International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

Vol. 40 No. 2 September 2023, pp. 164-170

Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law

Farah Diba Tanzilla, Margaretha Hanita, Bondan Widiawan

National Resilience Study, SKSG, University of Indonesia, Jakarta, Indonesia
Salemba Raya street no. 4, Jakarta, Indonesia 10430
Corresponding author : dibatanzilla66@gmail.com

Abstract – Cyber Security plays an important role in a country's national cyber security and defense efforts. With strong cyber security, Indonesia will be able to handle cybercrime problems and be able to survive potential cyber threats in the future which are increasingly diverse in form and mode. Protecting personal data is part of efforts to safeguard the cyber domain which has become a new commodity in the current technological era. The Indonesian government has just passed the Personal Data Protection Law at the end of 2022 which requires a two-year socialization and transition period until the end of 2024. During the socialization period, This law found that personal data leaks in Indonesia are increasing, which is important for further research. Therefore this study will aim to obtain an overview of the condition of cyber security in Indonesia, especially after the passage of the Personal Data Protection Law, find the core problem of the issue of data leakage, and outline suggestions that can be made by the Indonesian government as a form of support for efforts to strengthen cybersecurity in Indonesia. This research uses a qualitative analytical descriptive approach, data was collected through literature study and interviews as primary data sources. From this research, it was found that Indonesia is still in a precarious state of cybersecurity, where cyber threat issues still occur, including personal data leaks. Four factors cause the problem of data leakage as well as a perspective in suggestions for solving problems in cyber security in Indonesia, namely *Policies*, *Procedures*, *Equipment*, and *People*.

Keywords – Cyber Security, Personal Data Protection, Personal Data Leakage.

I. INTRODUCTION

In general, based on Law Number 27 of 2022 concerning the Protection of Personal Data, it is stated that "Protection of personal data is one of the contents of human rights which is part of personal self-protection, therefore a legal basis is needed to provide security for personal data based on The 1945 Constitution of the Republic of Indonesia". Personal data protection aims to guarantee citizens' rights to personal protection as well as to raise public awareness and guarantee recognition and respect for the importance of protecting personal data itself. The Personal Data Protection Act includes 76 articles that should guarantee data subjects the security of their data from parties who can access and use the data outside their control or illegally [1].

In Chapter 1 Article 1 of Law Number 27 of 2022 concerning the Protection of Personal Data, it is defined that personal data is data from a person or individual that can be identified independently or combined with other information that directly or indirectly goes through systems, both electronic and non-electronic. Information can be defined as ideas, statements, messages, data, facts, and explanations that can be processed by sight, and hearing, and presented in a format adapted to the development of information and communication technology. While the definition of personal data protection, is all efforts to protect personal data in a series of personal data processes, to guarantee the constitutional rights of personal data subjects. The subject of personal data is a person or individual whose personal data is attached to it, it is also defined that everyone is an individual or a corporation. In Article 2 it is explained that this law applies to everyone, public bodies and international organizations that carry out legal actions and are covered by the requirements: 1) are within the jurisdiction of the Republic of Indonesia, 2) are outside the jurisdiction of the Republic of Indonesia but has legal consequences in the jurisdiction of the Republic of Indonesia, 3) the subject of personal data of Indonesian citizens is outside the jurisdiction of the Republic of

Indonesia. It is emphasized that this law cannot be enforced in the processing of personal data by individuals in personal or household activities [1].

The digital revolution creates innovation and the ability to obtain, store, transmit, and manipulate data in real-time, complex, extensive, and even undetectable. The digital revolution is said to be synonymous with the data revolution because the digital revolution has resulted in the phenomenon of massive data collection without considering what type of data will be useful in the future. Therefore, various parties compete to collect almost all the data that can be obtained, both the government and the private sector compete to increase the capacity of data storage systems and do very little to delete data. Data managers are aware that data now has value and is a tangible and usable asset. This increases the need for personal data protection for data subjects or the public who own personal data [2].

Proper cyber-security requires preparation and strategic steps to run quickly and on target. Reflecting on countries that have had legal regulations in the form of personal data protection laws even decades ago, but until now they are still trying to strengthen the resilience of their cyberspace. Indonesia is now in a better phase and position compared to previous years in the field of *cyber-security*. In 2017 Indonesia was ranked 70th in the Global Security Index (GCI), increased in 2018 to rank 41, and ranked 24th in 2020 out of 194 countries in the world [3]. However, this title is not a guarantee of cyber security and resilience and Indonesia should continue to strive to strengthen its national cyber defense as well as be prepared for the potential for non-traditional crimes in the cyber sphere, which are now increasingly in various forms, especially those related to personal data protection.

II. Research Methodology

This research was conducted using descriptive-analytical methods and a qualitative approach. Data was collected through literature study and interviews by researchers directly with several sources who are experts and observers in the field of cyber security and cyber security in Indonesia. In the research process, researchers collected data on cases of cybercrime in Indonesia, especially on the issue of leakage of personal data from 2020-2023, cases that occurred before the enactment of the Personal Data Protection Law until after it was enacted and during the socialization period of the law. new law. The large number of cases of personal data leakage in Indonesia after the enactment of the Personal Data Protection Law deserves more attention, especially because until 2024 there will be a transition and socialization period which will become a benchmark for cyber defense preparations after the socialization period.

Using the *fishbone data analysis technique* or fishbone diagram analysis according to Prunckun to assess the cause and effect of a problem can then help to become a guide in collecting the data and information needed in this research.

III. Result And Discussion

3.1. Leakage of Personal Data After the Enactment of the Personal Data Protection Act

Before the existence of the Personal Data Protection Act, regulations or laws regarding personal data protection were divided and scattered in several laws and regulations which in fact could not be said to be specific and comprehensive so they still needed special laws regarding personal data protection. These laws include Law Number 11 of 2008 and Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE), Law Number 39 of 1999 concerning Human Rights (HAM), Law Number 14 of 2008 concerning Public Information Disclosure, as well as Law number 23 of 2006 and Law number 24 of 2013 concerning Population Administration [4]. Also Law number 36 of 2009 concerning Health states that every individual has personal rights and personal data protection, Law number 57 paragraph 1 number 36 of 2009 which contains that every individual should participate in protecting people's data [5].

Since the enactment of the Personal Data Protection Law on October 17, 2022, it is known that Indonesia has received 46,994,562 attacks in the period from October 2022 to July 2023. Data obtained from the Honeynet map page of the National Cyber and Crypto Agency shows *that* Indonesia received more attacks compared to a superpower like the United States which received 42,537,733 attacks, The recipient of cyber attacks in third place was India which received 42,090,699 attacks, fourth place China received 27,758,546 attacks, and Fifth place is South Korea which received 15,860,207 attacks [6].

During this period, the region in Indonesia that was in the red zone, namely the recipient of the most cyber attacks, was Riau Province with a total of 115,736,475 attacks. Followed by DKI Jakarta Province with 40,683,588 attacks, Central Java

Province with 37,774,936 attacks, West Kalimantan Province with 23,566,241, East Java Province with 22,409,586, Bali Province with 20,822,614 attacks, West Java Province with 18,204. 613 attacks, Gorontalo Province with 11,127,916 attacks, Aceh Province with 10,572,024 attacks, South Sumatra Province with 10,215,026 attacks, Banten Province with 5,810,746 attacks, North Sumatra Province with 2,486,656 attacks. Other regions such as the Riau Archipelago Province, Bengkulu, Lampung, Central Kalimantan, East Kalimantan, South Kalimantan, North Sulawesi, South Sulawesi, West Nusa Tenggara, and East Nusa Tenggara and West Irian Jaya received less than one million attacks. Meanwhile, the provinces of West Sumatra, Jambi, Bangka-Belitung, West Sulawesi, Central Sulawesi, Southeast Sulawesi, North Maluku, and Maluku did not receive cyber attacks during this period [6].

Even though the Personal Data Protection Law has been formed, it was found that in the period I, namely from January to June 2023, there has not been a single case that was sanctioned in the form of a fine as a result of the leakage of personal data. In about six months, it is known that there have been 35 cases of personal data leaks, the most leaks occurred in June, namely 15 cases of data leaks. So far the government has resolved data leak cases in previous years in the form of recommendations and written warnings. Based on a statement from Samuel Abrijani Pangerapan, Director General of Applications and Informatics of the Ministry of Communication and Informatics, sanctions in the form of new fines can be imposed at least since October 2024, which is exactly two years since the Personal Data Protection Act was passed, or since the socialization and trial period this law ends. This is related to the absence of government regulations (PP) regarding the application of fines in cases of personal data leaks that occur [7].

3.2. The Condition of Cyber Security in Indonesia After the Enactment of the Personal Data Protection Act

The condition of Cyber Defense in Indonesia, especially in the context of protecting personal data, still requires real action, especially from the Indonesian government. The cyber realm is part of the territory of the Republic of Indonesia which, although its territory is not visible, has a very important role and position in national security and defense. The resilience of the cyber area will not be built properly if it only relies on laws that incidentally cannot be implemented because of the absence of an institution responsible for this area, especially in the field of personal data protection. What needs to be considered is the absence of an institution that is directly responsible for personal data issues in Indonesia is clear evidence of the absence of integration from the Indonesian government to seriously deal with cyber problems that continue to batter Indonesia's sovereignty. In fact, institutions such as the National Commission for Personal Data Protection should be the driving force and person responsible for the Personal Data Protection Law, without this commission the Personal Data Protection Law is just a text without the ability to protect the rights of the Indonesian people or defend the national cyber area. Protection of personal data is the beginning of the formation of a national cyber security system that is able to protect the people and other data subjects who are part of the Republic of Indonesia.

The existence of the Personal Data Protection Law is not the end of the struggle to maintain national cyber sovereignty, the creation of a national cyber area that is safe and responsive to potential cyber crimes requires cooperation from various parties, both government and non-government. For the sake of strong state sovereignty in the cyber area, Indonesia still needs time for a socialization period or trial period for the Personal Data Protection Law that has been passed. In interviews conducted by researchers, experts in the realm of cyber security still have high hopes for the successful contribution of the Personal Data Protection Law to national cyber security and defense.

Data leaks, which are now a major issue in the realm of national cyber security, are not only experienced by Indonesia but also other countries almost all over the world. However, what makes the difference is the complexity of the cyber attack or data leak. According to Faisal Yahya, a country's cyber resilience is not only assessed from the state's side but from the entity that manages and owns cyber facilities which must be strengthened and increase *awareness* regarding potential cyber attacks. Both the public and data managers in the private sector and government agencies have the same responsibility for *cyber security awareness* . It was emphasized that the current reality shows that society dominates as a human factor in the realm of *cyber security* , the phenomenon *of work from home* or *work from anywhere* after the Covid-19 pandemic has created a new environment in the world of work, where indirectly the responsibility regarding cyber security is held by control. each personnel who accesses the online realm with personal devices in their activities. Even though institutions or companies have provided devices with cyber security to personnel, if this is not accompanied by *cyber security awareness* then the potential for cyber crime will continue to occur, because according to Faisal Yahya, " *the next version of cyber security is inside the people's head* " therefore education regarding *cyber security awareness* must be the main basis for activities in the cyber area [8].

Pratama Dahlian Persada stated that the condition of misuse of personal data in Indonesia has entered a critical stage, there are almost no boundaries between which parties may be able to access public personal data for illegal activities. With regard to defense and cybersecurity, Indonesia is also in a bad condition due to the absence of supporting features that are no less important in order to create a *cyber space* that can withstand threats. According to Pratama, there are at least seven important issues that need to be resolved intensively by the Indonesian government, namely:

- Implementation of the law has not been optimal, both in terms of the content of the law and other supporting factors.
- The sectoral ego of the leaders of state institutions makes it difficult to form comprehensive and intensive cooperation between institutions, especially for institutions that have direct contact with cyber defense and security issues and the protection of personal data. This is directly related to the vision and mission of the Indonesian government in implementing the Personal Data Protection Law.
- The vision and mission of cyber security and defense that have not been integrated, cooperation between institutions, especially under the auspices of the government, is the main key to the success of national cyber defense. Currently, the duties and functions of institutions under the Personal Data Protection Act are still not clearly defined.
- The quality and quantity of government institution personnel who have direct contact with cyberspace is still lacking in number and capacity. The increase in cybercrime cases in Indonesia has increased the need for personnel or human resources, increasing the number of personnel in related institutions is expected to strengthen the government's work performance. It should be understood that in the context of cyber defense, it requires not only sophisticated equipment and infrastructure but also competent and qualified human resources. So that increasing the competence of internal personnel in government institutions is no less important and cannot be underestimated. This is because sophisticated infrastructure will not make a maximum contribution if it is not run by the right personnel.
- Absence of Cyber Threats Curriculum in Indonesia. In connection with the previous point regarding education to achieve the maximum potential of existing human resources, Indonesia needs a curriculum regarding cyber security not only for adults but should have been educated from an early age, because as time goes by, the cyber domain can not only be accessed by adults but as well as children who will one day become the nation's successors. Therefore, cyber security education needs to be held immediately, so that the nation's future generations can continue to follow developments in the digital realm safely and avoid potential cyber threats.
- Awareness or awareness of *cyber security* for leaders in Indonesia. It is known that many leaders in Indonesia still underestimate the issue of cybersecurity, this is judged by the devices and applications used which are insecure and very easy to hack. For example, personal communication media in the form of messages that are widely used by the public, are also used by state leaders as a medium of communication to discuss state issues. This is said to be very risky because apart from the high possibility of being accessed by irresponsible parties, the providers of these applications and devices are also able to find out about the country's internal affairs in case of negligence, this issue has happened to leaders of other countries whose private message accounts have been hacked, This should serve as an example for the Indonesian government to be more careful and concerned about the communication media used, especially if the communication includes sensitive matters and is an internal state affair.
- Lack of critical infrastructure protection in Indonesia. According to the National Cyber and Crypto Agency, Critical Infrastructure is "important infrastructure to support vital functions in society, such as health, safety, economics and social welfare. Any disruption or obstacles to critical infrastructure will have serious consequences for these vital functions. For example, critical infrastructure including Ports, Airports, Hospitals, Telecommunication Infrastructure, Financial and Banking Services, etc." [9]. This is related to the readiness of the government and infrastructure control institutions in Indonesia which must prepare themselves to face potential threats in the cyber domain, especially after the socialization period for the Personal Data Protection Law ends in October 2024. Readiness for the protection of personal data needs to be assessed. repeated because it is one of the risk points, especially in the section on administrative fines, which are only intended for non-governmental parties, so it is necessary to redefine the sanctions that will be imposed if the violating party is part of a government institution or controller of vital infrastructure [10].

There are things that can be considered by the Indonesian government based on factors found using the fishbone method, related to *Policies*, *Procedures*, *Equipment* and *People*, including:

1. Prepare and increase *awareness* regarding potential cyber attacks that may occur after the two-year socialization period of the Personal Data Protection Law ends, in order to prepare supporting factors both in terms of implementing regulations and additions and improvements to the contents of the Personal Data Protection Law so that it can work optimally.
2. Explain and define in detail the contents of the Personal Data Protection Act regarding sanctions given to government agencies that manage and store personal data in the event of a personal data leak. Because the Personal Data Protection Act only explains the obligations and sanctions aimed at companies or non-governmental data controllers.
3. Adding the principle of transparency to the Personal Data Protection Act which includes provisions regarding the time when personal data is collected, processed and stored by the personal data manager [11].
4. Explain and reaffirm the division of authority between government agencies responsible for national cyber security and institutions that are data controllers and manage and store public personal data under the auspices of the Personal Data Protection Act. Comprehensive and synergistic division of tasks and authorities from responsible government agencies will be a good foundation in particular for the implementation of the Personal Data Protection Law.
5. Permanently establish a Personal Data Protection Authority Agency or National Commission for Personal Data Protection so that the Personal Data Protection Act can be applied immediately to government agencies that store and manage public data, as well as private parties such as organizations and companies and other parties who are data managers personal. So that monitoring, sanctions and prevention of personal data leaks can be carried out.
6. Conduct periodic inspections of institutions, companies and organizations that are the managers of personal data to ensure that the cyber security system used to store and access data meets established security standards.
7. Collaborating with private parties working in the field of *cyber security* both from within and outside the country to establish *cyber security standards* that must be met by institutions and parties managing personal data, adapting to problems and potential data leaks that have occurred and may occur in Indonesia.
8. Increasing investment in the development of *cyber security technology and devices* in Indonesia for both government and private institutions. The cyber security system is a technology that is constantly changing and developing following the potential for cyber threats which are increasingly in various forms of attack so that investment especially provided by the Indonesian government will be a springboard for personal data managers so that they can immediately improve and increase the quality of the cyber security system. The Indonesian government needs to understand that investing in technology is an investment that requires a lot of money, but the impact and security provided are commensurate with what is being guarded, namely the personal data of the Indonesian people.
9. Holding a *cyber security training program* as part of mandatory qualifications for government agency personnel, especially those who have direct contact with the management and control of personal data. This is important to improve the quality and efficiency of personnel so that they can better deal with the tasks and functions they carry out.
10. Carrying out mass recruitment of young people who have qualifications in the field of cyber security as well as cyber security experts in Indonesia to participate in becoming part of data management institutions and personal data protection institutions. Bearing in mind and considering that government institutions, especially those responsible for cyber security and resilience, still need additional human resources, especially those who have competence in *cyber security* .
11. Conduct socialization in the form of education regarding *cyber security* to the Indonesian people in order to create awareness of the importance of cyber security and the potential for cyber crimes that may occur in people's lives.
12. *cyber security* curriculum as part of the education curriculum in Indonesia which is given as early as possible so that children from school age to tertiary education have awareness of *cyber security* and are able to protect themselves from potential cyber threats.

IV. CONCLUSION

As previously mentioned regarding the condition of cyber attacks in Indonesia, even though the personal data protection law has been passed and implemented since October 17 2022, personal data leaks still occur with various motives and modes. The public, organizations and/or companies and other data management institutions still do not fully understand the contents of the Personal Data Protection Law and the preventive measures that can be taken to continue to protect the management and storage of personal data. Considering that this Law is a new regulation, it is the first step for the government to provide outreach to parties who manage and own personal data regarding procedures, as well as rights and obligations contained in the Personal Data Protection Law as well as procedures for carrying out reporting. theft of personal data that affects data owners and managers [5].

Challenges in implementing the Personal Data Protection Law are also something that cannot be avoided. Naturally, challenges are things that can occur unexpectedly, therefore the synergy between the government as the main person responsible and the community must be strengthened to minimize losses that can occur. from personal data leaks. Even though the government's responsibility as a data manager is greater, the role of the community is no less important in being more alert and observant of potential cyber crimes, especially in areas connected online. It is important for the public to understand and be aware of cybercrime actions so that personal data is not used illegally by irresponsible parties [5].

In an effort to create national cyber resilience, apart from the need for socialization from the government, cooperation from non-government parties such as the mass media is also needed to educate the public about potential threats in the cyber domain and ways to prevent them. It is hoped that the intensity of public education will increase the awareness of each individual and group regarding their personal data.

REFERENCES

[1] D. RI, "Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," Pemerintah Indonesia, Jakarta, 2022.

[2] W. Djafar, "Hukum Perlindungan Data Pribadi di Indonesia : Lanskap, Urgensi dan kebutuhan Pembaruan," *Jurnal Fakultas Hukum Universitas Gadjah Mada ,* pp. 1-14, 2019.

[3] BSSN, "bssn.go.id," 9 Agustus 2022. [Online]. Available: https://www.bssn.go.id/indeks-keamanan-siber-indonesia-peringkat-ke-24-dari-194-negara-di-dunia/.

[4] L. M. Jannah, "UU Perlindungan Data Pribadi dan Tantangan Implementasinya," 21 September 2022. [Online]. Available: https://www.jawapos.com/opini/01409091/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya.

[5] A. F. Sutarli, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia," *INNOVATIVE : Journal of Social Science Research vol. 3 no. 2 ,* pp. 1-14, 2023.

[6] H. W. B. S. d. S. N. BSSN, "honeynet.bssn.go.id," 27 July 2023. [Online]. Available: https://honeynet.bssn.go.id.

[7] I. CNN, "cnnindonesia.com," 19 Juni 2023. [Online]. Available: https://www.cnnindonesia.com/teknologi/20230619141948-192-963776/35-kebocoran-data-2023-kominfo-akui-cuma-beri-rekomendasi-dan-teguran.

[8] F. Yahya, Interviewee, *Wawancara Penelitian Tesis : Pelindungan Data Pribadi dan Ketahanan Siber.* [Interview]. 13 June 2023.

[9] BSSN, "Sosialisasi dan Permintaan Tanggapan atas Rancangan Peraturan BSSN tentang Perlindungan Infrastruktur Informasi Kritis Nasional," 13 September 2019. [Online]. Available: https://bssn.go.id/sosialisasi-dan-permintaan-tanggapan-atas-rancangan-peraturan-bssn-tentang-perlindungan-infrastruktur-informasi-kritis-nasional-iikn/.

[10] D. P. D. Persada, Interviewee, *Wawancara Penelitian Tesis : Pelindungan Data Pribadi dan Ketahanan Siber.* [Interview]. 9 June 2023.

[11] P. H. Saragih, Interviewee, *Wawancara Penelitian Tesis : Pelindungan Data Pribadi dan Ketahanan Siber.* [Interview]. 10 June 2023.

[12] S. Nadia, "Mengembalikan Humanisme Perlindungan Data Pribadi melalui Perluasan Yuridiksi Ekstrateritorial sebagai Upaya Diplomasi dalam Mewujudkan Keamanan Siber," in *Antalogi Esai Hukum dan HAM*, Jakarta, 2020, p. 55.

[13] Wahyudi, "ksi.Indonesia.org," 30 April 2020. [Online]. Available: https://www.ksi-indonesia.org/id/wawasan/detail/1292-mendesaknya-regulasi-pelindungan-data-pribadi-yang-kompherensif.

[14] T. W. Edgar and D. O. Manz, "Defining Cyber Space," in *Research Methods for Cyber Security*, United States, Elsevier Inc., 2017, p. 34.

[15] H. Yeli, "A Three-Perspective Theory of Cyber Sovereignty," PRISM, 2017, pp. 109-115.

[16] S. Ghernaouti, Cyber Power : Crime, Conflict and Security in Cyber Space, EPFL Press English Imorint, 2013.