KnE Social Sciences

VCOSPILED 2021
2nd Virtual Conference on Social Science In Law, Political Issue and Economic Development
Volume 2022

Knowledge E
enriching | engaging | empowering

Research article

Personal Data Collection: Recent Developments in Indonesia

Marchelfia Pratiwi P, Emy Rosnawati, Mochammad Tanzil Multazam*, and Noor Fatimah Mediawati

Universitas Muhammadiyah Sidoarjo, Sidoarjo, Indonesia

ORCID
Mochammad Tanzil Multazam: https://orcid.org/0000-0002-6373-1199

Abstract.
This study explains the relevant regulations on sanctions against perpetrators of personal data collection in the Indonesia cyber world. This research is based on a normative juridical approach. The results of this study show that to create legal certainty, it is necessary to establish a law that regulates clearly or specifically, is organized and comprehensive in the protection of personal data, and resolves existing laws governing personal data in a clear mechanism and in coordination with law enforcement.

Keywords: cyber law, personal data, privacy data retrieval sanction

Corresponding Author:
Mochammad Tanzil Multazam;
email:
tanzilmultazam@Umsida.ac.id

Published: 01 August 2022

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the VCOSPILED 2021 Conference Committee.

1. Introduction

Based on data obtained from APJII or the Association of Indonesian Internet Service Providers, it is stated that every year there is an increase in internet network users in Indonesia. In 2014, internet network users reached 88 million people. In 2016, data on Indonesian internet service providers increased users to 132 million. And in 2017 the increase in internet network users increased, amounting to 143.26 million. This figure continued to increase until 2018 which was 171.17 million. developments in the use of internet networks which resulted in many users using social media or social networks. Based on data in hootsuite (We are Social) or a tool to track and manage the number of social media users, in Indonesia in 2019 there were 150 million active social media owners. The increase reached 15% or 20% from 2018 and then 130 million mobile social media users or 8.3% or around 10% from 2018. So there are legal problems that arise, for example problems related to personal data protection. or called (the protection of privacy rights).[

One example of a case that occurs in a bank account is seen on an Automated Teller Machine (Atm) receipt. In this case, the suspect committed the act of stealing an account belonging to the General Elections Commission (KPU), by obtaining the identity of the

victim through a transaction receipt that had been discarded around the ATM machine. On the paper there is the victim's account number and the customer's balance is listed. Then the suspect used an ATM receipt to duplicate the identity card, by taking the victim's owner's data through the KPU's official website. After duplicating the identity card of the victim's owner, the suspect went straight to the bank with a falsified account book to take money and admitted that the Atm card had been left in the ATM machine. The data that has been made by the suspect is made exactly the same as that of the victim, so the Bank believes that the Atm card has been left in the Atm machine.[2]

Privacy data protection according to the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 is the protection of personal data in electronic systems including protection against the acquisition, data collection, processing, analysis, storage, appearance, announcement, sender, dissemination and destruction of personal data.[3]

In Indonesia, until now there is no strict protection in protecting personal data, or it can be said that personal data is still vulnerable and easy to be accessed and misused by others. So that cases of theft of personal data in the cyber world often occur. As for preventive measures, namely people who have access rights to their personal data, but do not understand how to secure important related data, so they can be said to be vulnerable and create opportunities for other people to enter or take advantage of the situation.

According to Fajrin widiyaningsih [4], explained that the theft of electronic documents is defined as "sariqah", which is someone taking other people's goods secretly from their storage area, so that the punishment for the thief of the document is different from the rules in the transaction information law. electronic because in this case it can be analyzed from the theft case, it can be punished by Islamic law, namely cutting off the hand or not. To change or damage an electronic document is equated with "hirabah", which is not being able to take someone's property openly without killing the owner, then the punishment can be cutting off the hands and feet crosswise. But in reality the law in force in Indonesia is the Information and Electronic Technology Law (UU ITE), so the punishment for document theft is reduced to "ta'zir" punishment, namely imprisonment and fines.[5]

Furthermore, according to Dwi Nugrahayu Devianti, Prija Djatmika, and Sukarmi, Lecturer of the Faculty of Law, Universitas Brawijaya, explaining that the legal consequences for users of other people's personal data, the data used is the result of data changes, the user can be subject to criminal sanctions for data falsification, if the data used If the original data belongs to someone else, then it will be subject to criminal sanctions

in the form of data theft. Owners of documents used by other people in lending and borrowing online applications can apply for compensation.

Personal Data is defined as any data about a person either identified and/or can be identified separately or in combination with other information either directly or indirectly through electronic and/or non-electronic systems. In chapter 2 article 3 paragraph (1) personal data consists of[6]:

1. General Personal Data, namely personal data consisting of: name, gender, nationality, religion and personal data combined to identify a person;
2. Personal Data is Specific, consisting of: Health data and information, biometric data, genetic data, health records, child data and other data.

According to Widodo, 2013 [7], cyber crime is every activity of a person or group of people and legal entities that use computers as targets of crime and attempts to use computer facilities or computer networks without the person knowing. With the aim of knowing things that are private so that it can cause changes to computer networks. The existence of criminal activity on computer networks can be classified into 2 (two) groups, namely:

1. Fraud of Data, is an unofficial data that is input into a computer system or network and the official data is stored, then converted into invalid or unofficial data again. The form of fraud is shown to falsification or separation of input data with output;
2. Program fraud is the act of a person changing a program on a computer network either directly or at the computer location and carried out remotely through a data communication network.

There are several types of cyber crime itself when viewed from its activities, namely [8]:

1. Carding is shopping that uses someone else's credit card number and identity, which was obtained illegally, by stealing data on the internet. The name for this perpetrator is carder. Another name for the crime is cyberfront or fraud against cyberspace.
2. Hacking is a system that breaks into other people's computer programs. Hackers themselves are people who like to tinker with computers, who have the expertise to create and read certain programs and break through security systems on computers.

3. Cracking is hacking for malicious purposes. The term for ”cracker” is a black hat hacker. In contrast to ”carders” who only peek at credit cards, ”crackers” peek at customers’ deposits at various banks or other sensitive data centers for their own benefit. even though they both penetrate the security of other people’s computers, hackers are more focused on the process, while cracking is more focused on activities to enjoy the results of their crimes.
4. Phishing is an activity to lure computer users on the internet (users) to want to provide information on the user’s personal data (username) and password (password) on a website that has been hacked by the perpetrator, which then changes the appearance of the website (deface). Phishing is usually directed at online banking users, because it contains vital user data and passwords.
5. Defacing is an activity that changes pages on other parties’ websites and websites. As happened on the website of the Ministry of Communication and Information, the Golkar Party, BI and KPU at the time of the election. In defacement, there are those who are just for fun, or show their skills and show off their ability to make programs, but there are also those who commit crimes, namely by stealing data and trading it to other parties.

2. Research Methods

In writing this article, the research method is normative juridical. This writing method uses materials and existing legal rules.[9] This research is based on the study of the rule of law that contains the content of theoretical concepts related to legal issues on what the author is researching.

The problem approach is the basic method in conducting research. The author uses the Statue Approach or statutory approach, which is an approach that is carried out by reviewing all laws and regulations relating to the problem of theft of personal data on social media and electronic transactions.

The following are the types of legal materials used by the authors to collect research data, including primary legal material sources consisting of a collection of several sources that have binding legal force, as follows:

1. The 1945 Constitution of the Republic of Indonesia article 28G (paragraph 1) concerning the right to personal protection;
2. Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE);

3. Law Number 23 of 2006 concerning Population Administration as amended to Law Number 24 of 2013;
4. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions;
5. Regulation of the Minister of Communication and Information Number 20 of 2016.
6. The Criminal Code (Criminal Code);
7. Civil Code (KUH Perdata);
8. Personal Data Protection Bill.

Then secondary legal materials consist of materials used to explain previous research, including legal books, scientific articles and several journals that are relevant to legal issues. The author uses a deductive analysis, which uses an analysis of legal materials from general to specific matters, which are associated with the problems studied. The analysis is carried out critically using legal principles in a systematic and orderly manner with the aim of obtaining answers to problems.

3. Results and Discussion

3.1. Types of Personal Data Crime in Cyber World Under the ITE Law

Along with the development of information and technology in the world of social media or the Internet in particular, which is not far from various legal issues, especially regarding the theft of personal data on social media, so that there are several types and motives of crime in the cyber world, namely:

1. Cyber crime as a pure crime

Where the person who commits a crime that is committed intentionally, where the person is intentionally and planned to do damage, theft, anarchic actions, against an information system or computer system.

1. Cyber crime as an act of gray crime

Where this crime is not clear between criminal crimes or not because he broke into but did not damage, steal or commit anarchic acts against the information system or computer system.

Meanwhile, based on the type of activity, the modus operandi of cybercrime can be divided into:

1) Unauthorized Access to Computer System and Service

Crimes committed by entering or infiltrating a computer network system illegally, without permission or without the knowledge of the owner of the computer network system that he enters. Usually criminals (hackers) do so with the intention of sabotage or theft of important and confidential information. However, there are also those who do so only because they feel challenged to try their skills to penetrate a system that has a level of protection.

1. Infringements of Privacy

Crimes directed against someone's information which is very private and confidential. This crime is usually guided by a person's personal information stored on a computerized data form, if known by others it can harm the victim materially or immaterially, such as credit card numbers, ATM card PIN numbers, someone's data used for online debt. , hidden disability or disease and so on.

3.2. Sanctions or Legal Basis for Types of Activities in Several Provisions of Law 11 of 2008

1. The legal basis for the crime of Unauthorized Access to Computer System and Service, is Article 30 of the Electronic Information and Transaction (ITE) Law which reads "every person intentionally and without rights accesses another person's computer or computer system, with the aim of obtaining electronic information. or electronic documents by breaking through, breaking into the security system". Meanwhile, the sanctions contained in the ITE Law are article 30 paragraph 3, article 35, and article 46 paragraph 3, explaining "everyone who fulfills the elements as referred to in article 30 paragraph 3, shall be sentenced to a maximum imprisonment of 8 (eight) years. and a maximum fine of IDR 800,000,000 (eight hundred million rupiah).

2. The legal basis for the crime of Infringements of Privacy, is contained in Article 26 of Law Number 11 of 2008 concerning ITE, which reads "the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned, every person whose rights are violated can be file a lawsuit for the losses incurred under this law.

3. The legal basis for cracking is articles 30, 31, 32, 33 and 35. Based on these articles, cracking and hacking are actions that are prohibited by the ITE Law. Within the scope of the enforcement jurisdiction, it is contained in Article 2 jo. Article 37 of the ITE Law, which reads ”every person who commits a legal act, both within the jurisdiction of the Republic of Indonesia and outside the jurisdiction of the Republic of Indonesia which has legal consequences and can harm the interests of Indonesia”.
4. The legal basis for carding is article 51 in conjunction with article 34 of the ITE Law which regulates actions taken by people who use credit cards, but does not include merchants or managers who can also be carding actors. Article 51 of the ITE Law states that anyone who intentionally and unlawfully violates the provisions of Article 34 paragraph 1, Article 34 paragraph 2, Article 35 or Article 36 paragraph 1, shall be sentenced to a maximum imprisonment of 10 years or a maximum fine of Rp. . 2,000,000,000, - (two billion rupiah).

Based on an explanation on the legal basis of several types of cyber crime activities, the ITE Law actually regulates the protection of a person’s personal data. This can be seen in the provisions contained in Article 26 of Law Number 11 of 2008 concerning ITE [?] which reads ”the use of any information through electronic media concerning a person’s personal data must be carried out with the consent of the person concerned, unless otherwise specified by the laws and regulations. From the explanation of the article, the use of information and electronic technology, especially regarding the protection of personal data, is a part of personal rights (privacy rights) which must receive protection from the State. Personal rights can be explained as follows:

1. Personal rights are the rights to enjoy a private life and be free from all kinds of interference
2. Personal rights are the rights to be able to communicate with other people without spying
3. Privacy rights are rights to monitor access to information about a person’s personal life and data.

When analyzed from the explanation of Article 26 of the ITE Law, there are still weaknesses, namely the absence of guarantees for compensation for the owner of the data used by the organizer or service provider with the aim of getting a profit, because there is still no regulated on sanctions for compensation for those who disadvantaged is the owner of the data. Therefore, it is necessary to reformulate an existing legal norm,

through the provisions of Article 28J paragraph 2 of the 1945 Constitution, Supreme Court Decision Number 6/PUU-VIII/2010, and Number 006/PUU-I/2003 which states his views regarding the protection of privacy must be protected by the state.

In this case the legal interest, these rights can be reduced as long as through the mechanism regulated in the law, because the definition of personal data previously mentioned does not adequately explain what is included in individual data, then in article 84 paragraph 1 of the Law, Law Number 24 of 2013 concerning Population Administration explains personal data which includes:

1. Information on physical and/or mental disabilities;
2. Fingerprint;
3. Iris of the eye;
4. Signature; and
5. Another data element that is someone's disgrace.

In addition, Article 95a of Law Number 24 of 2013 concerning Population Administration also states that there are criminal sanctions for violators as referred to, because there is a criminal element, then the provisions contained in Law Number 24 of 2013 concerning Population Administration need to be carried out reformulation of legal norms. As for the rules contained in Article 22 of Law Number 36 of 1999 concerning Telecommunications, it is stated that "everyone is prohibited from carrying out unlawful, illegal, or manipulating acts such as accessing telecommunications networks, accessing telecommunications services, and accessing telecommunications networks. special telecommunications.

Currently the existing law in Indonesia has a draft law on the protection of personal data, with the aim of combining a privacy regulation on personal data that has been spread into a separate law with the aim of providing boundaries between rights and obligations related to income and use of personal data. Article 29 of the Bill on the Protection of Personal Data states that "every owner of personal data and the operator of an electronic system can file a complaint with the Minister for the failure to protect the confidentiality of personal data". The complaint as referred to in paragraph (1) is intended as an effort to resolve the dispute by deliberation or through other alternative settlement efforts. The Minister can coordinate with the heads of the supervisory and regulatory agencies of the sector to follow up on the complaints as referred to in paragraph (1).

From a provision contained in the Bill on the Protection of Personal Data, until now there is no comprehensive special law that regulates the protection of personal data,

in the sense that the regulation is not scattered or is not regulated in several provisions or regulations such as currently available.

3.3. Regulatory Efforts in Personal Data Protection

In the effort to regulate the right to privacy on personal data, it is a manifestation of the recognition and protection of basic human rights. Therefore, the preparation of the Bill on the protection of personal data has a strong philosophical foundation and can be accounted for. The philosophical foundation in question is Pancasila which is the ideal of law (rechtsidee) as well as the idea of realizing the law to what it aspires to. So that in the Regulation of the Minister of Communication and Information Number 20 of 2016 concerning the protection of personal data, it can be processed through the acquisition and collection, processing and analysis, storage, appearance, announcement, sending, dissemination and opening of access or destruction.

Sunaryati Hartono said that the application or implementation of the national legal system (in a broad sense) which regulates the life of society, nation and state, especially the Indonesian legal system, needs to pay attention to its conformity with the following matters:

1. Values that live in society (whether the national legal system is in accordance with the values that live in society);
2. Philosophy of law (whether the national legal system is in accordance with the legal philosophy recognized by Indonesia);
3. Legal norms;
4. Legal institutions;
5. Processes and procedures to be applied in a national legal system;
6. Human resources in implementing a legal system adopted;
7. Educational institutions and legal education systems related to the legal system currently adopted or to be adopted;
8. Facilities and infrastructure in implementing the relevant legal system.

In this case, the juridical basis for personal data protection refers to Article 28G of the 1945 Constitution of the Republic of Indonesia. Therefore, personal data protection is a form of embodiment of the constitutional mandate that must be regulated in the form

of a law. Article 28G of the 1945 Constitution of the Republic of Indonesia in the fourth amendment states that ”everyone has the right to personal protection, family, honor, dignity and property under his control, and has the right to a sense of security and protection from the threat of fear of doing or do not do something that is a human right”. With the decision of the Constitutional Court Number 006/PUU-I/2003, it is emphasized that in protecting privacy data there must be a law that has been clarified in the form of a decision at the Constitutional Court which affirms that with provisions involving human rights, it must be contained in the Constitutional Court. makers in legislation.

Judging from the legal consequences in relation to the protection of administrative data in addition to administrative sanctions or civil law problems for perpetrators of misuse of privacy data. The civil lawsuit is based on an element of error or (fault liability, liability based on fault principle). What has been regulated in Article 1365Bw, as explained in Article 1365 of the Civil Code, states ”an act can be held legally responsible as long as it fulfills four elements, namely: the act, the element of error, the loss and the causal relationship between the error or loss.

In a preventive measure to avoid failures in the protection of personal data according to the regulation of the Minister of Communication and Information Number 20 of 2016 is that the protection of personal data that is managed must be carried out by every organization on an electronic system, at least in the form of activities that include:

1. Increase awareness of human resources in the environment to provide protection of personal data in the electronic systems they manage; and
2. Conduct training on preventing failure of personal data protection in the electronic system it manages for human resources in the environment.

Disclosure of public information which has several descriptions or functions to ensure that there is still an organization of personal data that complies with the provisions in the law and encourages all parties to protect the privacy of personal data so that law enforcement can effectively deal with the problem of the use of personal data, so that the importance of strengthening or improving in terms of substance, strengthening aspects of structure, and improving cultural aspects.

By enacting the destruction, prevention and control of criminal acts of misuse of personal data, law enforcement officers must make various efforts, including non-penal and penal efforts. Non-penal efforts are coaching and educational activities to eliminate a factor that occurs in criminal acts, by taking prevention through investigations of places that are considered very suspicious. In contrast to the penal effort, it is an effort to take action, in that action provides a deterrent effect to the perpetrators.

4. Conclusion

Regarding sanctions for perpetrators in abusing someone's personal data through electronic media, the implementation has not been maximized even though the injured party is given the opportunity to file a lawsuit to the Court, because in the provisions of Article 26 (2) of Law Number 11 of 2008. Regarding criminal decisions and compensation in This law has not yet been regulated, so there is a need for reformulation in legal norms by adding criminal sanctions for perpetrators and guarantees for the protection of personal data, so it is hoped that a more precise and comprehensive rule is in accordance with progress in socio-cultural, economic and political so that it can increase the value of ethical, moral and religious norms and expect a rule of law in Indonesia to be more advanced.

There is a link between personal data and a person's right to privacy, which lies in the matter of someone opening or disseminating his personal data to other parties. in accordance with the intentions and freedom of the person, so we need to carefully analyze whether a case that occurs can be categorized as a cyber crime or not, which has an impact on the number of public reports that go to the police. By enacting eradication, prevention and overcoming criminal acts of data misuse, law enforcement officers carry out various efforts including non-penal efforts (guidance in educational efforts) and penal efforts (actions to create a deterrent effect).

Acknowledgement

We thanks to Universitas Muhammadiyah Sidoarjo for supported this research.

References

[1] Pembobolan rekening lewat setruk ATM disebut pakai data pemilih milik KPU.

[2] Peraturan menteri komunikasi dan informatika nomer 20 tahun 2016 tentang perlindungan data pribadi dalam sistem elektronik.

[3] Widiyaningsih F. Mahasiswa jurusan siyasah jinayah UIN dengan skripsi yang berjudul. Tindak pidana pengaksesan sistem elektronik dalam UU no.11 tahun 2008 tentang informasi dan transaksi elektronik (dalam prespektif Figh Jinayah).

[4] Devianti DN, Djatmika P, Sukarm. Implementasi yuridis penggunaan data pribadi orang lain untuk kepentingan pengguna jasa layanan pinjam meminjam berbasis fintech menurut ketentuan perundang-undangan di Indonesia.

[5] Rancangan undang-undang perlindungan data pribadi.

[6] Widodo. Memerangi cyber crime (Karakteristik, motivasi, dan strategis penanganannya dalam prespektif kriminilogi). Yogjakarta: Aswaja Presindo; 2013.

[7] Available from: http://download.garuda.ristekdikti.go.id/article.php?article=971996&val=14963&title=ANALISA%20KASUS%20CYBERCRIME%20BIDANG%20PERBANKAN%20BERUPA%20MODUS%20PENCURIAN%20DATA%20KARTU%20KREDIT

[8] Amiruddin SH, Hum M, Asikin Z. Pengatar metode penelitian hukum. Jakarta: PT Raja Grafindo Persada; 2016.

[9] Undang-undang nomor 11 tahun 2008 tentang informasi dan teknologi elektronik.