Legal Protection of Personal Data Owners as Cybercrime Victims Based on regulations regarding Electronic Information and Transactions

Mona Minarosa
{mona_minarosa@borobudur.ac.id}

Universitas Borobudur, Jakarta, Indonesia

Abstract. Cybercrime is a crime committed using information and communication technology in computers and other devices connected using the internet network. The internet has become one of the obligations in life today. Technological developments have influenced the change in crime from what was previously a crime in the real world to a virtual crime or in cyberspace, but the impact felt by victims is accurate, such as the theft of money, personal data, or other important information. Internet connects every user. However, the negative impact cannot be avoided. Cause the creation of a new type of crime known as cybercrime, or crime committed via the use of the internet network. Because technological advancements in the internet world have progressed at such a rapid pace that people can access one's data without the other party's knowledge, the issue of protecting one's personal rights (privacy rights) is closely related to the protection of one's data (personal data) in the cyber world. They were concerned that there was a significant risk of infringing a person's rights.

Keywords: Internet; Cybercrime; Personal Data

1 Introduction

The use of information technology and the internet has changed the culture of the Indonesian people in their daily life in accessing information, entertainment, and as a tool for communicating and interacting between people. The rapid development of information technology and the internet certainly has a positive impact on society because it helps help improve the welfare of the community and even the economy of a country, making it easier for people to access information, get entertainment, and communicate without any distance restrictions. Computer network technology is becoming increasingly important. Apart from being a means of disseminating information over the internet, the business community's operations are also the most important and fastest-growing segment, crossing national lines. Despite this network, all types of information may be obtained for a period of 24 hours.

However, information technology and the internet also have a negative and dangerous impact on the security of personal data because all equipment connected to the internet can be stolen and used by irresponsible people called hackers. The crimes committed against personal

MIC 2021, October 30, Padang, Indonesia

DOI 10.4108/eai.30-10-2021.2315833

data protection are called hacking, namely accessing computer equipment by other people without permission by utilizing internet technology for personal gain or doing damage, by using the use of dangerous computer applications, such as viruses, malware, and spyware, and so on—ransom ware. Cybercrime is a crime committed using information and communication technology in computers and other devices connected using the internet network. Technological developments have influenced the change in crime from what was previously a crime in the real world to a virtual crime or in cyberspace, but the impact felt by victims is natural, such as the theft of money, personal data, or other important information.

Private details refers to facts, interactions, or views about specific persons that are extremely personal or sensitive. The individual concerned want to prevent or limit others from gathering, utilizing, or disseminating it to others. In contrast, as the number of users and the internet grew, so did the need of personal data security. Many recent examples, particularly those involving the leaking of personal data and criminal actions of fraud or obscenity, have reaffirmed the significance of enacting legislative measures to protect personal information.

Law Number 11 of 2008, as amended by Law Number 19 of 2016, regulating Digital Data and Information, is now the legal basis for cybercrime charges. Another crime against the security of personal data is manipulation (phishing), which is a crime committed by someone by sending an email and using a fake domain to trick the email recipient so that the perpetrator gets the necessary information or installs computer applications without the knowledge of the email recipient where the crime is intended to steal data owned by email recipients.

Another crime that is also dangerous for the security of personal data is social engineering attacks to manipulate someone via telephone or email or other communication media to provide personal data information, both information about banking security data or user passwords. This is quite dangerous because criminals often pretend to be employees of a bank, agency or company, so victims easily trust and provide the necessary information. Then criminals can freely take advantage of the crime. Indonesia as a state of the law is, of course, obliged to protect every citizen from any actions that can harm, primarily those actions that can damage the order of life of the nation and state

As well as crimes that occur in cyberspace or often called cybercrime. The crime that does not know space and time has experienced rapid development in recent times. Technological sophistication is being misused by irresponsible persons for personal gain, making it difficult for developing countries to take action against criminals, especially the police, because it requires a set of rules governing the misuse of this technology and adequate human resources facilities and infrastructure support [1].

In light of these circumstances, it is vital to adopt regulations that expressly govern cybercrime and provide legal protection against the use of information technology and the internet. To address these issues, the government passed Law No. 11 of 2008 Concerning Information and Electronic Transactions on April 21, 2008, which was later revised by Law No. 19 of 2016 Concerning Amendments to Law Number 11 of 2008 Concerning Information and Electronic Transactions. Transactions on the Internet (UU ITE). This legislation is broken into two sections: one that regulates electronic transactions and another that regulates forbidden conduct (cybercrime). In addition, as the number of users and the internet grew, so did the need of personal data security. Some recent examples, particularly those involving the leaking of personal data and criminal actions of fraud or pornography, have reaffirmed the significance of enacting legislative safeguards to protect personal data.

The idea of privacy is linked to the protection of personal data. The concept of privacy refers to the preservation of one's personal integrity and dignity. Individuals' right to privacy also includes the capacity to control who has information about them and how that

information is used [2]. The right to privacy, as well as the protection of personal data, is essential for human liberty and dignity. Personal data protection is a driving factor for achieving political, spiritual, religious, and even sexual liberation. The right to self-determination, freedom of expression, and privacy are all necessary for our development as human beings. Personal data collection and distribution infringe on a person's right to privacy since the right to privacy involves the ability to choose whether or not to supply personal data.

However, personal data protection is currently not regulated in a separate law. However, it is still spread in various rules and regulations. For example, Law Number 36 of 2009 concerning Health governs the confidentiality of the patient's condition, and Law Number 10 of 1998 concerning Banking regulates depositing customers' data and deposits. Legal provisions related to the protection of personal data, which are still partial and sectoral, do not seem to provide optimal and effective protection for the security of personal data as part of privacy.

a. What is the legal protection for personal data owners as victims of cybercrime based on Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions?
b. What preventive measures can the owner of personal data be taken so as not to become a victim of cybercrime?

2 Methodology

a. The approach method used in this research is normative juridical because this research is based on favourable law legislation and aims to acquire knowledge according to applicable rules.
b. Data Collection Techniques. This study relied on secondary data gathered through a literature review. The Indonesian Criminal Code (KUHP) and Law Number 11 of 2008 concerning Information and Electronic Transactions, as revised by Law Number 19 of 2016, are the primary legal sources that are binding and directly relevant to the object of investigation in this case (UU ITE).
c. Secondary legal materials provide explanations for primary legal materials, such as literature, research results, and scientific works.
d. Tertiary legal materials, namely legal materials that provide explanations and also instruction for primary legal materials and secondary legal materials, such as dictionaries [3].

3 Theoretical Review

3.1 Definition of Cybercrime

Cybercrime is committed using information and communication technology in computers and other devices connected using the internet network. Technological developments have influenced the change in crime from what was previously a crime in the real world to a virtual crime or in cyberspace, but the impact felt by victims is accurate, such as the theft of money, personal data, or other important information [4]. The internet, as an information technology system, has impacted law professionals' perspectives on the meaning of computer crime. The scope of cybercrime has widened as a result of the advancement of information technology in

the form of an internet network. As a result, cybercrime is described as a type of computer crime that may be further subdivided into information technology crimes, which encompass any crimes involving information systems and communication networks that are used to deliver/exchange data with third parties. Cyberspace is known as a new reality in human life, which is often called the internet. This new reality is formed through a computer network that connects countries or continents based on the transmission control protocol/internet protocol. That way, it can be said that cyber space (internet) has changed distance and time to be unlimited in its working system.

3.2 Types of Cybercrime

Cybercrime can be interpreted as a type of crime committed via the internet. With the development of technology, various kinds of crimes can be carried out because multiple factors cause them. In general, there are several types of crimes that can be committed related to the use of information technology, and the following are several types of cybercrime based on their activities, namely:

a) Unauthorized access to Computer System and Service
   Crimes are committed into a computer network system illegally, without permission, or without the knowledge of the owner of the computer network that is entered. Usually, criminals enter it to sabotage or steal essential and confidential data or information. However, some do so only because they feel challenged to try their skills to penetrate a high level of protection or security system.
b) Illegal Contents
   It is a crime to enter data or information that is not true, inappropriate, unethical, and considered unlawful or disturbing public order into the internet.
c) Data Forgery
   This type of crime aims to falsify data on essential documents on the computer / on the internet. These documents are usually owned by institutions or institutions with web-based database sites.
d) Cyber Espionage
   By breaking into the target party's computer system network, criminals exploit the internet network to spy on them. This crime is frequently committed against business competitors who have important papers or data saved on a computer system.
e) Cyber Sabotage and Extortion
   Data, computer programs, or a computer network system connected to the internet are disrupted or destroyed in this crime.
f) Offence against Intellectual Property
   This offense is committed against other people's intellectual property rights over the internet. For example, illegally imitating the appearance of another person's website on a web page, broadcasting information on the internet that is a trade secret of another party, and so forth.
g) Infringements of Privacy
   A crime committed against someone's private and personal information. Personal data saved in a computerized unique data form is frequently the target of this crime. Credit card numbers, ATM PINs, and knowledge regarding concealed records, for example, might injure a person materially or immaterially if it is known by others [5].

3.3 Personal Data

Private details refers to facts, interactions, or views about specific persons that are extremely personal or sensitive. The individual concerned want to prevent or limit others from gathering, utilizing, or disseminating it to others. According to Jerry Kang, personal data describes the information closely related to a person that will distinguish the characteristics of each individual [6]. The method for data security is divided into two classifications: safeguarding physical data, both visible and invisible data; and the existence of legislation limiting the use of data by unauthorized individuals, abuse of data for specific goals, and data deletion. In the development of secrecy, a fundamental notion has been recognized in a number of nations, both the sort of regulation and guidelines [7]. In the Netherlands, for example, it is referred to as decencies, which meaning personal rights. It is known as personlichkeitsrecht in Germany, which denotes personal ownership as a representation of one's individuality, and geheimssphare in Switzerland, it implies privacy rights.

Warren and Brandeis were the first to establish the notion of privacy, writing a paper titled "The Right to Privacy" in the Harvard University Law School scientific magazine. According to Warren Brandeis in the publication, with the growth and expansion of technology, there has been a general understanding that a person's right to enjoy life has been born. The right to enjoy life is described as a person's right to be free from interference in his or her personal life, whether by other individuals or the government [7].

Data is any information saved to be processed by technology that operates automatically in response to instructions supplied for its purpose. Information that is a specific aspect of health, social work, or education records, or stored as part of a suitable storage system, is classified as data. Data is described as an ordered set of symbols that represent quantities, activities, objects, and other things. Characters such as alphabets, integers, and special symbols are used to create data. [8] Personal data that is directly tied to electronic data is the focus of this paper's topic. The private grounds must be preserved, namely: first, in order to retain a particular degree of status, a person must mask part of his personal life while forming interactions with others. Second, someone in his life need isolation (alone time), which necessitates privacy. Third, while privacy is a right that exists independently of other rights, it will be lost if a person reveals private information to the public.

Fourth, privacy involves a citizen's right to just have internal ties, such as how a person develops a marriage and raises a family, and other people must not be aware of this intimate relationship, which Warren dubbed the right against the word. Fifth, because the damage sustained is difficult to quantify, privacy warrants legal protection. Because it has interfered with his personal life, the failure is far worse than the physical loss. If a loss occurs, the sufferer must be compensated. Samson Garfinkel makes classified that private information into 5 (five) categories, namely:

a. Personal data, information related to a person, including name, date of birth, school, and terms of parents
b. Private information, information relating to a person but not generally known, is protected by law. Examples: academic transcripts and banking records;
c. Personally, Identifiable Information is information derived from someone in the form of habits, favourite things, and others.;
d. Anonym zed Information is information relating to someone who has been modified so that the information is not the actual information.
e. Aggregate information, statistical information, is a combination of several individual details [9].

4 Results and Discussion

4.1 Personal Data Security

Because computers have begun to record population data, notably for population censuses, the phrase data protection was first used in Germany and Sweden in the 1970s, which governs personal data protection through laws and regulations [7]. In its execution, both the government and private firms have committed many infractions. As a result, legal measures are required to ensure that personal data is not exploited. The existence of rules limiting the use of data by unauthorized parties, abuse of data for specific goals, and data deletion are examples of data protection.

4.2 Personal Data Regulations

Legislation that regulates explicitly personal data protection currently does not exist in Indonesia. However, the protection aspect has been stated in several other laws and regulations there are:

a) Law Number 8 of 1997 concerning Corporate Manuscript
   According to article 1, corporate documents are defined as data, records and information made or received by the company in the context of carrying out its activities, either written on paper or other means or recorded in any form that can be seen, read or heard.
b) Law Number 43 of 2009 concerning Records
   The Records Law is a law that regulates the administration of archives within the government and the administration of the archive system by state institutions, local governments, educational institutions, companies, political organizations, community organizations, and individuals and recorded institutions. Regarding protecting personal data, the Record Law states that archival institutions and archive creators can close access to archives if necessary. For example, if the library is opened to the public, one can reveal someone's confidential or personal data. This law also regulates data security and includes criminal threats against anyone who knowingly provides a dynamic record to unauthorized record users.
c) Law Number 11 of 2008 as amended by Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE).
   Personal data protection is included in the Law on Information and Electronic Transactions as an element of private rights. Companies that provide items through electronic systems must give comprehensive and accurate information, such as contract conditions, producers, and products supplied, according to Article 9.

4.3 In the Legal Protection of Cybercrime Victims

In the legal protection of cybercrime victims, there are 2 (two) models, namely [10]:

a) The procedural rights model
   Cybercrime victims are guaranteed the right to bring criminal charges, assist prosecutors, or be presented at any level of justice if information is necessary under the procedural rights paradigm. Victims can implicitly react against criminals who have injured them in this concept. Victims are also being requested to play a more active role in supporting law enforcement agents in the investigation of cases, particularly those involving contemporary cybercrime.

b) The Service Model

This model emphasizes the need of establishing uniform standards for the treatment of cybercrime victims. The victim is seen as someone who needs to be serviced by the police and other law enforcement authorities under this concept. If done correctly, law enforcement officials' services to victims of cybercrime will have a good influence on law enforcement, particularly cybercrime. As a result, victims of this technical advancement will have more faith in law enforcement agencies. Victims' rights will be respected, and their interests will be protected, thanks to victim services. In Indonesia, cybercrime regulations can be interpreted in two ways: broadly and narrowly. Cybercrime refers to any illegal activity carried out using or aided by electronic technologies. This indicates that any traditional criminal activities in the Indonesian Civil Code, such as terrorism and human trafficking, can be classified as cybercrime in a wide sense, as well as financial crimes and money laundering, as long as they employ help or facilities.

The ITE Law, on the other hand, regulates cybercrime in a limited manner. Several criminal offenses that come under the category of cybercrime are categorized under that statute. Specifically, the ITE Law groups various criminal offenses that come under the heading of cybercrime.

4.3.1 Crimes Related to Illegal Activities

Distribution or dissemination, transmission, accessibility of illegal content consisting of [4]

a. Morality (Article 27 paragraph (1) UU ITE)
   Everyone distributes, transmits, and makes access to electronic information and electronic documents that include decency-infringing content knowingly and without rights.
b. Gambling (Article 27 paragraph (2) of the ITE Law)
   "Every person intentionally and without rights distributes and transmits and makes accessible Electronic Information and Electronic Documents containing gambling content.
c. Insults and defamation (Article 27 paragraph (3) UU ITE)
   "Every person intentionally and without rights distributes and transmits and makes accessible Electronic Information and Electronic Documents that have insulting and defamatory content
d. Extortion or threats (Article 27 paragraph (4) UU ITE)
   Every person intentionally and without rights distribute and transmits and makes accessible Electronic Information and Electronic Documents containing extortion and threats."
e. Fake news that misleads and harms consumers (Article 28 paragraph (1) of the ITE Law) Everyone, with or without rights, purposefully disseminates inaccurate and misleading information, resulting in consumer losses in online transactions.
f. It generates hatred based on ethnicity, religion, race, inter-group (Article 28 paragraph (2) of the ITE Law. Everyone, with or without rights, distributes material meant to incite hatred or enmity toward certain persons and civic groups based upon race, religion, race, or intergroup relations.
g. Sending information containing threats of violence or intimidation aimed at personally. Every individual provides Electronic Information and Electronic Documents that contain threats of violence or intimidation targeted at them purposefully and without their consent.

4.3.2 In any way, by doing illegal access (Article 30 UU ITE)

a. Every person intentionally and without rights or against the law accesses a computer and electronic systems belonging to other persons in any way.
b. Any person intentionally and without rights or against the law accesses a Computer and Electronic System in any way by violating, breaking through, exceeding, or breaking into the security system.

4.4 Prevention Efforts That Personal Data Owners Can do So as Not to Be a Victim of Cybercrime

There are several ways that the owner of personal data, both private and corporate, can protect the security of personal data and avoid becoming a victim of cybercrime. This prevention can be done using technology to help detect and prevent cybercrimes and socialize individual data owners, both by the government and financial service providers to increase security awareness of the importance of personal data security and avoid these crimes and legal sanctions against criminals.

Keeping every device (PC, laptop, and other gadgets belonging to the victim) up to date is one of the easiest and most efficient ways to prevent hackers and other cybercriminals from hacking and stealing critical information from victims. Vendors of victim's computers and gadgets will offer updates for these devices on a regular basis. These updates are frequently meant to plug security vulnerabilities that may exist on these devices, and they should be followed in order to prevent sensitive data theft. Updates to the web browser, operating system, and other plugins should also be installed with the latest version.

Installing antivirus application forms to protect, identify, and remove spyware such as computer viruses, trojan horses, malware, key loggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraud-tools, adware, and spyware is also a great way to prevent computer devices from cybercrime. It is critical for a business owner to invest in antivirus software for all corporate computers. Antivirus applications are mandatory, especially for computers that store sensitive customer information and must be updated regularly following the recommendations of the antivirus application.

5 Conclusion

In providing legal protection to owners of personal data as victims of cybercrime, the government has issued Law Number 11 of 2008 as amended by Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE), which regulates cybercrimes and criminal sanctions.

a. Cybercrimes consist of crimes related to illegal activities (Articles 27 to 31), crimes related to harassment (Article 32 and Article 33), crimes of facilitating prohibited acts (Article 34), criminal acts of falsifying information or electronic documents (Article 35), and additional criminal acts (Article 36). For the perpetrators of this cybercrime, the ITE Law provides criminal sanctions as regulated in Article 45 to Article 52, namely maximum imprisonment of 12 (twelve) years and a maximum fine of Rp. 12,000,000,000.00 (twelve billion rupiahs).

b. Prevention efforts taken by owners of personal data so as not to become victims of cybercrime include keeping every computer (PC, laptop, and other gadgets) up-to-date. Malware such as computer viruses, hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraud-tools, adware, and spyware may all be prevented, detected, and removed with antivirus software. Furthermore, the owner of personal data must always get the most up-to-date knowledge about cybercrime and its attack strategies through forums, conferences, and journals, so that preventative actions may be performed based on the information obtained.

References

[1] Andika, Tri. *Sovereignty in the Information Sector in the Digital Age: An Overview of Theory and International Law.* Journal of Bina Mulia Hukum, Volume 1, Number 1, (2016)

[2] Djafar, Wahyudi., and Asep Komarudin. *Protection of the Right to Privacy on the Internet: Some Key Explanations*. Elsam, Jakarta (2014).

[3] Soekanto, Soerjono. *Introduction to Legal Research*. University of Indonesia UI-Press, Jakarta, p. 12 (2015)

[4] Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments Electronic Information and Transactions.

[5] Mansur, Dikdik M. Arief, dan Elisatris Gultom. *Cyber Law Aspek Hukum Teknologi Informasi.* PT. Grafika Aditama, Bandung, pp. 89 (2005)

[6] Kang, Jerry. *Information Privacy in Cyberspace Transactions*. Stanford Law Review Vol 50, p. 5, (April 1999)

[7] Dewi, Shinta. *Privacy Protection for Personal Information in E-Commerce According to International Law.* Widya Padjajaran, Bandung (2009).

[8] Purwanto. *Research on Legal Protection of Digital Data.* National Legal Development Agency, Jakarta (2007)

[9] Garfinkel, Simson. *PGP: Pretty Good Privacy*. O'Reilly & Associates, Inc., pp. 12 (1995)

[10] Maskun. *Kejahatan Siber (Cyber Crime).* Prenada Media Grup, Jakarta (2013)