LEGAL BRIEF
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 13, No. 4, 2024, pp. 969-975
Published by: IHSA Institute (Institut Hukum Sumberdaya Alam)

General Election Commission's Responsibility for Personal Data Leaks in the Election Database System

Elza Armaini[1], Khalid[2]

[1,2] Prodi Ilmu Hukum, Fakultas Syariah dan Hukum, Universitas Islam Negeri Sumatera Utara, Medan

Abstract: This research is a type of normative legal research with the aim of the research being to find out howstate responsibility for leaks of public data in the election database system andwhat legal measures can be taken againstpublic data leaks in the election database system. The results of this study indicate that the KPU must be responsible for cases of leaks of public personal data, this is based on Article 47 of Law No. 27 of 2022 concerning personal data protection which states that managers of public personal data are responsible for errors or negligence that cause leaks of per-sonal data. In addition, this legal responsibility is also strengthened by the legal substance in Article 12 of the Law which states that the public is given the right to sue and receive compensation for violations of the management of personal data. Furthermore, based on the civil law aspect, the public also has the right to legal remedies in the form of lawsuits through legitimacy and non-legitimacy, this is based on the provisions of Article 1366 of the Civil Code which states that everyone has the right to be responsible not only for losses caused by their actions but also for losses arising from their negligence. So from this article it can be concluded that the case of per-sonal data leaks is a violation of negligence committed by the KPU which gives rise to legal re-sponsibility that must be resolved by the KPU.

Keywords: Legal Responsibility; KPU; Personal Data Protection.

1. Introduction

As a citizen, it has become a necessity to obtain rights in terms of protection in various aspects, especially for personal data, because personal data is a valuable asset for each individual, and can cause bad risks if misused, both for the individual himself or for the country where he lives (Saddam, Saddam, Saddam, & AliarahmanMoch, n.d.)(Asri, 2018). Constitutionally, Indonesia is a country that protects the privacy and data of its citizens, as stated in Article 28G paragraph (1) of the 1945 Constitution which reads: "Everyone has the right to protection of themselves, their families, honor, dignity, and property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a basic human right (Simamora, 2022), (Hilmi, 2022).

Personal data is related to the population context such as Name, Population Iden-tification Number (NIK), and Family Card (KK), and other data to be kept confi-dential (Djafar, 2019), (Siahaan et al., 2024). These data are very vulnerable to misuse in various contexts of activities/activities, such as illegal sales from one institution to an-other, in the field of research, even to monitoring activities or commonly known as es-pionage. This is also not possible in government institutions that manage citizens' per-sonal data, one of which is the state institution KPU RI which is a state institution that functions in organizing democracy in Indonesia (Fadhil, 2018), (MODUS & DI, n.d.).

The data leak incident began when an anonymous hacker named "Jimbo" claimed to have hacked the KPU website and obtained voter data. In his upload, it was revealed that of the 252 million data obtained, some were duplicated. The filtering produced 204,807,203 unique data. This figure is almost the same as the number of voters on the KPU's permanent voter list, which reached 204,807,222 voters from 514 districts and cit-

Correspondence:
Name: Elza Armaini
Email: elzaarmaini900@gmail.com

Received: Aug 30, 2024;
Revised: Sep 09 2024;
Accepted: Sep 24, 2024;
Published : Oct 30, 2024;

ies in Indonesia and 128 representative countries, related to information from two hundred million personnel data, including Population Identification Number (NIK), Family Card Number (NKK), Identity Card Number (KTP), Polling Station (TPS), e-KTP, gender, and date of birth. The data also includes data from the Consulate General of the Republic of Indonesia, the Embassy of the Republic of Indonesia, and the Consulate of the Republic of Indonesia (Michael & Rasji, 2024).

"Jimbo" shared 500,000 sample data that he managed to obtain through one of the uploads on the BreachForums site which is often used for buying and selling hacking results. He also shared several screenshots from the site https://cekdptonline.kpu.go.id/ to ensure the truth of the data obtained.In the upload, "Jimbo" also claimed to have found 204,807,203 unique data, a number almost the same as the number of voters in the KPU RI's permanent voter list (DPT) of 204,807,2003 voters. In the "leaked" data, "Jimbo" obtained personal data, such as NIK, KTP number, full name, gender, date of birth, place of birth, marital status, full address, RT, RW, to village, sub-district, and district codes, as well as TPS. The data was sold for 74,000 US dollars or around 1.1 billion (Mudjiyanto, Launa, & Leonardi, 2024), (Mudjiyanto & Roring, 2024).

Through this incident, it is only right that the General Election Commission (KPU) must be responsible for the leaked personal data of the public, because this is a mandate of Law No. 27 of 2022 concerning the protection of personal data in Article 39 paragraph 1 which states that personal data controllers are required to protect personal data from unauthorized processing (Priliasari, 2023), (Sirait, Ginting, & Ginting, 2023). Prevention as referred to in paragraph (1) is carried out by using a security system for personal data processed using an electronic system reliably, safely and responsibly (Barkatullah, 2019), (Aruan, 1911).

In addition, Article 26 of Law No. 19 of 2016 concerning electronic information and transactions has stated that anyone can file a lawsuit against the acquisition of personal data without their consent (Rumlus & Hartadi, 2020), (Sylfia, Amrullah, & Djaja, 2021). At least against violations of personal data protection can be sued as an Unlawful Act (PMH) on the basis of errors based on the provisions of Article 1365 of the Civil Code, or on the basis of impropriety or carelessness in Article 1366 of the Civil Code (Kusuma & Rahmani, 2022), (SUPRIYANTI, 2023).

Therefore, legal certainty and the responsibility of the KPU as the election organizer and person in charge of Personal Data Protection are urgent aspects in connection with the increasingly massive use of the internet and the rampant cases of data leaks (AHMAD, 2023), (Press, 2023). Thus, accountability for Personal Data leaks is a very important aspect to be further studied based on existing laws and regulations. This is to create legal certainty for the community as Indonesia's ideal as a country of law (ZELAFIARA, 2022), (Putra, Abdurrachman, & Hamzani, 2023).

Based on the above issues, it is interesting to conduct further studies to find out the process and legal certainty of the settlement which will be outlined through research entitled "Responsibility of the General Election Commission for Leaks of Public Data in the Election Database System Reviewed from the Civil Law Aspect".

2. Materials and Methods

The type of research used in writing this journal is normative legal research. Normative legal research is a type of legal research in which analyzing problems is carried out by means of library legal research which is carried out by examining library materials or from legal data sources originating from laws and regulations where law is conceptualized as what is written in laws and regulations. The data sources used by the author in compiling this scientific article are divided into two, namely Primary Legal Materials in the form of statutory regulations and secondary legal materials in the form of publications regarding laws that are not official documents.

3. Results and Discussion

3.1. General Election Commission's Responsibility for Public Data Leaks in the Election Database System

The KPU as a data controller is certainly obliged to prevent unauthorized access to Personal Data. This is in accordance with the provisions contained in Article 39 paragraph (1) of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). The prevention referred to in this case is by implementing a security system for Personal Data that is processed and/or processing Personal Data in an electronic system reliably, safely, and responsibly. There are several legal bases regarding the regulation of the General Election Commission's obligations to maintain and provide security guarantees for the personal data of the community that is managed, some of these regulations include.

a. The 1945 Constitution of the Republic of Indonesia

Implicitly, the right to privacy is contained in Article 28G paragraph (1) of the 1945 Constitution which states that everyone has the right to protection of themselves, their families, their honor, their dignity and their property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a basic human right. Based on these provisions, it is certainly clear that data controllers are required to make maximum efforts to prevent unauthorized things. These efforts can be made by preparing and implementing technical operational steps to protect Personal Data from interference with Personal Data processing that is contrary to the provisions of laws and regulations and determining the level of security of Personal Data by considering the nature and risks of Personal Data that must be protected in the processing of Personal Data.

b. Law Number 27 of 2022 concerning Personal Data Protection

Indonesia currently has special regulations governing Personal Data. Based on Article 1 paragraph (1) it states that what is referred to as personal data is data about an individual who is identified or can be identified individually or combined with other information either directly or indirectly through an electronic or non-electronic system. This law has become a new legal umbrella for society and the government to prevent and overcome crimes in the digital era such as theft of Personal Data. So that the leakage of Personal Data can harm the community both in material and immaterial forms. Therefore, there needs to be legal accountability for the leakage of Personal Data. Based on Article 47 of the Personal Data Protection Law, it states that the Personal Data Controller must be responsible for the processing of Personal Data and demonstrate accountability in fulfilling the obligation to implement the Personal Data Protection principle. In addition, the PDP Law also provides the public with the right to sue and receive compensation for violations of data processing carried out by the Personal Data Controller as regulated in Article 12 of the Personal Data Protection Law.

c. Law No. 24 of 2013 concerning Population Administration

In relation to personal data, there are laws and regulations that previously mentioned personal data, namely the Population Administration Law. Article 79 of this Law provides an obligation for the state to store and protect the confidentiality of Personal

Data and Population Documents. Personal Data and Population Documents are included in Personal Data, which data must be protected, stored, maintained and maintained for its truth and confidentiality. Personal data that must at least be protected is the Population Identification Number or NIK, address identity and individual identity which are clearly stated in Article 84 of this Law

The existence of these obligations and provisions requires the state to create prohibitions and sanctions for violators of population data management. In Chapter II concerning the Rights and Obligations of Residents, Article 2 of this law states that every resident has the right to obtain, among other things, protection from implementing agencies that misuse personal data or errors in the dukcapil registration system so that they can obtain compensation. If the application of criminal sanctions is deemed insufficient for law enforcement, there are sanctions in civil law, namely compensation.

3.2 Responsibility of the General Election Commission for Leaks of Public Data

Of course, through the incident of the leaking of personal data of the public managed through the KPU database system, it becomes a big problem regarding the security of personal data of the public managed by state institutions, one of which is the KPU. How can an institution that has reliable human resources and is supported by sophisticated technology, but can still be hacked by hackers. So from this incident it can be concluded that the cause of the leaking of personal data by the KPU database was due to the element of negligence of officers and the technology used by the KPU is still minimal in preventing hacking.

Through this incident, it is only right that the General Election Commission (KPU) must be responsible for the leaked personal data of the public, because this is a mandate of Law No. 27 of 2022 concerning the protection of personal data in Article 39 paragraph 1 which states that personal data controllers are required to protect personal data from unauthorized processing. Prevention as referred to in paragraph (1) is carried out by using a security system for personal data processed using an electronic system reliably, safely and responsibly. The forms of responsibility imposed by the KPU for leaks of personal data from the public in the election database system based on the Law include:

a. Investigation through the DKPP (Election Supervision Honorary Council) hearing

Article 1 paragraph (24) of the Election Law states that "The election organizers' honorary council, hereinafter abbreviated as DKPP, is an institution tasked with handling violations of the election organizers' code of ethics. In its structure, DKPP consists of 7 administrators, 1 person from the KPU element, 1 person from the Bawaslu element, and 5 people from community leaders. The DKPP management is directly inaugurated by the President.

In the case of personal data leaks by the KPU, the DKPP (Election Organizer Honorary Council) held a DKPP hearing and stated that the voter data leak showed that the KPU's information and technology security system, internet platform, and database were not secure, so it was very possible that data manipulation would be used to calculate the election results. Possible things that could happen include data manipulation, making fake ID cards, and voting at the last minute before the polling stations opened. Through this hearing, the DKPP only imposed sanctions in the form of warnings on the Chairman of the KPU RI Hasyim Asy'ari and the ranks of Commissioners.

The sanctions based on the Personal Data Protection Law are in accordance with those stated in Article 57 paragraph (2) which states that sanctions for failure of personal data controllers include written warnings, temporary suspension of personal data processing activities, deletion or destruction of personal data and/or administrative fines in the form of a maximum fine of 2 (two) percent of annual income or annual receipts.

Furthermore, evidence that the KPU is not responsible for the incident of the leaking of public personal data is that it did not carry out the order of Article 46 of the Law on Personal Data Protection which states that in the event of a failure to protect personal data, the personal data controller is required to provide written notification no later than 3x24 hours to the personal data subject and the institution. The written notification as referred to contains the personal data that was revealed, when and how the personal data was revealed and efforts to handle and recover from the disclosure of personal data by the data controller.

Through these provisions, it can be concluded that the KPU as the controller of personal data is obliged to inform the data subject or citizen of the hacking of their population identity. However, from the date of the hacking, which was known from October 2023 to May 2024, the KPU has never provided written notification to any data subject or data owner regarding the hacking that occurred.

b. Civil Liability

In the concept of civil law, at least violations of personal data protection can be sued as Unlawful Acts (PMH) on the basis of errors based on the provisions of Article 1365 of the Civil Code, or on the basis of impropriety or carelessness in Article 1366 of the Civil Code.Legal measures that can be taken againstPublic data leak in election database systempersonal data leaks, namely through the litigation process and the resolution of personal data leak disputes through non-litigation processes. Settlement of Personal Data leak disputes through the litigation process is the process of resolving personal data disputes through the court mechanism.

However, this responsibility emphasizes the responsibility to the government which in other words is called governmental liability, namely the state or government must provide compensation if there is a loss either directly or indirectly caused to citizens. The general understanding is that the government or government officials or other officials have an obligation to be responsible if there is a claim or lawsuit filed by a person or civil legal entity for fulfillment in the form of payment of money either in the form of subsidies or compensation, issuance, cancellation or revocation of decisions or regulations, and fulfilling obligations according to laws and regulations. Simply put, it can be interpreted as the government's obligation to provide compensation or damages due to its actions that harm the people.

Based on the theoretical study above, the researcher's analysis is that in the concept of civil liability, there must be a loss that must be detailed in material terms by the community who suffers a loss due to the leaking of their personal data. In addition, the concept of liability for compensation can be processed if there is a complaint and claim submitted through a district court or similar.

However, until now, no plaintiff or community has sued the KPU as the data controller, so the KPU is not burdened with the responsibility to compensate for the leak of personal data. However, researchers observed that the reason for the absence of lawsuits arising from the leak of personal data of the public in the election database system by the KPU is that no personal data owner or community knows from the leaked data the identity of who was included in the hacking because the KPU did not provide clear notification to the data subject, namely the public, about who the owner of the hacked data is, even though the notification is actually an order of the Law that must be carried out by the KPU.

4. Conclusions

Personal Data Leaks can harm the public in both material and immaterial forms. Therefore, there needs to be legal accountability for the occurrence of Personal Data leaks. Based on Article 47 of the Personal Data Protection Law, it states that the Personal Data Controller must be responsible for the processing of Personal Data and demonstrate accountability in fulfilling the obligation to implement the Personal Data Protection principle. Therefore, for the leak of Community data in the election database, the KPU is charged with the responsibility to accept all lawsuits arising from reports submitted by the Community.

The concept of civil liability requires that there be losses that must be detailed in material terms by the community that suffers losses due to the leaking of their personal data. In addition, this concept of liability for compensation can be processed if there are complaints and demands submitted through the district court or similar.

However, until now, no plaintiff or community has sued the KPU as the data controller, so the KPU is not burdened with the responsibility to compensate for the leak of personal data. However, researchers observed that the reason for the absence of lawsuits arising from the leak of personal data of the public in the election database system by the KPU is that no personal data owner or community knows from the leaked data the identity of who was included in the hacking because the KPU did not provide clear notification to the data subject, namely the public, about who the owner of the hacked data is, even though the notification is actually an order of the Law that must be carried out by the KPU.

References

AHMAD, M. (2023). TANGGUNG JAWAB HUKUM PENGENDALI DATA PRIBADI JIKA TERJADI KEBOCORAN DATA BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI.

Aruan, J. A. (1911). PERTANGGUNGJAWABAN HUKUM PENGELOLA SISTEM ELEKTRONIK KESEHATAN DI INDONESIA SEBAGAI PENYELENGGARA ELEKTRONIK SEHUBUNGAN DENGAN PERLINDUNGAN DATA. *" Dharmasisya" Jurnal Program Magister Hukum FHUI*, *1*(4), 20.

Asri, D. P. B. (2018). Perlindungan hukum preventif terhadap ekspresi budaya tradisional di Daerah Istimewa Yogyakarta berdasarkan undang-undang nomor 28 tahun 2014 tentang hak cipta. *JIPRO: Journal of Intellectual Property*, 13–23.

Barkatullah, A. H. (2019). *Hukum Transaksi Elektronik di Indonesia: sebagai pedoman dalam menghadapi era digital Bisnis e-commerce di Indonesia*. Nusamedia.

Djafar, W. (2019). Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. In *Seminar Hukum dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM* (Vol. 26).

Fadhil, A. S. (2018). Perlindungan hukum hak cipta sinematografi terhadap kegiatan download dan upload (telaah penerapan Undang-undang Nomor 28 Tahun 2014). Jakarta: Fakultas Syariah dan Hukum UIN Syarif Hidayatullah.

Hilmi, Z. (2022). KONSEP PERLINDUNGAN DATA PRIBADI DALAM PENGAWASAN PEMILU TAHUN 2024. *Jurnal Keadilan Pemilu*, *3*(1), 83–92.

Kusuma, A. C., & Rahmani, A. D. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). *SUPREMASI: Jurnal Hukum*, *5*(1), 46–63.

Michael, M., & Rasji, R. (2024). Analisis Yuridis Peristiwa Kebocoran Data Daftar Pemilih Tetap Dalam Penyelenggaraan Pemilihan Umum Tahun 2024. *Jurnal Ilmu Hukum, Humaniora Dan Politik*, *4*(4), 958–967.

MODUS, M., & DI, D. A. N. P. (n.d.). Untuk Memenuhi Persyaratan Memperoleh Gelar Magister.

Mudjiyanto, B., Launa, L., & Leonardi, A. (2024). Cybercrime, Perlindungan Data Warga Negara, dan Integritas Pemilu. *Oratio Directa (Prodi Ilmu Komunikasi)*, *5*(2).

Mudjiyanto, B., & Roring, F. P. (2024). Tendensi Politik Kejahatan Dunia Maya. *JIKA (Jurnal Ilmu Komunikasi Andalan)*, *7*(2), 26–51.

Press, U. G. M. (2023). *G20 di tengah perubahan besar: momentum kepemimpinan global Indonesia?* UGM PRESS.

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *12*(2).

Putra, T. W., Abdurrachman, H., & Hamzani, A. I. (2023). *Pertanggungjawaban Pidana terhadap Kejahatan Hacking*. Penerbit NEM.

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *Jurnal Ham*, *11*(2), 285–299.

Saddam, M. S. A. S. A., Saddam, A. S. A. S. A., Saddam, A. S. A. S. A., & AliarahmanMoch, A. S. (n.d.). "PERLINDUNGAN HUKUM TERHADAP PENGGUNA LAYANAN PENYELENGGARA SISTEM ELEKTRONIK AKIBAT PENYALAHGUNAAN DATA PRIBADI. Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta.

Siahaan, I. R., Sipayung, R. N., Lita, I., Naseela, Q. Z. I., Hanny, H., & Rakhmawati, N. A. (2024). ANALISIS PRAKTIK PERLINDUNGAN DATA PRIBADI PADA APLIKASI'SATUSEHAT'TERHADAP REGULASI HUKUM DI INDONESIA. *Jurnal Teknoinfo*, *18*(1), 141–150.

Simamora, I. M. M. (2022). Perlindungan Hukum Atas Hak Privasi Dan Kerahasiaan Identitas Penyakit Bagi Pasien Covid-19. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, *1*(7), 1089–1098.

Sirait, R. M., Ginting, R. F., & Ginting, C. D. B. (2023). Tantangan Hukum Penggunaan Data Biometrik Dalam Keperluan Bisnis. *Jurnal Konseling Pendidikan Islam*, *4*(2 Juli), 467–477.

SUPRIYANTI, N. (2023). PERLINDUNGAN HUKUM ATAS KERAHASIAAN DATA WAJIB PAJAK DALAM PROSES VALIDASI MELALUI E-PHTB NOTARIS/PPAT. Universitas Islam Sultan Agung Semarang.

Sylfia, A., Amrullah, M. F., & Djaja, H. (2021). Tanggungjawab Yuridis PT. Tokopedia atas Kebocoran Data Pribadi dan Privasi Konsumen Dalam Transaksi Online. *Bhirawa Law Journal*, *2*(1), 21–27.

ZELAFIARA, E. G. A. (2022). KEBIJAKAN FORMULASI TERHADAP KEBOCORAN DATA PRIBADI BERDASARKAN RANCANGAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI.