International Conference on Education
Vol. 1, June 2022, pp. 145-150
Faculty of Teacher Training and Education, Universitas Ahmad Dahlan

Initiating anti-personal data abuse education toward the 5.0 era

Dwi Herdila Cahyani Putri*, Nadia Regita Pramesti, Salsya Yunita Safitri, Muhammad Randy Ardianto
Universitas Ahmad Dahlan, Jl. Jend. Ahmad Yani, Kragilan, Tamanan, Banguntapan, Bantul, Yogyakarta, 55191 Indonesia
*Corresponding e-mail: dwi2015024184@webmail.uad.ac.id

Abstract

Cybercrime has become a threat in different human lives, including the misuse of personal data. The weakness of the cyber world is not only due to the lack of regulation or the absence of regulations regarding cyber security and personal data protection, but the lack of public knowledge that makes it easy to submit personal data. Therefore, we need an education system that can overcome these problems, and the Anti-Personal Data Abuse Education system is an education system that provides knowledge of the security of managing personal data and information to the public. This study aims to find out how the problem of misuse of personal data in Indonesia is currently and how to formulate efforts to prevent misuse of personal data through Anti-Personal Data Abuse Education. This study uses a normative juridical method with a Conceptual Approach. In conclusion, Anti-Personal Data Abuse Education is needed as an education system that can educate the public towards the 5.0 era.

Keywords: personal data abuse, society 5.0

How to cite: Putri, D. H. C., Pramesti, N. R., Safitri, S. Y., & Ardianto, M. R. (2022). Initiating anti-personal data abuse education toward the 5.0 era. *Proceedings of the International Conference on Education, 1,* 145-150.

INTRODUCTION

The development of Information and Communication Technology shows a significant increase. Improving the quality of Indonesian society sustainably by utilizing information technology and science is one of the national development goals and a global challenge. This development has led to a "borderless world", which means that everyone can access everything via the Internet.

In the development of technology and information technology, personal data information, including name, email, and mobile number, is precious because it can have economic value in the business world. That makes some actors or technology users take the time to create applications or sources of income through information and communication technology. The technology continues to be developed to make it easier for the global community to carry out their activities in the digital era. Based on internet world stats data, Indonesia's internet users reached 212.35 million in March 2021. Indonesia is in third place with the most internet users in Asia with this number.

Currently, people's dependence on information technology is getting higher so that the risks they face are higher (Darmawan, 2017). The development of internet technology resulted in the emergence of a new crime called cybercrime through the internet network. The emergence of several cybercrime cases in Indonesia, such as fraud, hacking, wiretapping other people's data, and data manipulation with computer programs to access other people's data.

The exchange of information is effortless because almost all social media are user-generated content. The ease of disseminating this information does not rule out the possibility of its users spreading personal information to the general public. That is what makes the basis for cybercriminals to carry out their criminal tactics. Based on ID-SIRTII data, the number of cyberattacks increased, from 28,430,843 in 2015 to 135,672,984 in 2016. Moreover, 47% of all

Received March 12, 2022; Revised May 25; Accepted June 29, 2022

cases are malware attacks, 44% are frauds, while the rest are in the form of other cybercrimes, such as website defacement, data manipulation and data leakage activities.

On the other hand, BSSN also noted that the number of cyberattacks in 2020 reached 495.3 million, an increase of 41 % from the previous year in 2019, which was 290.3 million. Bareskrim also conveyed an increase in cybercrime reports. In 2019, there were 4,586 police reports filed through Patrolisiber, an increase from the previous year of 4,360 reports in 2018. On the one hand, this increase in the number of internet users is good news for increasing the ability of the global community to adapt to technological growth, but on the other hand, security threats. Cyber is also increasing.

As a state of law, Indonesia has provided several regulations regarding this matter. However, the reality is that the regulations given by the government to minimize cybercrime are still not able to cover it up. The weakness of the legal umbrella provided by the government makes the perpetrators of crimes increasingly ventured to carry out their crimes. Likewise, the lack of participation from the global community in reducing the number of cybercrimes makes these crimes still rife. There is still a lack of knowledge and public awareness of efforts to protect personal data. Those who are not aware of the law often become victims of these crimes (Noor, 2020).

The public needs to understand personal data protection regulations, principles, and practices. So that personal data and information are not misused by irresponsible parties. Therefore, preventive measures are needed to be able to overcome this. In particular, this writing is expected to be a recommendation for the government to protect personal data and information through Anti-Personal Data Abuse Education.

RESEARCH METHOD

The normative juridical research method is a legal research method that examines library materials or mere secondary materials (Soekanto & Mamudji, 1994). The data analysis method is carried out by collecting data through the study of library materials or secondary data, including primary legal materials, secondary legal materials and tertiary legal materials, in the form of documents and applicable laws and regulations relating to personal data protection. This research uses qualitative data analysis methods, normative juridical with a conceptual approach. A conceptual approach is used to analyze and comprehensively examine the concept of misuse of personal data.

RESULTS AND DISCUSSION

Personal data protection problems and regulations in Indonesia

Data protection in general terms refers to the practices, safeguards, and binding rules put in place to protect personal information and ensure that data subjects remain in control of their information. In short, data owners must decide whether they want to share information or not, who has access, for how long, for what reasons (Djafar, 2019). In the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD defines personal data as “any information relating to an identified or identifiable individual (data subject)”. Personal data is generally divided into two categories: General Personal Data, such as name, date of birth, address, email address, location data, IP address, web cookie; and Specific (Sensitive) Personal Data, such as race, ethnicity, religion, political views, sexual orientation, genetics, mental and psychiatric conditions, criminal records.

Article 1 number 1 and 2 Regulation of the Minister of Communication and Information Technology no. 20 of 2016 concerning Protection of Personal Data in Electronic Systems states that personal data is intended as a clear and precise identity of a person, which is the determination of personal evidence against him which is maintained, kept accurate and kept

confidential. While Article 2 number 1 regulates the acquisition, collection, processing, analysis, storage, appearance, announcement, delivery, dissemination and destruction of personal data is the protection of personal data in an electronic system that respects personal data as privacy.

The development of science and technology today is popularly used big data. Big data is considered a solution in processing data because it can process large and varied data and make accurate attachments, thus making big data not only used by the government but also by the private sector. Companies use it to study consumer behaviour, such as loyalty, visiting patterns, purchase history, and others, to market their products or services effectively. However, the misuse of big data can also threaten a person's privacy. Misuse of personal data can also unwittingly occur because it is the potential victim's negligence (society) in carrying out their daily activities (Situmeang, 2021). For example, without us realizing it when downloading the application, attaching personal data in the platform or form, and so on, that could potentially cause harm to the data owner. In Indonesia, several studies have shown that the awareness of the Indonesian people towards the protection of their data on the internet is still low. As a result, the Indonesian people do not take this case of violation of the protection of personal data seriously (Angendari, 2019).

Misuse, theft, sale of personal data violate the law in information technology. It can also be categorized as a violation of human rights because personal data is part of human rights that must protect (Situmeang, 2021). The fourth amendment to the 1945 Constitution is regulated regarding human rights (as a form of guarantee for protecting the rights of citizens). That is also in line with Law Number 39 of 1999 concerning Human Rights (Kemenkumham, 2019), which includes several articles which guarantee the protection of the right to privacy of citizens: Article 14 Paragraph (2) states that Everyone has the right to seek, obtain, possess, deviate, process, and convey information by using all types of available means. Article 28 G states that every person has the right to protection for personal, family, honour, dignity and property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that constitutes a threat rights.

Indonesia signed the OECD guidelines in 2004 and followed the guidelines for enforcing privacy and data protection regulations. Indonesia as an APEC member has also followed the 2004 APEC Privacy Framework (APEC Privacy Framework). However, Indonesia does not have policies or provisions that specifically regulate the protection of personal data; so far, it is still contained separately in several laws and regulations.

(1) Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions
(2) Government Regulation Number 82 of 2012 concerning Electronic System and Transaction Operators
(3) Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998 concerning Banking
(4) Law Number 8 of 1999 concerning Consumer Protection (Consumer Protection Law)
(5) Law Number 39 of 1999 concerning Human Rights (Human Rights Law)
(6) Law Number 23 of 2006 concerning Population Administration as amended by Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration (Law on Population Administration)
(7) Law Number 36 the Year 2009 concerning Health (Health Law)
(8) Law Number 14 of 2008 concerning Public Information Disclosure (Public Information Disclosure Act)
(9) Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems (Kominfo, 2016).

As for the Draft Law on Personal Data Protection, the provisions regulated in the Bill on Personal Data Protection are deemed too bureaucratic. The process to obtain legal certainty will be very long, convoluted and uncertain.

Anti-abuse of personal data education as a preventive effort

Personal data protection in the digital world is increasingly important because the use of electronic documents and internet networks is increasing, primarily since the covid 19 pandemic, almost everyone works, studies transact from home by relying on the internet network. In this case, information and communication technology (ICT) developments are used in the education sector, namely the online-based Feeder application as the Higher Education Database (PD-DIKTI) in Indonesia, which also does not rule out the possibility of data misuse.

The protection of personal data is a shared responsibility for both the community, individuals and legal entities, and the government. These efforts can be through preventive and repressive efforts. Preventive efforts, for example, through prudence in providing personal data and surveillance efforts. Legal protection for misuse of personal data can be done through self-regulation or prevention efforts if the current regulations do not cover the system for misuse of personal data (Wulansari, 2015).

It is not an intelligent move to expect other parties to protect personal data on the internet, be it governments or Internet service providers. Article 26 of the ITE Law states that the use of personal data through electronic media must be based on the consent of the person concerned; therefore, a phenomenon that is so massive that efforts to protect personal data need to be advocated. The goal is to strike a balance between concern for the protection of privacy of information and the concern and desire of individuals to share information about their data (Noor, 2020).

Anti-Abuse of Personal Data Education is a new solution offering to deal with the misuse of personal data. Based on Law no. 20 of 2003 concerning the National Education System, education is a conscious and planned effort to create a learning atmosphere. They are a learning process so that students actively develop their potential to have religious, spiritual strength, self-control, personality, intelligence, noble character, and the necessary skills: himself, society, nation and state. The above definition emphasizes that: First, an unplanned effort, let alone an unintentional one, is not education. Second, creating a learning atmosphere and teaching students are the fundamental concepts of educational activities. Third, the activities that are realized and planned must be directed at developing students' potential. Fourth, the aspects included in the self-potential of students include dimensions: spiritual, self-control, personality, intelligence, noble character, practical skills (Ilham, 2019).

Anti-Data Abuse Education System must be based on philosophical, sociological, and juridical foundations:

The philosophical foundation is based on the legal ideals in the Preamble to the 1945 Constitution, namely the purpose of establishing a State Government, including "The state protects the entire Indonesian nation and all of Indonesia's bloodshed..." And "Educating the nation's life". That means that the state is obliged to provide protection and guarantee human rights, including personal data protection.

On a sociological basis, Indonesian society today is also part of the information society in a global interconnection space. Therefore, the protection of personal data privacy is necessary to provide security for every individual, both Indonesian citizens and foreign nationals in Indonesia, about the collection, processing, administration and dissemination of Personal Data.

The juridical basis, namely the 1945 Constitution of the Republic of Indonesia, has been amended, namely Article 31 concerning National Education and Law of the Republic of Indonesia Number 20 of 2003 concerning the National Education System.

It is expected that the Anti-Abuse of Personal Data Education includes the principles of data privacy protection, following (da Cunha et al., 2019).

(1) Restrictions on collection: there should be limits in collecting private data. The data obtained must use legal and fair means and, if necessary, use the person's knowledge and consent.
(2) Data quality: privacy data must be by the purpose for which the data is used and must be accurate, complete and up to date.
(3) Specification of the purpose: the purpose for which the data was collected must be specific, and any subsequent use of the data must be limited only to the specification of that purpose.
(4) Use of restrictions: data may not be disclosed, publicly available or used for purposes other than the specific purpose except (a) with the consent of the data owner or (b) with the consent of the legal authority.
(5) Security measures: data must be protected with appropriate safeguards from loss, damage, use, alteration or disclosure.
(6) Disclosure: there should be a general policy regarding the disclosure of private data.
(7) Individual participation: individuals should have the right to be informed about their data and delete or correct their incorrect data.
(8) Accountability: the data controller is responsible for complying with these measures.

CONCLUSION

Misuse of personal data is a consequence of the development of information and communication technology and life leading to the era of society 5.0. The regulation of personal data protection in Indonesia has not yet become a definite legal policy for the public. Apart from that, the public's ignorance and lack of knowledge about personal data protection are essential to pay attention to. Advocacy efforts are needed from an early age as self-regulation through an anti-personal data misuse education system. The Anti-Data Abuse Education System as a solution is based on philosophical, sociological, and juridical foundations, which are expected to include the principles of data privacy protection.

REFERENCES

Angendari, D. A. D. (2019). The case of Dukcapil data: Lessons on privacy and personal data in Indonesia. http://theconversation.com/cases-datadukcapil-learning-terkait-privasi-dan-data-private-di-indonesia-121264

da Cunha, T. E., Helan, Y. G. T., & Thaddeus, D. W. (2019). The Implementation of the Feeder Application Is Linked to the Protection of Lecturer and Student Personal Data Judging from Law Number 12 of 2012 concerning Higher Education. *Champion's Familiar Journal*, *4*(3), 21-30.

Ilham, D. (2019). Initiating value education in the national education system. *Didactics: Journal of Education, 8*(3), 109-122.

Kemenkumham. (2019). *Law Number 39 of 1999 concerning Human Rights*.

Kominfo. (2016). *Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems*.

Napitupulu, D. (2017). Study of the Role of Cyber Law in Strengthening National Information System Security. *Deviance Journal of Criminology*, *1*(1).

Noor, M. U. (2020). The Relationship of Millennial Generation Education Level to Privacy and Personal Data Protection Efforts on the Internet. *Bibliotics: Journal of Library and Information Studies*, 154-156.

Situmeang, S. M. T. (2021). Misuse of Personal Data as a Perfect Form of Crime in Cyber Law Perspective. *SASI, 27*(1), 38-52.

Soekanto, S., & Mamudji, S. (1994). *Normative Legal Research: A Brief Review*. Jakarta: King Grafindo Persada.

Djafar, W. (2019) *Personal Data Protection Law in Indonesia: Landscape, Urgency, and Need for Update*.

Wulansari, F. (2015). Legal Protection of Customer's Personal Data in the Implementation of Internet Banking Services Linked to Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking.