STATE RESPONSIBILITY FOR THE IMPACT OF RANSOMWARE ATTACKS ON THE TEMPORARY NATIONAL DATA CENTER (PDNS)

Setyo Utomo[1)]

[1]STIH Sumpah Pemuda, Jl. Sukabangun II No.2298, Sukajaya, Kota Palembang, Sumatera Selatan 30961
E-mail : doctorsetyojpu@gmail.com

Abstract

Indonesia as a country has a big task in protecting its people. The task of protection is embedded in the Preamble to the 1945 Constitution of the Republic of Indonesia as the nation's ideal. This protection is also carried out as an effort to guarantee the rights of the people (citizens), including personal rights and privacy. Recently, there has been a hacking of the National Data Center which resulted in a number of personal data of the community and important state data being leaked. This study aims to be a subject of in-depth study regarding the legal consequences of the data leak that occurred at the PDN RI. The formulation of the problem presented is how is the state's responsibility related to the leak of personal data at the National Data Center? The research method used is normative legal with a statutory, conceptual, and case approach. The results of this study indicate that the Government has absolute responsibility for data security at the PDN. The hacking of the PDN must be used as an evaluation by the Government of Indonesia in order to improve governance and superior IT-based human resources. Based on the legal provisions of the Personal Data Protection Law, the Government of Indonesia as the person responsible for the data can be subject to administrative sanctions.

Keywords: *national data center; ransomware; cyber attack;*

Abstrak

Indonesia sebagai sebuah negara memiliki tugas besar dalam melindungi rakyatnya. Tugas perlindungan ini tertanam dalam Pembukaan Undang-Undang Dasar 1945 Republik Indonesia sebagai cita-cita bangsa. Perlindungan ini juga dilakukan sebagai upaya untuk menjamin hak-hak rakyat (warga negara), termasuk hak pribadi dan privasi. Baru-baru ini, terjadi peretasan terhadap Pusat Data Nasional yang mengakibatkan sejumlah data pribadi masyarakat dan data penting negara bocor. Penelitian ini bertujuan untuk menjadi subjek kajian mendalam mengenai dampak hukum dari kebocoran data yang terjadi di PDN RI. Rumusan masalah yang diajukan adalah bagaimana tanggung jawab negara terkait kebocoran data pribadi di Pusat Data Nasional? Metode penelitian yang digunakan adalah hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Hasil penelitian ini menunjukkan bahwa Pemerintah memiliki tanggung jawab mutlak terhadap keamanan data di PDN. Peretasan PDN harus dijadikan evaluasi oleh Pemerintah Indonesia untuk memperbaiki tata kelola dan sumber daya manusia berbasis IT yang unggul. Berdasarkan ketentuan hukum Undang-Undang Perlindungan Data Pribadi, Pemerintah Indonesia sebagai penanggung jawab data dapat dikenakan sanksi administratif.

Kata kunci: *pusat data nasional; ransomware; serangan siber*

INTRODUCTION

Indonesia in its statement of the ideals of the formation of its nation in the Preamble to the 1945 Constitution of the Republic of Indonesia clearly states "protecting the entire

Indonesian nation..." Based on a contextual perspective, this protection is not only limited to physical protection. However, it is related to non-physical protection in the form of protecting the rights of citizens to ensuring the security of life. This spirit is related to the protection of the nation and its people which has become a primary national interest.

As a country of law, Indonesia places the law itself as the highest thing. This placement refers to the public as supreme and is then known as the supremacy of law (Samin, 2023). The implementation of the supremacy of law must not leave behind the three basic legal concepts, namely justice, benefit, and legal certainty. These three concepts must be reflected in the determination of policies or decision-making of all stakeholders in the Indonesian state.

The law is responsive, meaning it can adapt to new social needs in accordance with the times (Soemitro, 2020). The implementation of the law is indeed carried out rigidly, but the existing legal norms can be said to be flexible. Legal norms can change depending on the conditions of the times and the needs of society. The implementation of the change aims to create a situation that has legal certainty, the formation of orderly social institutions, and provisions that are not outdated.

This digital era opens up opportunities related to convenience and effectiveness. This cannot be denied because in the midst of the Industrial Revolution 4.0 era, the development of information technology is growing rapidly. This increasingly rapid development has spread throughout the world, including Indonesia (Mulyanto et al, 2024). The touch of information technology has entered into various aspects of life that cannot be separated, such as the encroachment of technology in the world of education, social, government, trade, and so on.

The development of information technology related to digitalization is also inseparable from the governance of the Indonesian Government. Currently, almost all ministries, institutions, and agencies carry out their governance using the help of information technology. In addition to keeping up with the times, the use of digital governance is related to the effectiveness, efficiency, and improvement of the quality of government management. This aims to realize Good Governance as expected by many people.

Along with the spirit of digital technology transformation carried out by the international world, the Indonesian Government has also renewed the governance of its

ministries and institutions with digitalization. The renewal was carried out through the Indonesian Ministry of Communication and Information together with stakeholders with a project output called PDN (National Data Center). This data center is a data integration program for ministries and institutions of the Indonesian Government for the management of data related to the placement, storage, and recovery of data used by central and regional agencies. This facility can be said to be important and vital for the country because this PDN can be said to be the main data of the Indonesian Government.

At the end of June 2024, the Indonesian Government announced that the National Data Center had experienced a cyber attack, resulting in a data breach. The ransomware cyber attack effectively paralyzed several service systems and performance systems of ministries or institutions whose systems were related to PDN. The ransomware attack used was the Brain Cipher Ransomware type, which is a new development of the Lockbit 3.0 ransomware (BSSN Legal and Communication Bureau, 2024). This cyber attack was exacerbated by the negligence of the Indonesian Government (in this case the Ministry of Communication and Informatics) which did not have a copy of the data (backup).

The biggest impact of the cyber attack on the National Data Center is the leaking of personal data of Indonesian people to irresponsible parties. This data leak incident is not the first time it has happened in Indonesia. Previously, there were leaks of Tokopedia data, BPJS data, BRI Life data, Bank Jatim user data, KPAI data, POLRI database, Indihome customer data, PLN user data, and several other cases. This strengthens Indonesia's position in the ranking of the number of cybercrime cases on an international scale, becoming the third highest in the world (Saly, 2023).

The many cases of data leaks in Indonesia should make the government improve itself. The personal data of the Indonesian people is a vital and important thing that needs to be protected. In terms of legislation, Law Number 27 of 2022 concerning Personal Data Protection has been issued. However, in practice, personal data protection can be said to be minimally implemented considering the many cases of data leaks in Indonesia. This creates a gap, where in the abstract view the personal data of the Indonesian people is protected. In fact, the Indonesian government still cannot carry out the mandate of the law regarding personal data protection.

The National Data Center leak is the peak of the Indonesian Government's failure to maintain people's personal data and their privacy rights. Another very concerning

impact is the disruption of public service processes and other government work programs that are directly related to the community. An example of this is the cessation of the Indonesian Ministry of Education and Culture's service system and the management of KIPK (Smart Indonesia College Card) and BPI (Indonesian Education Assistance) scholarship funds. This certainly causes great losses for the people, especially for the fate of their academic sustainability which depends on the Indonesian Ministry of Education and Culture's government program. The impact resulting from the data leak and the absence of data backup is a fatal mistake for the Indonesian Government.

The role of legal protection in theory and practice is the main topic that will be discussed in this study. National scale personal data leaks are a very fatal problem and have high urgency. Based on the background that has been explained, the formulation of the problem that can be taken is how is the state's responsibility regarding personal data leaks at the National Data Center?.

The purpose of compiling this research academically is for in-depth study material related to the legal consequences of data leaks that occurred at PDN RI. In addition, this research is a material for educating the public regarding cyber attacks that are included in cybercrime and the position of the case. The expected output is that the Government of Indonesia can better protect the personal data of its people and the public can be more careful regarding the use of information technology after the data leak at PDN RI.

RESEARCH METHODS

This research uses a normative legal research method (normative juridical). This method is used with the aim of producing new arguments, theories, or concepts as prescriptions in solving the problems faced (Marzuki, 2005). This research was conducted by examining library materials (secondary data) (Soekanto & Mamuji, 1995), which covers primary, secondary, and tertiary legal materials. The approaches used in this research are the legislative approach, the conceptual approach, and the case approach.

DISCUSSION

Chronology of the Ransomware Cyber Attack on the Indonesian National Data Center

Ransomware attacks targeting the National Data Center have put Indonesia in a state of cyber emergency. The attack has paralyzed 282 central and regional agencies in Indonesia. In addition, 47 Kemendikbud services were disrupted and KIPK scholarship applicant data was lost (Dwi, 2024). The National Data Center has an important role in the implementation of electronic-based government systems.

The National Data Center experienced its first cyber attack on June 18-19, 2024. This was based on digital forensics results and showed the addition of new users and attempted cyber attacks. Continuing until June 20, 2024, Directory Backup was disabled by a new user on PDNS 2. The ransomware was then actually executed on June 20, 2024 at 00.57 on the device backed up on PDNS 2 (Bestari, 2024).

Before the cyber attack occurred, on June 17, 2024 there were indications of Windows Defender security being disabled (Dirgantara & Ramadhan, 2024). The effort raises the possibility of malicious activity or dangerous illegal activity. This malicious activity is the main stage of a cyber attack. This is because the activity is related to the installation of malicious files, disabling cyber protection, deleting important files, and disabling running services. A moment later, Windows Defender crashed and could not operate on June 20, 2024. The impact of this incident, PDN experienced a data leak and a number of important state data were encrypted.

Following the cyberattack targeting the National Data Center, BSSN conducted in-depth digital forensics on June 23, 2024. Analysis was continuously conducted based on existing digital evidence. A day later, June 24, 2024, BSSN officially stated that the National Data Center had experienced disruption caused by a cyberattack of destructive hardware or ransomware brain chipper.

A national cyber disaster is finally inevitable. It is feared that it will affect national sovereignty and threaten state security. The extent of the leaked data from ministries and institutions is also unpredictable. As an initial mitigation step, the Indonesian government is implementing data backup and service recovery efforts using a backup server system or other server services. Furthermore, in the backup of cold site data that is upgraded to

hot site, layered protection is carried out. This double protection is an effort to minimize cyber attacks that can possibly be carried out again by cybercrime perpetrators.

State Responsibility Regarding Personal Data Leaks at National Data Centers

Indonesia as a country of law certainly implements its state administration based on applicable laws. As the legal basis of Indonesia, the Constitution of the Republic of Indonesia 1945 states that there are four goals in the formation of the Indonesian nation, namely protection, intelligence, welfare, and the implementation of world order. The element of protection is an effort to implement protection for the entire nation and all of Indonesia's blood as the nation's ideal (Ridlwan, 2012). The reflection of the nation's ideals is carried out through the issuance of regulations governing the protection of the Indonesian people. Human rights are also included in the matters guaranteed by the Indonesian Government.

Protection and guarantee of human rights are indeed carried out by the state based on the 1945 Constitution of the Republic of Indonesia. Specifically, the regulation and guarantee of human rights are regulated in Law Number 39 of 1999 concerning Human Rights. Among the rights that are protected and guaranteed are personal rights and privacy. Protection of personal rights covers a wide range of things, especially with the development of the times. Protection of personal data on digital media is very important. Based on this urgency, Law Number 27 of 2022 concerning Personal Data Protection was issued.

The issuance of Law Number 27 of 2022 is the main normative reference (as well as a specialized normative regulation) regarding the legal provisions for the protection of personal data. The implementation of guaranteeing the security of personal data is the responsibility of the person in charge of the data. This guarantee is of course carried out with a protection scheme related to information technology that is considered capable. The responsibility for guaranteeing data security and protection is related to the digital governance carried out by the person in charge of the data. In essence, the person in charge of the data guarantees security and makes every effort to prevent data leaks. Through Law Number 27 of 2022, the Government of the Republic of Indonesia creates a legal standing regarding legal protection of personal data.

Legal protection is the main function of a sovereign state. This protection is carried out to guarantee justice for the people of Indonesia. The state is responsible for obtaining

justice for each individual and is enforced fairly in the eyes of the law. This implementation also goes hand in hand with the protection of human rights to create order and security. However, the creation of order and security is not the main goal of the law, but rather an intermediate goal. The main (further) goal is to realize true peace in society (Sinaulan, 2018).

Indonesia in the implementation of its governance uses digital-based data center governance. The data center is a state facility that has the ability to manage, organize, and organize information and communication technology services in the form of services (Riasetiawan, 2016). Based on a national perspective, the existence of a data center is important for the implementation of maintenance and archiving of data assets managed by both regional and central governments. The existence of data centers in Indonesia has many positive impacts related to the development of digitalization in the government sector. However, this development is not followed by an increase in cybersecurity, resulting in hacking and data leaks in national data centers.

The data leak in the National Data Center has caused national public unrest in Indonesia. Many people are worried that the leak of personal data can affect the security of other data that has the potential to cause major losses, such as banks for example. Regarding the personal data of Indonesian people (as recorded in immigration for example), the full name is recorded along with personal identification in the form of fingerprints and authentic retinal recordings of each individual.

Basically, the Indonesian Government has implemented an electronic-based government system since the issuance of Presidential Regulation Number 95 of 2018. The Presidential Regulation instructs the implementation of an electronic-based government system starting from preparation (both governance, planning, architecture, and management) and provisions for the implementation, acceleration, and evaluation of SPBE. Through this Presidential Regulation, the National Data Center was formed to integrate government data from regional to national scales covering all ministries, institutions, and agencies of the Indonesian Government.

The implementation of governance and operations of the National Data Center is the responsibility of the government. This is based on Presidential Regulation Number 95 of 2018 which indicates the formation of PDN in accordance with existing legal norms. The Indonesian government in its efforts to organize SPBE through the PDN program is

carried out by the Ministry of Communication and Information along with stakeholders as third parties assisting the program implementers.

In relation to the major incident of the National Data Center leak, the Indonesian Government should have taken full responsibility. This is related to the PDN which is under the auspices of the state and the Indonesian Government casu quo Kominfo is the party responsible for the data. As regulated in the Personal Data Protection Law, the government is obliged to be responsible and comply with legal provisions. In relation to the management of personal data of the Indonesian people, the Indonesian Government is obliged to ensure the security of data processing, record data processing activities, maintain data confidentiality, provide public notification in the event of a data leak, and evaluate the impact of data protection.

The Personal Data Protection Law expressly regulates the obligation to protect personal data from unauthorized processing. This is also related to the state's responsibility to provide protection and legal certainty regarding the personal rights and privacy rights of the Indonesian people. The cybercrime case of hacking the National Data Center made the Indonesian Ministry of Communication and Information the main figure and the most responsible for the incident. Furthermore, the National Cyber and Crypto Agency is also responsible for the governance and security guarantees of the implementation of the electronic-based government system that has been implemented.

Kominfo and BSSN are state-formed institutions that carry out their duties and functions in the operationalization of PDN. The Minister of Kominfo of the Republic of Indonesia and the Head of BSSN as policy makers must carry out their responsibilities for cyber attacks on PDN. The connection between these cyber attacks must be used as the main evaluation in the context of organizing and allocating program implementation to improve the performance of the ministry.

Based on Article 57 of the PDP Law, data custodians who violate the provisions of Article 38 of the PDP Law regarding the obligation to protect data from unauthorized processing are subject to administrative sanctions. The sanctions given can be in the form of written warnings, temporary suspension of personal data processing, deletion of personal data, and/or administrative fines. The Indonesian government in this case the Ministry of Communication and Information, BSSN, and stakeholders can be subject to these administrative sanctions. This is because it has been proven that there has been

negligence and inability to be responsible in safeguarding the personal data of the Indonesian people.

Public notification of the data leak is the right step taken by the Indonesian Government. Based on this notification, the public can take anticipatory measures to protect personal data in the form of changing passwords on applications that are considered important. In addition, this notification is intended so that the public can take preventive measures and care for personal data so as not to be significantly impacted by PDN hacking.

The provision of a complaint mechanism is the next responsibility of the state. This provision is related to measuring the extent to which the PDN hacking has an impact and who has suffered losses due to this incident. The implementation is also an effort by the Indonesian Government to organize and regulate the priority scale in resolving data-related problems in the ministries and institutions of the Republic of Indonesia.

The Indonesian government through the cyber attack incident on the National Data Center and negligence in the absence of data backup indicates many normative violations that have occurred. These violations have certainly resulted in a decline in public trust in the government. The government has tactically violated the constitutional rights of the people as regulated in Article 28 of the 1945 Constitution of the Republic of Indonesia concerning the guarantee of protection of personal rights.

The government also in this case committed a violation of Law Number 39 of 1999 concerning Human Rights and Law Number 27 of 2022 concerning Protection of Personal Data. This clearly shows that there needs to be a restructuring and improvement of the quality of the government sector, especially in the field of information technology and cyber. Increasing awareness and education must also be carried out in order to fulfill the government's responsibility for this incident to the public. Personal data is important and vital, therefore protecting personal data is a big responsibility.

The responsibility of the Indonesian Government after the cyber attack on the National Data Center is an effort to restore data and create normal and effective government services. There are countless complaints about the paralysis of government services in various institutions and agencies. Fast and safe steps are needed by the public who are worried about the condition of their personal data. The government is obliged to restore the situation and conditions to their original state. In fact, in the author's opinion,

the Indonesian Government is obliged to provide compensation to citizens affected by the data hacking.

The implementation of the Indonesian Government's responsibility in the National Data Center hacking incident was carried out in various ways. The most important thing is that the government's mitigation efforts and solution provision can minimize the unrest and threat of losses that are rolling in the community. Of course, in the future, there needs to be an evaluation and improvement of performance along with human resources in the scope of cyber strategic studies so that this cyber attack incident does not happen again. Effectively, the Indonesian Government must make improvements and equalize human resources in terms of cyber knowledge. Governance related to cyber must also be improved by restructuring decision makers to people who are experts in their fields.

CONCLUSION

The cyber attack on the National Data Center of the Republic of Indonesia resulted in the paralysis of services and operations of a number of ministries and government agencies. The ransomware cyber attack was carried out from June 17, 2024 to its peak on June 20, 2024. There were malicious activities that resulted in the deactivation of cyber protection, the operation of unauthorized data processes, and ended with the hacking and locking of important state data from hackers.

The Indonesian government is obligated to take responsibility for data recovery efforts and normalization of digital-based government governance and services. Minimizing the impact and consequences of PDN hacking is a priority that is the government's main concern. Restructuring the Ministry of Communication and Information and related institutions is the main thing that must be done to improve cyber-based human resources. Normatively, the Indonesian government cq Ministry of Communication and Information and BSSN can be subject to administrative sanctions in accordance with the provisions of the Personal Data Protection Law.

REFERENCE

Bestari, N. P. (2024). Chronology of hacker seizing control of national data center revealed by BSSN. *CNBC Indonesia*. Retrieved from https://www.cnbcindonesia.com/tech/20240627170323-37-549971/kronologi-hacker-rebut-kendali-pusat-data-nasional-diungkap-bssn

BSSN Legal and Communication Bureau. (2024). BSSN identifies temporary national data center attacked by ransomware. *bssn.go.id*. Retrieved from https://www.bssn.go.id/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware/

Dirgantara, A., & Ramadhan, A. (2024). Budi Arie reveals chronology of cyber attack on PDN that paralyzed services. *Kompas.com*. Retrieved from https://nasional.kompas.com/read/2024/06/27/17585061/budi-arie-beberkan-kronologi-serangan-siber-ke-pdn-yang-bikin-layanan-lumpuh

Dwi, A. (2024). 6 impacts of ransomware attacks on PDNS servers. *tempo.co*. Retrieved from https://tekno.tempo.co/read/1886038/6-dampak-serangan-ransomware-ke-server-pdns.

Fransisco, W. (2020). Public interaction towards law in the new normal life post COVID-19. *Journal of Judicial Review, 22*(2), 153. Retrieved from https://doi.org/http://dx.doi.org/10.37253/jjr.v22i2.1483

Government of the Republic of Indonesia. (1999). *Law Number 39 of 1999 concerning Human Rights*.

Government of the Republic of Indonesia. (2018). *Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems*.

Government of the Republic of Indonesia. (2022). *Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection*.

Hansen Samin, H. (2023). Legal protection against personal data leakage by data controllers through a progressive legal approach. *Jurnal Sains Student Research, 1*(2), 2. Retrieved from https://doi.org/10.61722/jssr.v1i3.386

Marzuki, P. M. (2005). *Legal research: Revised edition*. Jakarta: Kencana.

Mulyanto, H., Rohmani, M. N., Prasetya, M. A. B., & Santoso, A. P. A. (2024). The importance of implementing Pancasila values in the development of technology among the millennial generation. *Proceedings of the National Seminar on Law, Business, Science, and Technology, 4*(1), 637.

Riasetiawan, M. (2016). *Data center for government*. Yogyakarta: Department of Computer Science and Electronics FMIPA UGM.

Ridlwan, Z. (2012). Indonesian state law is the opposite of Nachtwachterstaat. *Fiat Justitia Journal of Legal Studies, 5*(2), 148.

Saly, J. N., Artamevia, H., Kheista, K., Juni, B., Gulo, S., Rhemrev, E. A., & Christie, M. (2023). Analysis of personal data protection related to Law No. 27 of 2022. *Serina Humaniora Journal, 1*(3), 148.

Sinaulan, J. H. (2018). Legal protection for community members. *IDEAS Journal of Education, Social, and Culture, 4*(1), 79-84.

Soekanto, S., & Mamuji, S. (1995). *Normative legal research, a brief review*. Jakarta: PT Raja Grafindo Persada.

Soemitro, R. H. (1985). *Some problems in the study of law and society*. Bandung: Remaja Karya.