NEGREI
Academic Journal
of Law and Governance

Institut Agama Islam Negeri (IAIN) Curup, Indonesia
ISSN 2775-8621 (p), 2798-3803 (e)
volume 2, number 2, 2022
DOI: http://doi.org/10.29240/negrei.v2i1.5227

Comparison of Personal Data Protection Laws Using Narrative Policy Framework Between Indonesia, Malaysia, and Japan

Yusran Panca Putra
University of Bengkulu
Correspondence: yusranpanca@unib.ac.id

Abstract. The era of information and communication technology continues to grow and shows a significant increase. is a type of offensive maneuver used by a state, individual, group, or organization that targets computer information systems, infrastructure, computer networks, and or personal computer devices using malicious acts which usually originate from anonymous sources who steal, modify or destroy the specified target by hacking a vulnerable system. Cyberattacks can happen in any part of the country. The increasing use of the internet has the risk of increasingly massive hacking threats. The National Cyber and Crypto Agency (BSSN) noted that until April 2022, cyber attacks in Indonesia reached 100 million cases. This research benchmarks the situation of cyber attacks and personal data protection regulations in Indonesia with countries that have better handling of cyber crimes. The method is to compare narrative elements in the form of heroes, villains, and victims in each country, using the Narrative Policy Framework (NPF) analysis method. The Narrative Policy Framework is an approach or research framework on the public policy process, it is identified that the hero character represented by comprehensive personal data protection regulations has long been used by Japan and Malaysia. The character of heroes in Indonesia seems not to be too dominant because there are villains who are present in the form of the absence of unified regulations for the protection of personal data from the threat of cyber attacks

Keywords: Benchmarking, Cyber Attacks, Narrative policy framework

Introduction

The development of information and communication technology shows a significant increase. Improving the quality of Indonesian society in a sustainable manner that utilizes information technology and science is one of the goals of national development as well as a global challenge (Sudaryanti 2013). However, it should also be noted that the use of information technology is like a double-edged sword. Technology, if used properly, can help human life, but technology can also become very dangerous if its use is not restricted, such as in cases where personal data is not protected (Aprilianti 2020), as is currently happening in Indonesia, namely cyber attacks.

Cyber-attacks are part of the use of armed force when an attack is carried out by another state or subject to international law causing damage to the computer system of the country being attacked. However, it can only be called a war if there is evidence of physical damage and loss or loss of life (Parks 2013).

Interpol (2020) shows the vulnerability of cyber attacks in Europe and Asia during the Covid-19 pandemic but has not yet explained specifically the comparison of policy strategies in each region. This is complemented by other research (Sunkpho et.al.2018) which explains that compared to 5 (five) other ASEAN countries (Malaysia, Singapore, Thailand, Vietnam and the Philippines), only Indonesia does not have cyber security laws and laws cybercrime laws specifically. Indonesia only has an Electronic Information and Transaction Law that is enforced to accommodate the complexities of national cybersecurity affairs. Regarding data security issues, only Thailand and Indonesia do not yet have personal data protection laws. In fact, communist countries like Vietnam already have comprehensive laws governing data security and protection in one regulation called the Law on Cyber Information Security (LCIS).

Cyberattacks can happen in any part of the country. The increasing use of the internet has the risk of increasingly massive hacking threats. The National Cyber and Crypto Agency (BSSN) noted that until April 2022, cyber attacks in Indonesia reached 100 million cases. The types of cyber attacks that are often found in BSSN are dominated by ransomware and malware attacks (aptika.kominfo.go.id), Indonesia has a Personal Data Protection Law (PDP) as a regulation to maintain virtual space and public data security.

This research benchmarks the situation of cyber attacks and personal data protection regulations in Indonesia with countries that have better handling of cyber crimes. The method is to compare narrative elements in the form of heroes, villains, and victims in each country, using the Narrative Policy Framework (NPF) analysis method.

The Narrative Policy Framework is an approach or research framework on the public policy process, the NPF requires a narrative component that can be described as part of the policy content. The NPF contains the definition of the required policy narrative. First, the policy narrative must have at least one character whose meaning and presence can be identified. Second, the policy narrative must also refer to public policy interests.

NPF is able to review a policy peer to peer through narrative elements by examining the fundamental weaknesses of Indonesian policies compared to the state, so that it can become the basis for building policy solutions that are right on target. The emergence of NPF as part of the research paradigm is inseparable from the structuralism and post-structuralism paradigms, which contributed to the emergence and development of NPF as a research approach, both positivistic research and post-positivistic research (Salahudin 2019). The NPF research tradition is very helpful in describing social phenomena related to active narratives and strategies and social groups in the public policy process.

Research methods

This study uses a qualitative approach with the Narrative Policy Framework (NPF) analysis method. The NPF data analysis technique is in the form of descriptive statistics using tables and images that can clearly describe the research object. NPF is able to empirically explain policy processes and narratives regarding various policy issues at a certain level of analysis (Jones and Shanahan 2014). NPF is considered an appropriate research approach to use in the context of post-positivistic research, because of that recently many researchers are interested in using the NPF approach in their research, especially research related to big data issues, social media, policy narratives, strategy politics, and socio-cultural behavior in the context of public policy (Salahudin 2019). This research conducted a benchmarking study between Indonesia and comparator countries, namely Malaysia and Japan. The form of review of each policy through a simple NPF analysis methodology can be seen more clearly in Figure 1.

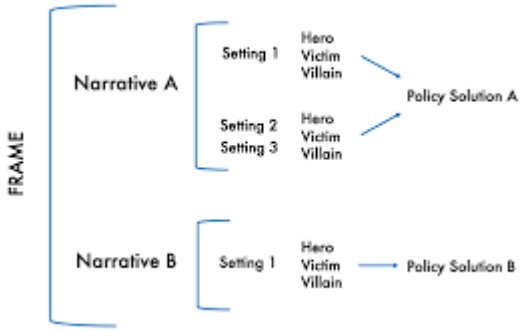

Figure 1 NPF Analysis Methodology

In each country, benchmarking will be carried out regarding the policy framework through several narrative elements, namely: settings and characters which include heroes, victims, and villains. Heroes are parties that are able to solve problems, villains are parties that cause problems, and victims are parties that are harmed. Characters in NPF do not have to be human, but can be abstract objects. From these characters a policy narrative plot is compiled by linking each character in a complete policy setting.

The policies implemented by each country were reviewed by observing cases of cyber attacks that occurred in each country, so that discrepancies were found between the situation in Indonesia and the comparator countries. The findings of this gap are then used to find policy solutions that need to be implemented by Indonesia in strengthening the protection of personal data security in Indonesia.

Discussion

Indonesia

In Indonesia, there is no law that specifically regulates the protection of personal data, but aspects of its protection are already reflected in other laws and regulations. The most basic aspects of privacy protection in Indonesia are listed in the Indonesian Constitution, namely the 1945 Constitution of the Republic of Indonesia (1945 Constitution), regulated in Chapter XA concerning Human Rights in Articles 28C to 28I, which include:

1. Article 28C (1) states that "Everyone has the right to develop himself through meeting his basic needs, has the right to education and to benefit from science and technology, arts and culture, in order to improve his quality of life and for the welfare of mankind". This article implicitly covers the right to feel safe and comfortable, to be let alone which is a basic human need. The right to benefit

from science and technology can also be a legal basis for the protection of privacy data in electronic systems.

2. Article 28D (1) states that "Every person has the right to recognition, guarantees, protection and fair legal certainty and equal treatment before the law". This article provides an explicit legal basis for protection of privacy.

The Indonesian Constitution does not explicitly regulate the protection of personal data in the 1945 Constitution. Likewise with privacy, even though the 1945 Constitution expressly states that there is protection for human rights. However, the 1945 Constitution shows that there is a strong and fundamental legal basis for further regulation for the implementation of privacy and privacy protection which includes privacy data. In the 1945 Constitution, provisions regarding data privacy are implicitly found in Article 28F and protection related to data privacy in Articles 28C and 28G (1) of the 1945 Constitution regarding freedom to store information and protection of data and information attached to it. Next, we will discuss laws and other regulations in Indonesia that contain protection for personal data.

1. Law Number 39 of 1999 concerning Human Rights
2. Law Number 19 of 2016 concerning Information and Electronic Transactions
3. Law Number 36 of 1999 concerning Telecommunications
4. Government Regulation Number 82 of 2012 concerning Implementation of Electronic Systems and Transactions
5. Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems
6. Academic Text of the Personal Data Protection Bill

Jepang

Japan has had personal data privacy protection regulations since 2000. The Data Protection Art is a legal rule adopted by the Federal Government of Japan. Keidanren, a representative body that specifically regulates industrial and trade issues in Japan, formulated legal rules related to privacy protection of personal rights. Regulating personal data as a form of protection for the Japanese government in the era of trade competition in the European Union, the Data Protection Art was born (Indriyani 2017). The principles of personal data protection in the Data Protection Art are that personal data is confidential, the

owner of personal data who is recorded knows with certainty 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 agreement, the owner of personal data has the right to make changes or corrections to his personal data, and if there is a violation of the use of personal data, it is required to restore or compensate for damages caused by violations that occur at a later date.

Malaysia – The Personal Data Protection Act No. 709 of 2010

Malaysia has The Personal Data Protection Act No. 709 of 2010(PDPA Malaysia) "An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidentally thereto". There are seven principles in PDPA Malaysia adopted from the EU Data Protection Directive from the OECD Guidelines or APEC Framework. With PDPA 2012 in Malaysia, the guarantee of personal data security from internet users has increased. Because Malaysia's PDPA refers a lot to the rules in the EU Data Protection Directive from the OECD Guidelines or APEC Framework, Malaysia also stipulates in PDPA that it is not permitted to transfer personal data outside Malaysia, unless permission has been obtained from the Minister of Information, Culture and Communication and the country or place which is the place for transferring personal data can provide guarantees of personal data protection that is equivalent to the PDPA provides (Greeneaf 2014).

Benchmarking menggunakan Narrative Policy Framework

From the discussion of laws governing the protection of personal data in Indonesia, Japan and Malaysia, an analysis was carried out using the Narrative Policy Framework, as shown in Table 1 below.

Table 1 Benchmarking Using Narrative Policy Framework

No	Character	Jepang	Malaysia	Indonesia
1	Hero	Regulation: Data Protection Art Literasi: increasing security awareness	Regulation: PDPA - Organization: NACSA - Literasi: increasing security awareness	Regulation: Criminal Code, ITE Law, Banking Law, Telecommunications Law, Consumer Protection Law, Population Law, Human Rights Law, Population Administration Law, Public Information Disclosure

				Act, Health Law, PP No 71/2019, Minister of Communication and Information No 20/2016 - Organization: BSSN
2	Villain	- Cyber attacks - *Security Awarness*	- Cyber attacks - *Security Awarness*	- Cyber attacks - *Security Awarness* - There is no integrated regulation for personal data protection
3	Victim	Security of people's personal data	Security of people's personal data	Security of people's personal data

Based on the results of the benchmarking/comparison in the table above, we can see that each country has its own heroes, villains and victims, where Malaysia and Japan Sudan's personal data protection regulations are accommodated in one product, namely PDPA and Data Protection Art, while Indonesia has not. accommodated in one product, there are many regulations that regulate data protection, namely the Criminal Code, the ITE Law, the Banking Law, the Telecommunications Law, the Consumer Protection Law, the Population Law, the Human Rights Law, the Population Administration Law, the Public Information Disclosure Law, the Health Law, PP No 71/2019, Minister of Communication and Informatics No 20/2016, to produce comprehensive personal data protection regulations, Indonesia needs integrated regulations.

Conclusion

The high level of community activity involving digital technology is an easy target for cyber crimes. The threat of cyber attacks in the new normal era is not only increasing in number but also getting more adept at approaching their victims. Not only using technology, a social engineering approach is also taken to be able to infiltrate the personal data of potential victims. Through benchmarking with the Narrative Policy Framework (NPF) analysis method, it was identified that the hero character represented by comprehensive personal data protection regulations has long been used by Japan and Malaysia. The character of heroes in

Indonesia seems not to be too dominant because there are villains who are present in the form of the absence of unified regulations for the protection of personal data from the threat of cyber attacks.

Bibliography

Sudaryanti, K. D. 2013. "Perlindungan Hukum Terhadap Investor Dalam Perdagangan Obligasi Secara Elektronik." Kertha Wicara 2(1):1–5.

Aprilianti, Ira. 2020. "Hari Konsumen Nasional Perlindungan Data Pribadi Di Tengah Pandemi Covid 19." Referensi.Eslam.or.Id 1. Retrieved November 14, 2020 (https://referensi.elsam.or.id/2020/04/hari-konsumen-nasionalperlindungan-data-pribadi-di-tengah-pandemi-covid-19/)

Andreya, Ericha 2022 "Antisipasi Bersama Tingkatkan Sistem dan Cegah Serangan Siber" https://aptika.kominfo.go.id/2022/09/antisipasi-bersama-tingkatkan-sistem-dan-cegah-serangan-siber/

Parks, P. J. (2013). Cyberwarfare. Reference Point Press.

Salahudin.2019. Filosofi dan Metodologi Narrative Policy Framework (NPF). Universitas Muhamadiyah Yogyakarta.

Jones, Shanahan (2014).The science of stories: Applications of the narrative policy framework in public policy analysis

Sunkpho, Jirapan., Sarawut Ramjan, Chaiwat Ottamakorn. 2018. "Cybersecurity Policy in ASEAN Countries". Information Institute Conferences, Las Vegas, NV, March 26-28.

Indriyani, M. 2017. "Perlindungan Privasi Dan Data Pribadi Konsumen Daring Pada Online Marketplace System." Justitia Jurnal Hukum 1(2):191–208.

Greeneaf, Graham. 2014. Asian Data Privacy Laws-Trade and Human Rights Perspective. New York: Oxford University Press.

https://aptika.kominfo.go.id/2022/09/antisipasi-bersama-tingkatkan-sistem-dan-cegah-serangan-siber/