Legal Protection as a Form of State Responsibility for Victims of Cyber Crime in Indonesia

Mujiono Hafidh Prasetyo[1]
{mujionohafidhprasety@lecturer.undip.ac.id[1]}

Faculty of Law, University of Diponegoro, Semarang, Indonesia[1]

Abstract. The development of information technology does not always have a positive impact, but it can also have a negative impact on people who judge a crime known as cybercrime. It is a legal obligation for the state government to protect every citizen from actions that can harm the rights of its citizens, one of the cyber crimes in order to provide a sense of security for those who use information technology in their activities in cyberspace. The purpose of this article is to look at forms of cybercrime crime, analyze cybercrime crime victims and forms of legal protection by the State against victims of cybercrime crime. This research uses doctrinal legal research. Sources of legal information use primary legal materials (regulations and relevant documents) for further qualitative analysis. What is used are statutory, conceptual, analytical approaches and comparisons in helping to deal with problem formulations. The results of the study stated that victims of telematics crimes were the trigger for crimes due to their negligence. In positive law, legal protection for victims of cybercrime crimes is the same as legal protection for victims of conventional crimes, namely protection in the form of compensation, restitution and compensation.

Keywords: legal protection, victims, cybercrime

1 Introduction

Technological developments from time to time will be more sophisticated and continue to develop every year. The use of information technology, media, and communication has changed the behavior of society and human civilization globally. The development of this technology is used by humans to meet their needs such as the use of gadgets for long-distance communication and as entertainment. The internet is useful for knowing outside information and various knowledge and so on. Information and Communication Technology as part of science and technology in general are all technologies related to information retrieval, collection, processing, storage, dissemination and presentation [1].

ICETLAWBE 2020, September 26, Bandar Lampung, Indonesia

DOI 10.4108/eai.26-9-2020.2302588

Entering the 21st century, there are many changes, especially in the fields of technology and information. Almost everyone in the world uses technology, not apart from the state of Indonesia. With technology that is growing rapidly, of course there are also many gaps in crimes that are often committed. Moreover, these crimes are not visible to the naked eye which sometimes we are also not aware of. Crimes like this are often of special interest to irresponsible people, especially when law enforcers don't understand technology.[1] So that the protection system is very weak from various kinds of products that enter Indonesia. Especially if the crime in the cyber world is in the form of a corporation, it will be more dangerous and it is very difficult to prove it. Currently, a new legal regime has been born, known as cyber law or telematics law. Cyber law, or cyber law, is internationally used for legal terms related to the use of information and communication technology. Likewise, telematics law is the embodiment of the convergence of telecommunications law, media law and informatics law. Other terms that are also used are law of information technology and virtual world law.

Based on data from the Cyber Police until August 2020 the number of police reports made by the public with a total of 20,033 reports details of the reports are as follows: 8,541 Online Fraud, 7,460 Spread of Provocative Content, 1,308 Pornography, 1,056 Illegal Access, 168 gambling. 244 Extortion, 386 Data / Identity Theft, 244 Electronic System Hacking, 64 Illegal Interception, 92 Change of Status Display, 139 System Interference, and 331 Data Manipulation [2].

Looking at the data above, a specific set of rules is needed to regulate cyber crime and legal protection for the use of information, media and communication technology in order to develop optimally. In order to overcome the various problems above, the government on April 21, 2008 has enacted Law Number 11 of 2008 concerning Information and Electronic Transactions (IET Law). In general, Law Number 11 of 2008 concerning Information and Electronic Transactions (IET Law) can be divided into two major parts, namely regulating electronic transactions and regulating prohibited acts (cybercrimes).

The state considers it necessary to support the development of information technology through legal infrastructure and its regulation so that the use of information technology is carried out widely to prevent its misuse by taking into account the religious and socio-cultural values of the Indonesian people.[3] As a rule of law, it is the state's obligation to protect every citizen from any actions that can damage or harm society. One of them is the legal protection provided by the state for technology users. Legal protection for victims of abuse of digital technology is of course very necessary, this is because when a criminal event occurs, the rule of law often focuses on punishing the perpetrators of crime, while victims are often ignored. The victim also deserves attention because basically the victim is the party who is sufficiently harmed in a criminal act. The impact of crime causes casualties and losses. The losses incurred can be suffered by the victim himself or by other parties indirectly. The nature of the crime should be seen as something that is detrimental to the victim, therefore the punishment imposed on the offender must also take into account the interests of the victim in the form of restoration of the losses suffered [4]. The losses that must be recovered are not only physical losses but also non-physical losses.

Efforts to protect victims are actually very important. Because in addition to reducing the suffering of the victim for the crime they have experienced, it can also prevent the occurrence of continued victims, so that this can reduce the crime rate. For this reason, the author wants to see further how legal protection for victims is the responsibility of the State for victims of cybercrime in Indonesia.

2. Methods

This research uses doctrinal legal research. Sources of legal information use primary legal materials (regulations and relevant documents) for further qualitative analysis. The approach used is statutory, conceptual and analysis in helping solve the problem formulation. The data source of this research consists of primary legal materials, secondary legal materials to be continued by analyzing as a whole, the laws and regulations, literature, data, and several related documents, as well as tertiary legal materials to explain and assist in analyzing primary legal materials. or secondary [5]

3. Result and Discussion

3.1 Forms of Cybercrime Crime

As a rule of law it is an obligation of the state to protect every citizen from any actions that can damage or harm society, one of which is the legal protection provided by the state to people who use technology, law and technology are two different words but affect each other and also can affect the life of the community itself. The regulation of cybercrime in Indonesia can be seen in two senses, namely in a broad sense and in a narrow sense. Broadly speaking, cyber criminal acts are all criminal acts using means or with the help of electronic systems, this means that all conventional criminal acts in the Criminal Code (KUHP) as long as using assistance or means such as terrorism, human trafficking, can include in the category of cyber crime in a broad sense the same is true of banking and money laundering crimes. However, in a narrow sense, the regulation of cyber crime is regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions (IET Law).

Crimes that are closely related to the use of computer-based technology and telecommunications networks in some literature and practice are grouped into several forms, including:[6]

a. Unautherized acces to computer system and service, namely crimes committed into a computer network system illegally, without permission or without the knowledge of the owner of the computer network system that is entered. Usually the criminals (hakcer) do so with the intention of sabotage by stealing important and confidential information. However, there are also those who do it just because they feel challenged to try their skills to penetrate a system that has a high level of protection. This crime is increasingly prevalent with the development of internet technology.
b. Illegal Contens, namely crimes by entering data or information on the internet about something that is untrue, unethical, and can be considered to violate the law or disrupt public order. For example, the loading of fake news or slander that will destroy the dignity or self-respect of other parties, things related to pornography or the loading of information that is state secret, agitation and propaganda against the legitimate government and so on.
c. Data Forgery, namely crimes by falsifying data on important documents stored as scripless documents via the internet. This crime is usually aimed at e-commerce documents by making as if a “typo” occurred which in turn will benefit the perpetrator because the victim will enter personal data and credit card numbers which can be misused.

d. Cyber Espionage, which is a crime that utilizes the internet network to spy on other parties by entering the target party's computer network system. These crimes are usually directed against business rivals whose important documents or data (data base) are stored in a system connected to a computer network.
e. Cyber Sabotage and Extortion, which is a crime committed by disturbing, destroying or destroying data, computer programs or computer network systems connected to the internet. Usually this crime is committed by inserting a logicbomb, computer virus or a certain program, so that data, computer programs or computer network systems cannot be used, do not run properly, or run as the perpetrator wants.
f. Offense Against Intellectual Property, namely crimes aimed against intellectual property rights owned by other parties on the internet. For example, illegally imitating the appearance of someone else's website, broadcasting information on the internet turns out to be someone else's trade secret, and so on.
g. Infringements of Privacy, namely crimes that are usually directed against a person's personal information stored on a Computerized form of personal data, which, if known by other people, can harm the victim materially or materially, such as credit card numbers, ATM PIN numbers, disabilities or hidden disease and so on.[6]

In the IET Law several criminal acts that fall into the cybercrime category are classified, namely:[7]

a. Criminal acts related to illegal activities, namely:
    1. Distribution or dissemination, transmission, accessibility of illegal content, which consists of:
        a) Decency (Article 27 paragraph (1) of the IET Law); "Anyone who knowingly and without rights distributes and/or transmits and/or makes accessible to Electronic Information and/or Electronic Documents that have content that violates decency".
        b) Gambling (Article 27 paragraph (2) of the IET Law); "Anyone knowingly and without right distributes and/or transmits and/or makes electronic information and/or electronic documents that have gambling content accessible".
        c) Insult and defamation (Article 27 paragraph (3) of the IET Law); "Anyone knowingly and without right distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents that have content of defamation and/or defamation".
        d) Extortion or threats (Article 27 paragraph (4) of the IET Law);
        "Anyone knowingly and without right distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents that have contents of extortion and/or threats"
        e) Fake news that is misleading and detrimental to consumers (Article 28 paragraph (1) of the IET Law); "Everyone knowingly and without right spreads false and misleading news that results in consumer losses in electronic transactions"
        f) Generating a sense of hatred based on ethnicity, religion, race and inter-group (Article 28 paragraph (2) of the IET Law); "Anyone who knowingly and without rights disseminates information aimed at creating hatred or enmity for individuals and/or certain groups of people based on ethnicity, religion, race and inter-group"

g) Sending information that contains threats of violence or fright that is aimed personally (Article 29 of the IET Law); "Every person knowingly and without authority sends Electronic Information and/or Electronic Documents that contain threats of violence or scare aimed personally"

2. In any way by doing illegal access (Article 30 of the IET Law):
   a) Everyone who knowingly and without rights and unlawfully accesses computers and/or Electronic Systems belonging to other people in any way.
   b) Anyone who knowingly and without right or unlawfully accesses computers and/or electronic systems in any way for the purpose of obtaining Electronic Information and/or Electronic Documents.
   c) Everyone who knowingly and without or against the law accesses computers and/or electronic systems in any way by violating, by passing, by passing, or breaking into security systems.
3. Illegal interception of information or electronic documents and electronic systems (Article 31 of the IET Law)
   "Anyone who knowingly and without right or against the law intercepts or wiretaps Electronic Information and/or Electronic Documents in certain computers and/or Electronic Systems belonging to other people."
4. Criminal acts related to interference (interference)
   a) Interference with Electronic Information or Documents (data interference to Article 32 of the IET Law) "Everyone knowingly and without rights or against the law in any way changes, adds, reduces, transmits, destroys, removes, removes, hides an Electronic information. And/or Electronic Documents belonging to other people or the public."
   b) Interference with Electronic Systems (system interference Article 33 of the IET Law) "Every person intentionally and without rights or against the law takes any action that results in disruption of the Electronic System and/or causes the Electronic System to not work properly"
5. Criminal acts facilitate prohibited acts (Article 34 of the IET Law)
   a) Anyone who knowingly and without right or unlawfully produces, sells, copies for use, imports, distributes, supplies, or owns:
      1) Computer hardware or software that is designed or specifically developed to facilitate the actions referred to in Article 27 to Article 33;
      2) Computer passwords, Access Codes or similar things that are intended to make Electronic Systems accessible for the purpose of facilitating acts as referred to in Article 27 to Article 33.
6. Criminal act of falsification of information or electronic documents (Article 35 of the IET Law) "Every person intentionally and without rights or against the law manipulates, creates, changes, removes, destroys Electronic Information and/or Electronic Documents with the aim of making Electronic Information and/or The Electronic Document is considered as if the data is authentic".[7]

3.2 Overview of Cybercrime Crime Victims

3.2.1 Definition of Victims of Crime

Perpetrator and victim are like two sides of a coin. Generally, people cannot think of a crime without its victims. Although there are also victimless crimes, in the sense that the perpetrator is also the victim. The existence of victims in almost every crime is also evident from the formulation of laws against acts that are declared as crimes [8].

The victims of a crime are not always individuals or individuals, but can also be groups of people, communities, or legal entities. Even in certain crimes, the victims can also come from other life forms such as plants, animals, or ecosystems. Various definitions of victims have been put forward both by experts and originating from international conventions that discuss crime victims.[9] According to Muladi, victims are people who have either individually or collectively suffered losses, including physical or mental, emotional, economic losses, substantial disturbances to fundamental rights, through actions or omissions that violate criminal law in each country, including abuse of power [9].

Meanwhile, according to Arif Gosita, victims are those who suffer both physically and spiritually as a result of the actions of other people seeking the fulfillment of their own or other people's interests that are contrary to harmful human rights interests.[1] A crime victim is defined as someone who has suffered losses as a result of a crime and or whose sense of justice has been directly impaired as a result of his experience as a target (target) of crime [10].

3.2.2 The Causes of Victims of Cybercrime Crime

As for the reasons for the misuse of the convenience of digital technology, among others:[11]

1) Unlimited internet access, now the internet is not rare anymore, because everyone has taken advantage of internet facilities. By using the internet we are given the convenience of easy access to everything without any restrictions. With that comfort, it is the main factor for some people to easily commit cybercrime crimes.
2) Computer user negligence. This is one of the main causes of computer crime. As we know, people using internet facilities always enter all important data into the internet. So that it makes it easy for some people to commit crimes.
3) Easy to do for little safety reasons and no super modern equipment is required. This is the driving factor for crime in cyberspace. Because like us, the internet is a tool that we can easily use without requiring special tools to use it. However, the main driver of crime on the internet is the difficulty of tracking down people who abuse the facilities of the internet.
4) The perpetrators are generally intelligent people, have great curiosity and are fanatical about computer technology. Computer criminals' knowledge of how a computer works is far above that of computer operators.
5) Weak network security system. As we know that people in using internet facilities are mostly concerned with their design by underestimating the level of security. So that the weak network security system becomes a gap for most people to commit crimes.
6) Lack of public attention and law enforcement. In fact, computer criminals still continue to commit crimes. This is due to the low level of knowledge about the use of the internet which is deeper in the community.

3.3 Legal Protection by the State Against Cybercrime Crime Victims

Conceptually, victim protection is an effort to protect a person / legal entity, who has suffered physical, mental, emotional damage, loss of property or destruction of their rights through actions or omissions that have been regulated in the criminal law due to an unlawful act. can be allowed to take place in the midst of society, which rapes the scale of social values and feelings of law that live in society caused by the perpetrators of the crime [12].

Victims in this case are those who have been harmed both materially and non-materially as a result of cybercrime crime. In the legal protection of cybercrime victims, there are basically two models, namely the procedural rights model and the service model:[11]

a. The Procedural Rights Model

   In the procedural rights model, victims of cybercrime crimes are given the right to make criminal charges or assist prosecutors, or the right to be presented at every level of justice where information is needed, implicitly in this model victims are given the opportunity to "retaliate" the perpetrators of crimes who have harmed them. In this procedural model, victims are also asked to be more active in assisting law enforcement officials in handling their cases, especially those related to modern crimes of cybercrime. The existence of procedural rights can also revive the confidence of the victim after he has been harmed by those who are not responsible (the defendant), besides that this can also be a consideration for the prosecutor in the event that the prosecutor makes the charges too light.

b. The Service Model

   This service model focuses on the need to create standard standards for coaching victims of cybercrime crime. This model sees the victim as a figure that must be served by the Police and other law enforcement officials, services for cybercrime victims by law enforcement officials if done properly will have a positive impact on law enforcement, especially cybercrime, thus victims of this technological development will have more trust in the institution. law enforcers by providing services to victims, thus victims will feel their rights are protected and their interests are guaranteed. In the trial process, especially with regard to proving cybercrime, many cases that occur as a result of the development of information technology require law enforcement officers to prepare human resources who are reliable and understand and understand technology, given that cybercrime crime is a modern crime that must be received serious attention from the government, because crimes in cyberspace will have an impact on the real world. With the existence of the IET Law, it is hoped that it can help law enforcement officials in protecting people who use technology.

A person who has been a victim of Information Technology crime in the IET Law has been guaranteed by the state, where the state guarantees security and protects all citizens who are active in the world of technology. In the IET Law in Article 27 it explains, namely: (1) everyone knowingly and without right distributes and/or transmits and/or makes electronic information and/or electronic documents that have contents violating decency accessible. (2) Any person who knowingly and without rights distributes and/or transmits and/or makes electronic information and/or electronic documents that contain gambling content accessible. (3) Any person who knowingly and without rights distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents that contain defamatory and/or defamation. (4) Any person who knowingly and without rights distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents that have the contents of extortion and/or threats [13].

In this regard, the law must be able to provide protection to consumers who have good intentions. In this case, the protection provided to consumers is those who buy and sell in the real world.[8] That way the protection for victims of electronic crimes contained in article 28 paragraphs 1 of the IET Law is:

a. Compensation

   The purpose of compensation is none other than to develop justice and the welfare of victims as members of society. And the measure of its implementation is by giving the opportunity to victims to develop their rights and obligations as humans. On that basis, the program for providing compensation to victims should be a combination of efforts from various approaches, both approaches in the field of social welfare, humanitarian approaches and approaches to the criminal justice system.

b. Restitution

   Restitution is more directed at the perpetrator's responsibility for the consequences caused by the crime so that the main target is overcoming all losses suffered by the victim. The benchmarks used in determining the amount of restitution given are not easy to formulate. This depends on the social status of the perpetrator and the victim. In the case of a victim with a lower social status than the perpetrator, it will prioritize material compensation, and vice versa if the victim's status is higher than the perpetrator, then the restoration of dignity and good name will take precedence.

c. Compensation

   Compensation is a form of compensation that can be seen from a humanitarian and human rights perspective. The idea of realizing social welfare in society based on a commitment to social contracts and social solidarity makes society and the State morally responsible and obliged to protect its citizens, especially those who experience disaster as victims of crime. Compensation as a form of compensation that does not depend at all on the proceedings of the judicial process and the decisions that are passed, even the source of funds for this is obtained from the government or public funds [14].

It is determined that the person who provides compensation and restitution is the perpetrator of the crime to the victim who is the victim, provided there is a binding court decision, that the perpetrator of the crime is proven to have committed a mistake as reported.

4. Conclusion

The position of the victim in criminal law is very important in order to make it easier for law enforcement officials to find and find clarity about the criminal act committed by the perpetrator of the crime. Regarding the protection of victims of telematic crimes in Article 28 paragraph 1 of the IET Law the same as the protection of other victims, namely the provision of compensation, restitution and compensation. In the legal protection of cybercrime victims, there are basically two approaches that can be used, namely: 1) a procedural rights model, in which the victim plays a more active role and can assist prosecutors in prosecuting and the right to be present at every level of the judicial process and 2) a model service in this case sees the victim as a person who must be served by the police and other law enforcement officials, thus the victim will feel guaranteed his interests are guaranteed in a fair atmosphere. Providing assistance to victims of cybercrime as well

as in the real world must be carried out at all stages of examination, starting from investigation, trial and post-trial.

References

[1] B. Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: Rajawali Press, 2010.
[2] Patrolisiber, "Polisi Siber, Jumlah laporan Polisi yang Dibuat Masyarakat," *Patrolisiber*.
[3] D. A. ; S. Tanthawi, "Perlindungan Korban Tindak Pidana Cyber Crime Dalam Sistem Hukum Pidana Indonesia," *J. Ilmu Huk. Pasca Sarj. Univ. Syiah Kuala*, vol. 2, no. 1, p. 57, 2014.
[4] S. N. Nur, *Tinjauan Viktimologis Tindak Pidana Penipuan Online Shop Melalui Situs Jejaring Sosial*. Makasar: Universitas Hasanuddin, 2014.
[5] S. ; H. D. ; A. P. Kurniawan, "Urgensi Pencegahan Tindak Pidana Curang (Fraud) dalam Klaim Asuransi," *J. Halu Oleo Law Rev.*, vol. 4, no. 1, p. 65, 2020.
[6] J. Sitompul, *Cyberspace, Cybercrime, Cyberlaw, Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2012.
[7] A. ; M. L. Wahid, *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama, 2005.
[8] S. R. Syahdeini, *Kejahatan dan Tindak Pidana Komputer*. Jakarta: Pustaka Utama Grafiti, 2009.
[9] D. M. A. [et. al. Mansur, *Urgensi Perlindungan Korban Kejahatan*. Jakarta: Raja Grafindo Persada, 2008.
[10] G. Widiartana, *Viktimologi Perspektif Korban Dalam Penanggulangan Kejahatan*. Yogyakarta: Universitas Atma Jaya Yogyakarta, 2009.
[11] A. Dermawan, "Perlindungan Hukum Terhadap Korban Penyalahgunaan Kemudahaan Teknologi Digital," *J. Manaj. Inform. dan Tek. Komput.*, vol. 2, no. 1, p. 123, 2015.
[12] D. Wahyudi, "Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia," *J. Ilmu Huk.*, vol. 2, no. 1, p. 105, 2016.
[13] A. ; A. Dermawan, "Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi," *J. Sci. Soc. Res.*, vol. 2, no. 2, p. 44, 2019.
[14] R. Yulia, *Viktimologi Perlindungan Hukum Terhadap Korban Kejahatan*. Yogyakarta: Graha Ilmu, 2010.