionally, in civil law, Article 26 of the ITE Law allows individuals to file a lawsuit if their personal data is obtained without consent [9]. These provisions aim to safeguard personal data and impose strict penalties on violators.

In the case of a personal data breach, the Ministry of Communication and Information Technology (Kominfo) and other central and regional government agencies managing Electronic-Based Government Systems (SPBE) or other public services are responsible for the failure to protect such data. This responsibility includes the obligation to promptly address the breach, inform the affected parties, and take steps to prevent similar incidents in the future. If negligence is proven, these entities can face sanctions inaccordance with applicable regulations. Furthermore, Article 12, paragraph 1 of the (UU PDP) stipulates that Data Subjects have the right to file a lawsuit and receive compensationfor violations of the processing of their personal data, according to the relevant regulations.Therefore, if consumer personal data is processed incorrectly or leaked, they can seek compensation for the resulting damages.

3.2 Comparison of the Indonesian Government's Legal Protection

In Indonesia, the act arrange about personal data legal protection of are carried out

separately, which have been regulated in regulations such as the 1945 Constitution of the Republic of Indonesia in Article 28 G which contains norms on the protection of personal data, as well as in the latest regulation, namely the rule Number 27 of 2022 aboutPersonal Data Protection (PDP) [5]. This regulation represents a significant advancementin Indonesia's data protection regime, aiming to centralize and standardize previously fragmented regulations.

The rule of PDP regulate designed to be more comprehensive and aims to align closely with the principles of the General Data Protection Regulation or GDPR. The PDP rules needs to be handled or managed. lawfully, in an equitable and transparent manner. The law grants the individual rights to access, correct, delete, and the handling of their personal information. Consent must be decidedly given and can be withdrawn at any time. Additionally, the law includes provisions for the sharing of data personal information abroad, ensuring that recipients of the data have adequate protection in place[6].

In the European Union, there is a similar regulation known as the General Data Protection Regulation (GDPR). This regulate that oversees the protection of information for individuals or residents of the European Union, both within and outside the EU, and applies to any entity managing such data, regardless of its location[7]. Both individuals and companies within the European Union, as well as foreign companies that collect and regulate data from EU residents, are subject to GDPR. This regulation applies universally to guarantee the protection of personal data irrespective of the location of processing or thelocation of the entity handling it.

In comparing data protection between Indonesia’s rules PDP and rules GDPR it is crucial to examine how these regulations are applied in real-world cases of data breaches. Example recent breach occurred on June 20, 2024, when the National Data Center (PDNS)was compromised by ransomware known as Brain Cipher. This attack affected 282 ministries, agencies, and local governments using PDNS, with 44 of these entities in the process of immediate recovery due to having backups. These incidents illustrate significantgaps in the implementation and efficacy of Indonesian data protection regulations compared toward the robust framework established by GDPR. They underscore the need for stronger regulatory measures, improved data security practices, and more effective response mechanisms to protect personal data and mitigate the impact of breaches [8].

The data leak at Kominfo, which involved millions of Indonesian citizens personal data, highlights significant shortcomings in the implementation and oversight of the regulate PDP , despite its enactment in 2022. This breach serves as evidence that Indonesia’s data protection system is not yet fully effective in preventing or responding to large-scale data breaches. According to UU PDP, data controllers are obligated to protect personal data and prevent unauthorized access. However, there has been a lack of prompt reporting and important action to address the breach within the timeframe set by the law. In contrast, the EU regulation GDPR require organizations report data breaches to the data protection authority within seventy two hours of discovering data leak, as outlined in Article 33 of GDPR. Failure to report within this timeframe lead in substantial fines, up to twenty million euros or four percent of the company's worldwide annual income, as specified in Article 85[9] of GDPR. This rapid reporting mechanism is designed to mitigate the impact of data breaches and provide timely alerts to affected users, a practice that has not yet been fully realized under UU PDP in Indonesia.

Additionally, the data breach at Kominfo highlights the need for stronger cybersecurity infrastructure, both within the government and the private sector in Indonesia. GDPR requires organizations to implement stringent cybersecurity standards and designate a

Data Protection Officer to manage and manage the data policies, the UU PDP in Indonesia has not yet widely mandated the appointment of a DPO, resulting in often poorly coordinated data security management as outlined in Article 53 of UU PDP.

4 Conclusion

The data leak that occurred at Ministry of Communication and Telecommunication highlights fundamental weaknesses in Indonesia's personal data protection system, despite the existence of the Personal Data Protection Law (UU PDP). This incident shows that Indonesia's cybersecurity infrastructure and law enforcement mechanisms are still inadequate to prevent or respond to data breaches effectively. In contrast, the GDPR in the European Union offers stronger and more coordinated protection standards, which can be used as a model for Indonesia. To protect consumer rights and restore public trust, Indonesia needs to immediately strengthen supervision, increase law enforcement capacity, and ensure that every institution that manages personal data is able to meet high security standards. Only with these steps can similar incidents be prevented in the future and personal data protection can be improved. The Ministry of Communication and Informatics (Kominfo) has a major responsibility to protect public data, including taking swift action in the event of a data breach, in accordance with the Personal Data Protection Law (UU PDP) No. 27 of 2022. In addition, the Government has an obligation to ensure data security, notify victims, and take steps to prevent similar incidents from happening again. Protection of consumer rights is also an important focus, ensuring that consumers receive adequate compensation if consumer data is misused. The success of personal data protection will increase public trust in the government.

References

[1] K. C. Laudon, J; Laudon, *Essential of Management Information System.* Prentice Hall, 1998.

[2] M. H. Putri, D. D. F., & Fahrozi, "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi," *Borneo Law Rev.*, vol. 5 (1), pp. 46–68, 2021.

[3] S. D. R. B. A. P. L. F. Djarwadit., "Analysis of the Indonesian Government' S Efforts," *Anal. Indones. Gov. Efforts Overcoming Public Data Leak Cases*, vol. 1, pp. 254–266, 2023.

[4] R. Mutiara, U., & Maulana, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi," *Indones. J. Law Policy Stud.*, vol. 1 (1), p. 42, 2020.

[5] J. O. Guswan Hakim, "Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa dan Indonesia," *Halu Oleo Leg. Res.*, vol. Volume 5, p. 445, 2023.

[6] S. J. Rizka Putri Awwaliyah, "Perbandingan General Data Protection Regulation (GDPR) dengan Regulasi Perlindungan Data di Negara - Negara Asia Tenggara," *JurnalHukumdanKewarganegaraan*, 2024.

[7] Syafira Agata Ramadani, "Komparasi Pengaturan Perlindungan Data Pribadi Indonesia dan Uni Eropa," *Rewang Rencang J. Huk. Lex Gen.*, p. 79, 2022.

[8] C. Indonesia, "Kominfo Klaim Hacker PDNS Belum Ancam Bocorkan Data Warga. Indonesia," 2024.

[9] C. Indonesia, "204 Juta Data Pemilih KPU Dibobol, Ancam Integritas Pemilu?," 2023. [Online]. Available: https://www.cnbcindonesia.com/tech/20231201110304-39- 493711/204-juta-data-pemilih-kpu-dibobol-ancam-integritas-pemilu