THE ISSUES OF DATA PROTECTION AGAINST LEAKING OF PERSONAL DATA IN SOCIAL SECURITY HEALTH SERVICES (A COMPARISON BETWEEN INDONESIA AND OTHER COUNTRIES REGULATIONS)

Charisma Septi Jayanti
Suraji

ABSTRACT

The growing use of technology and information, particularly in terms of internet access, has both positive and harmful consequences, one of which is cybercrime. The Health Social Security Organizing Agency (BPJS), which is operated by the Indonesian government, was one of the enterprises afflicted by cybercrime, with personal data belonging to members being leaked. This research aims to examine legal issues over personal data leaks involving millions of personal data acquired by Indonesia's Health Social Security Agency, as well as legal parallels to personal data protection in other countries. This research uses normative legal methods that are prescriptive by reviewing laws and regulations such as Act No. 11 of 2008 on Information and Electronic Transactions. The absence of laws that comprehensively managed the protection of personal data can increase the potential for leaks and crimes against citizens' personal data which is a constitutional right that information should be protected and safeguarded to prevent misuse of information.

Keywords: Cybercrime, Personal Data Leakage, Comparative law

INTRODUCTION

Humans have a wide range of technological interests in their daily lives. The goal of implementing this technology is to improve the efficacy and efficiency of public services in order to educate the nation's citizens and to provide everyone with more possibilities to progress their minds and abilities. By using the internet, electronic transactions have become simpler, easier, and less expensive. The more evolved the times, the more technology exists that has a great impact on human life, but it also comes with a slew of negative consequences, one of which is the prevalence of cybercrime, or crime in cyberspace.

The digital crime case that occurred recently was the case of data leakage of participants from the Social Security Helath Services (Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan)) organized by the Indonesian government. BPJS itself is a legal entity established by the government to run health insurance for all Indonesian people. This agency (BPJS Kesehatan) data leak case was revealed at the end of May.

This matter was first brought to light by a Twitter account called Kotz. This account makes purchasing and selling offers on an online forum, notably Raid Forums, as both a buyer and a vendor of personal data (reseller). By displaying around 100,000 samples, the seller revealed that he had 279 million copies of Indonesian people' identifying data. Data in the form of population identification numbers (NIK), names, addresses, telephone numbers, and e-mail addresses that are sold on unlawful sites are examples of leaked data (dark web). A total of 20 million data equipped with photos. The leak of BPJS data is detrimental to people who are themselves registered in the BPJS Health insurance program. Leaked data can cause material and immaterial losses. The leaking of BPJS data makes the public do not have a sense of security in being able to store data from government and private agencies because they are vulnerable to becoming victims of cybercrime.[1]

Indonesia is a country that recognizes the existence of human rights, violations of personal data must be protected in accordance with the rules set forth in Article 28 G paragraph (1) of the Constitution of the Republic of Indonesia, which states that everyone has the same right to protect himself, his family, and his family. Their honor, dignity, property under their control, and the right to a sense of security and protection from threats of terror to do or not do something in accordance with human rights are all protected. In addition, the violation of personal data leakage which resulted in the health social security participants can be sued in court because of the loss of data dissemination as regulated in Act Number 11 of 2008 concerning Electronic Information and Transactions.

The author aims to make this case into a research paper that addresses the state's responsibility for the leakage of personal data to participants in social security services for health and how to compare personal data protection with other nations that have unique data protection legislation. The theme of debate, namely the security of personal data, is identical in this study, but the primary case studies and analysis are different. The purpose of this study is to examine and analyze the concept of personal data protection that occurs in participants of social security services on health organized by the government in the perspective of comparative law with other countries. This study is presented systematically based on the main material relevant to the focus of the problem, namely the protection of personal data.

[1] Akbari Amarul Zaman, Jumadi Anwar, and Aryo Fadlian, Criminal Liability of BPJS Data Leak in perspective of ITE Law, *Jurnal De Juncto Delicti*, 1.2 (2021), p. 148.

RESEARCH METHOD

The research method aims to direct and seek and find logical reality to answer the formulation of the problem. In this study, researchers used normative legal research methods, namely legal research conducted by looking at library materials or optional information of secondary data such as books, scientific journals, articles and laws and regulations such as Act No. 11 of 2008 on Information and Electronic Transactions.

The type of approach used in this study is a legal approach that examines the rule of law related to the issue of personal data protection. Based on the study (Peter Mahmud, 2008) the approach of legislation is carried out by reviewing all laws and regulations related to legal issues that are being addressed whether there is consistency and conformity between a law and other laws The result of the review is an argument to solve the issues faced. In addition, this research will also use statutory approach and a conceptual approach in order to explain the understanding of legal issues of the leakage of personal data that occur in social security health services of Indonesia (BPJS Kesehatan) and also use the comparative approach of law to review the rules that apply in Indonesia and other countries.

DISCUSSION

Personal Data Protection Problems

The the protection of personal data for consumers or participants in a law have not been specially regulated in Indonesian government. The regulation, on the other hand, is structured into articles, each of which has at least 32 data protection regulations. This case results in the development of numerous regulations that have the authority to manage a person's data and information without any constraints in order to prevent leaks or violations that result in a person's data and information being unprotected.

Protection of personal data includes the rights of a human being because it involves his personality. Indonesia is a country that respects the protection of human rights, and every citizen has constitutional rights, namely rights guaranteed by law. With these constitutional rights, the state and its citizens have a constitutional obligation to protect all citizens.[2] This regulation is written in the Preamble to the 4th Paragraph of the 1945 Constitution of the Republic of Indonesia (UUD RI 1945), which states that the state is obliged to protect the entire Indonesian nation in improving general welfare, educating the nation's life, and implementing world order based on independence, world peace, and social justice.

The right to protect personal data should guarantee protection from the threat of fear to do or not to do something, which is a human right.[3] However, in practice, there are still things or events that cause protected personal data to leak to the public where the personal data has been filled into private personal data. One example is the leakage of personal data experienced by institutions or the Social Security Administrator for Health (BPJS Kesehatan), which can be a large leak of personal data.[4] This problem can be crucial because it involves the leaking of 279 million BPJS Kesehatan participant data and the potential for misuse of other people's personal information to be misused for crimes, namely pretending to be someone else in order to take legal action.

The Ministry of Communication and Information as the authorized government brought in the Board of Directors of BPJS Kesehatan as the manager of the leaked personal data under the mandate of Government Regulation Number 71 of 2019. This regulation is also based on the Minister of Communication and Information Regulation Number 20 of 2016 concerning Personal Data Protection in Electronic Systems. After the meeting, BPJS Kesehatan revealed that it had formed a special team to protect participant data and prevent data leaks from being accessed. However, following the regulation's mandate, electronic system operators do experience serious problems due to data protection failures, so they are obliged to report to other authorized parties and must provide written notification to the owner of personal data.[5]

The legal basis that is used as the basis by participants who are victims of data leakage from the BPJS Kesehatan social security service in-laws and regulations can be used to file a lawsuit against the government, which is under the provisions of the 1945 Constitution Article 28 G paragraph (1) explain that everyone has the right to personal protection, family, honor, dignity, property under his control, right to a sense of security and protection from the threat of fear to do or not do something which is a human right. The protection of personal data is also explicitly regulated in the Electronic Information and Transactions Law (UU ITE) Article 26, which can be concluded that the protection of personal information when it comes to personal data in electronic media and causing losses, a lawsuit, or civil sanctions can be filed, then on Article 1365 of the Civil Code which essentially explains that every legal act that causes harm to another person, the person causing the loss must replace it. As for the Financial Services Authority Circular Number 14/SEOJK.07/2014 concerning Confidentiality and Security of Consumer Personal Data and/or Information, consumer data and/or information must be kept confidential and protected from being leaked and used for improper purposes.

Comparison of Personal Data Protection Laws

The extensive use of the internet nowadays, information may be received very quickly, accurately, globally, and even across national lines. This state is, of course, accompanied by a growth in human-made information technology, thus it cannot be denied

[2] Cynthia H, Registration of Personal Data Through Prepaid Cards in a Human Rights Perspective. *Jurnal HAM*, 9.2 (2018) , p. 191 – 204.
[3] *Ibid*
[4] Akbari Amarul, p. 150-151.
[5] Wahyunanda Kusuma Pertiwi on Kompas.com with the title of the article "Kronologi Kasus Kebocoran Data WNI, DIjual 0,15 Bitcoin hingga Pemanggilan Direksi BPJS" https://tekno.kompas.com/read/2021/05/22/09450057/kronologi-kasus-kebocoran-data-wni-dijual-0-15-bitcoin-hingga-pemanggilan?page=all accessed January 23, 2022 at 22:22.

that the internet's good influence can assist humans in their daily activities. However, due of the increasing risk of digital crime, such as unauthorized internet use, skimming, and even information dissemination, the negative impact of the internet is related to this. The widespread dissemination or leakage of information that exists in several well-known companies in Indonesia is often a public concern because of the large number of leaked personal data that can be used by other parties to carry out illegal acts. In Indonesia, there are already at least several regulations that regulate digital crime, namely Act Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). Several other rules regarding personal data protection are regulated in at least 32 different laws and regulations, such as Act Number 36 of 2009 concerning Health, which regulates the confidentiality of the patient's condition, while Act Number 10 of 1998 concerning Banking regulates personal data regarding depositors 6and the savings. In addition, the regulation on the protection of privacy and personal data is also contained in Act Number 36 of 1999 concerning Telecommunications, Act Number 39 of 1999 concerning Human Rights, Act Number 23 of 2006 concerning Population Administration (amended by Act Number 24 of 2013), and Act Number 11 of 2008 regarding Electronic Information and Transactions (amended by Act Number 19 of 2016), as well as Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions.

In contrast to Indonesia, other countries specifically regulate the rules regarding the protection of personal data and even have a particular supervisory agency to guarantee the implementation of the law on the protection of personal data, such as countries in Europe, America, East Asia and Southeast Asia.[6]

a. Countries In Europe

In European Union countries such as Germany, Sweden, France, Switzerland and Austria, the issue of data protection is a concern, and it is considered necessary that personal data is a fundamental right to privacy that a person must own. Therefore, personal data protection is regulated in a particular regulation, namely The General Data Protection Regulation (GDPR). This regulation is under the fundamental rights needs of the European Union on facing the current digital era. Governments in the European Union have also established a supervisory institution to monitor and protect the rights of citizens in processing personal data and providing sanctions for those who violate the rules regarding the illegal use of personal data by digital criminals in cyberspace.[7]

Protection of this data began with the enactment of GDPR in Germany, followed by other countries such as Sweden, France, Switzerland and Austria. Meanwhile, in the United Kingdom, the Data Protection Act regulations were enacted in 1998 and applied in 2000.[8] The Data Protection Act states that the protection of personal data allows data subjects to obtain information regarding the processing of their data until the data is destroyed to prevent data processing which can threaten its importance.[9] The existence of a security agency and strict sanctions in the European region make its people more aware of cyber crimes that occur in its territory and make the protection of personal data considered to be a personal word that must be acknowledged and appreciated.

In addition, the United Kingdom has also established an independent institution as a body that oversees information rights, namely the protection of personal data and guarantees for the protection of information rights in *Privacy and Economic Communication* (EC *Directive*) *Regulation 2003, Freedom of Information Act 2000, the Environmental Information Regulation 2004, INSPIRE Regulations*, dan *Re- Use of Public Sector Information Regulation*.[10]

The essential principles in the Data Protection Act 1998 also regulates that the management of personal data must be used in accordance with legitimate purposes in accordance with existing laws, the data must be stored not exceeding the period of purpose, the process of managing personal data must be in accordance with the rights the subject is the owner of personal data under the law, and transfers may not be made outside the European Union unless the country receiving the data guarantees the protection of the personal data in accordance with the rights of the subject of the data owner in the process of managing his personal data.[11]

b. United States of America

The Federated States, such as United States of America and its states, apply protection for personal data specified in the US Privacy Law. This rule has been implemented since 1974, which contains a complete list of accurate data processing and prevention of personal data breaches and other matters.[12] This rule applies across the United States and makes the protection of personal data a constitutional right for any individual that personal data must be maintained and taken care of in order to avoid cybercrime or theft of personal data information.

c. East Asian Countries

Hong Kong was the first Asian country to address the issue of personal data privacy. This is demonstrated by the creation of a separate agency, the Privacy Commissioner for Personal Data, to deal with personal data issues (PCPD). This regulation, in theory, imposes constraints on the gathering of personal data that are proportionate to the legitimate purpose of use and collection. Furthermore, if the data is to be released to the public, both parties, data owners and data processors, must accept its use.

[6] Fanny Priscilla, Personal Data Privacy Protection Legal Comparison Perspective, *Jurnal Jatiswara*, 34.3 (2019), p. 245.
[7] *Ibid*
[8] *Ibid*
[9] Edmon Makarim, Introduction to the Law of Telematics (A Compilation of Studies), (Jakarta : Raja Grafindo Persada, 2004) p. 170.
[10] *Information Commission Office* (ICO), "About ICO" https://ico.org.uk/about-the-ic , accessed on January 25, 2022.
[11] Latumahina, R. E., Legal Aspects of Personal Data Protection in Cyberspace, *Jurnal Gema Aktualita*, 3.2 (2014), p. 18-19.
[12] Dewi, S., The Concept of Legal Protection over Privacy and Personal Data Is Associated With the Use of Cloud Computing in Indonesia, *DEMO 2 JURNAL*, 94 (2016), p. 26.

The processing of personal data must also be stored properly and given a storage time limit so that there is no leakage or hacking by irresponsible parties. If this rule is violated by one of the parties, the government will issue a warning letter or subpoena to the party concerned.[13]

In South Korea, the protection of personal data is regulated in the Personal Information Protection Act (Pipa) in 2011. The principle of protection of personal data owned by South Korea is not much different from the rules held by Hong Kong, which must have a clear goal in the process of collecting personal data, it must be ensured that it is accurate, complete and correct, the data used is in accordance with its purpose, maintaining the security of personal data and managing personal data that must not violate the rights concerned in accordance with legal provisions.[14]

Personal data protection regulations have been in place in Japan since the year 2000. The Federal Government of Japan has accepted the Data Protection Art as a legal rule. Keidanren, a representative group that primarily governs industry and trade concerns in Japan, spearheaded the development of legislative standards linked to the protection of personal rights. The Data Protection Art was created as a kind of protection for the Japanese government in the era of commercial competitiveness in the European Union.[15] The principles of personal data protection in the Data Protection Art are that personal data is confidential, the owner of the recorded personal data knows for sure the purpose of using his personal data by any party, there is an agreement in the form of a privacy policy as a form of data use that is not in accordance with the consent, The owner of personal data has the right to make changes or corrections to his data, and it is obligated to restore or compensate for any violations created in the future in the event of a violation of the use of personal data.

d. Countries in Southeast Asia

The country in Southeast Asia that has special rules regarding data protection is Malaysia. The Personal Data Protection Act No. 709 of 2010 (PDPA Malaysia), which was passed in May 2010, has seven principles derived from the EU Data Protection Directive, the OECD Guidelines, or the APEC Framework. The goal of this rule is to govern how personal data is processed by data users in commercial transactions with the goal of protecting the data.[16] According to PDPA Malaysia, it is not permissible to transfer personal data outside Malaysia unless the Minister of Information, Culture, and Communication has granted permission and the country or place to which the personal data is transferred can provide a guarantee of personal data protection equivalent to that provided by PDPA Malaysia.[17]

Singapore had the Personal Data Protection Act (PDPA) in 2012 after Malaysia. Regulations regarding personal data in Singapore have been in full force since 2014. The rules regarding personal data between Malaysia and Singapore have many similarities because they both adopt the rules contained in the European Data Protective Directive (EUDP). However, there are differences in the regulations belonging to Malaysia and Singapore, namely Singapore's 2012 PDPA is equipped with a special agency for registering telephone numbers called the Do Not Call (DNC) Registry, where the public has the right to accept or reject short messages (SMS or MMS) from parties or organizations. unwanted marketing.[18]

CONCLUSION

Personal data protection has not been governed in Indonesia by a unified law that expressly covers data privacy. Many, on the other hand, are governed by at least 32 separate statutes, each addressing a different legal issue. In the instance of a personal data leak at the Social Security Health Services (BPJS Kesehatan), it was determined that there was a breach of personal data security, with at least 279 million records leaked and exchanged on the internet. In accordance with Act No. 11 of 2008 on Information and Electronic Transactions, the owners of personal data or participants whose data has been disclosed can launch a civil complaint for data leakage and several other rules considering that the rules regarding the protection of personal data that are not only contained in one law. The impact that such cases can have is the potential misuse of other people's personal information to be misused for crimes, i.e. pretending to be someone else to take legal action.

The need for special arrangements regarding the protection of personal data as a form of respect for citizens' constitutional rights should be realized, as has been done in European countries, the United Kingdom, and even other Asian countries, by establishing and appointing a special supervisory agency to ensure the implementation of the personal data protection law.

REFERENCES

Books :
Makarim, Edmon. (2004). Introduction to the Law of Telematics (A Compilation of Studies), Jakarta : Raja Grafindo Persada.
Marzuki, Peter Mahmud. (2008). Research Method, Jakarta: Kencana Prenada Media Group.

Journals :
Cynthia, H. (2018). Registration of Personal Data Through Prepaid Cards in a Human Rights Perspective. *Jurnal HAM*. Vol 9 No 2. 191 – 204.

[13] Greeneaf, Graham, *Asian Data Privacy Laws-Trade and Human Rights Perspectives*. New York: Oxford University Press, (2014),p. 80.
[14] Latumahina, R. E, p. 329-337.
[15] Indriyani, M., Privacy Protection and Personal Data of Online Consumers On Online Marketplace System, *Justitia Jurnal Hukum*, 1.2 (2017) p. 202-203.
[16] Lia Sautunnida, Urgency of Personal Data Protection Act in Indonesia; Comparative Study of English and Malaysian Law, *Kanun Jurnal Ilmu Hukum*, 20.2 (2018), p. 378.
[17] *Ibid*, p. 320-328.
[18] Latumahina, R. E, p. 19.

Graham, Graham. (2014). *Asian Data Privacy Laws-Trade and Human Rights Perspectives*. New York: Oxford University Press. 80.

Indriyani, M. (2017). Privacy Protection and Personal Data of Online Consumers On Online Marketplace System. *Justitia Jurnal Hukum* Vol 1 No 2. 202-203.

Latumahina, R. E. (2014). Legal Aspects of Personal Data Protection in Cyberspace. *Jurnal Gema Aktualita* Vol 3 No 2. 18-19

Lia Sautunnida. (2018). Urgency of Personal Data Protection Act in Indonesia; Comparative Study of English and Malaysian Law. *Kanun Jurnal Ilmu Hukum* Vol 20 No 2. 378.

Priscilla, Fanny. (2019). Personal Data Privacy Protection Legal Comparison Perspective. *Jurnal Jatiswara* Vol 34 No 3. 245.

Sinta Dewi. (2016). The Concept of Legal Protection over Privacy and Personal Data Is Associated With the Use of Cloud Computing in Indonesia. *DEMO 2 JURNAL* Vol 94. 26.

Zaman, Akbari Amarul, Jumadi Anwar, Aryo Fadlian. (2021). Criminal Liability of BPJS Data Leak in perspective of ITE Law. *Jurnal De Juncto Delicti* Vol 1 No 2, 148.

Website :

Information Commission Office (ICO). "About ICO" https://ico.org.uk/about-the-ic . accessed Januari 25, 2022 at 13.45

Wahyunanda Kusuma Pertiwi on Kompas.com with the title of the article "Kronologi Kasus Kebocoran Data WNI, DIjual 0,15 Bitcoin hingga Pemanggilan Direksi BPJS" https://tekno.kompas.com/read/2021/05/22/09450057/kronologi-kasus-kebocoran-data-wni-dijual-0-15-bitcoin-hingga-pemanggilan?page=all accessed January 23, 2022 at 22:22.

Charisma Septi Jayanti
Faculty of Law Sebelas Maret University
Ir. Sutami St. No 36A, Jebres, Surakarta, Indonesia
Email : chariseptii@gmail.com

Suraji
Faculty of Law Sebelas Maret University
Ir. Sutami St. No 36A, Jebres, Surakarta, Indonesia
Email : suraji.esha@gmail.com