LEGAL PROTECTION AGAINST CRIME VICTIMS CYBER CRIME IN INDONESIA

Susanto[1], Fridayani[2], Andi Irawan[3]
[1]susanto@unpam.ac.id, [2]02918@unpam.ac.id, [3]Andiirawanoke@gmail.com
[1,2,]Lecturer of Law Faculty of Pamulang University, [3]Student of Law Faculty of Pamulang University,

Abstract

The advancement of data innovation nowadays brings a gigantic affect for the social life of the communitythe quick improvement of get to between districts driven to a really contract and without being constrained by space and time As a result of the development of the data innovation isn't continuously a positive affect on human life innovation clients this advancement is additionally went with by the improvement of the wrongdoing is known as cybercrime or cyber wrongdoing. Wrongdoing in the internet happen due to the negative impact of mechanical advancements different modes of violations that happened within the virtual world influence to human life in the genuine worldAs the state government's lawful commitment to secure every citizen of the activities that could harm the rights of its citizensone of which could be a wrongdoing that happens within the virtual world that frequently result in fabric and non-misfortunes for its usersIn tending to these issues the government has ordered Law No. 11 Year 2008 on Data and Electronic Exchanges. With the ITE Law is anticipated to supply lawful assurance for individuals who utilize the innovation and can give a sense of security for those who utilize data innovation in exercises in the internet.

Catchphrases : Assurance Law, Victims, Cybercrime

Abstrak

Kemajuan inovasi data saat ini membawa dampak yang sangat besar bagi kehidupan sosial masyarakat, peningkatan kecepatan akses antar kabupaten didorong menjadi sebuah kontrak yang nyata dan tanpa terkendala oleh ruang dan waktu. Terus memberikan dampak positif pada kehidupan manusia pengguna inovasi, kemajuan ini juga dibarengi dengan semakin membaiknya kejahatan yang dikenal dengan istilah cybercrime atau kejahatan dunia maya. Perbuatan salah dalam internet terjadi akibat dampak negatif dari kemajuan teknologi, berbagai modus pelanggaran yang terjadi di dunia maya, pengaruhnya terhadap kehidupan

manusia di dunia nyata, sebagai komitmen sah pemerintah negara untuk mengamankan setiap warga negara dari aktivitas yang dapat merugikan hak-haknya. warga negara, salah satunya bisa jadi merupakan perbuatan salah yang terjadi di dunia maya yang seringkali menimbulkan dampak buruk dan merugikan bagi penggunanya. Untuk mengatasi hal tersebut pemerintah telah memerintahkan Undang-Undang Nomor 11 Tahun 2008 tentang Pertukaran Data dan Elektronik. Dengan adanya UU ITE diharapkan dapat memberikan jaminan hukum bagi masyarakat yang menggunakan teknologi dan dapat memberikan rasa aman bagi yang menggunakan teknologi data dalam aktivitasnya di internet.

A. Introduction

Today, the development of world information has a great impact on people's lives. These developments have made international relations borderless and have had a profound impact on social change. In addition to providing benefits for the welfare and development of society, the consequences of these technological advances include commercial fraud, fraud, online gambling, identity fraud, child pornography and terrorism, intellectual property theft and other computer threats computer users. network as a tool There are many other evils that can harm and damage the earth and its life. Crimes that occur in cyberspace are due to the negative effects of technological progress. Crimes that occur in all shapes and forms affect the legal protection of users. This is important because everyone deserves to be protected as human beings. One aspect of the government's responsibility to protect its citizens is to provide legal guarantees and concrete measures to protect its citizens from all forms of crime or other abnormal behavior that may affect them both in the real world and in the online world. Indonesia is a country governed by the rule of law in the constitution. Of course, as a constitutional nation, the government has a duty to protect all its citizens from harm. This is especially true if these actions may undermine the integrity of the state and the well-being of the nation. Any crime that occurs in cyberspace is called cybercrime. This crime, which knows no time or place, has grown rapidly in recent years, and with the advancement of technology, irresponsible people are exploiting it for people's profit, because it is difficult for developing countries to respond to cybercriminals, especially the police. . A set of rules governing the misuse of this information requires human resources and supporting facilities and

infrastructure. In the above situation, there should be a special law for the legal protection of the use of information, information technology and information technology to control computer crimes and ensure the efficient development of communication, information and information technology. To avoid the various problems above, the government clarified the Information and Access to Theater Act no. 11 (UU ITE) of April 21, 2008. In general, the ITE Law is divided into two parts: electronic transactions law and cybercrime law. Cyber crime is a serious concern and must be addressed.

We can see that in 2004 the government really took it seriously. Indonesia ranked first in the number of cyber crimes and was considered worse than other countries, including the United States. In 2004 Indonesia ranked first in cybercrime, but the number of cases resolved by the courts was low. In this case, the number of men and women is very high, and most of the information collected by the police is not data based on police investigations, but in the form of sacrifice reports. Polda Metro Jaya also records the total loss to the community due to cybercrime based on police reports received. In Polda Metro Jaya, social losses reached 4 billion rupiah in 2011 and increased to 5 billion rupiah in 2012. This requires serious consideration by all parties as information technology has been used, especially the Internet, as a way to create a communicative community. According to a survey conducted by the Association of Internet Service Providers (APJII) in 2012, the number of Internet users reached 63 million, or 24.23% of the country's population, living Indonesia ranks 8th in the world in number of Internet users. . Due to the large number of users of technology, it is easy to commit crimes, especially on the Internet. Legal protection for people who use technology is essential because when crimes occur, the law focuses on punishing the perpetrators, while the victims of these crimes are ignored. Of course, the victims also need attention, because they are the ones who suffer the most in crimes. The impact of crime can include injury and death. The resulting injuries can affect the victim himself or others. Since the nature of the crime must be considered harmful to the victim, the punishment for the offender must also take into account the interests of the victim. Mode of payment for losses incurred. The diseases that need to be recovered are not only physical diseases but also non-physical diseases. Efforts to protect victims are very important. This is because it can not only reduce the suffering of the victims as a result of the crimes they suffered, but it can also prevent the continuation of the attack, so

the level of crime will decrease. Therefore, the author carefully looks at the protection of the law. of the victims I want to see. cybercrime in Indonesia.

B. Problem Formulation

In order to avoid expansion in the discussion of this article, the author limits the formulation of the problem to be discussed, namely what is the form of legal protection for victims of cyber crime in Indonesia?

C. Research Methods

In discussing this problem, the author uses a normative juridical method, to see how legal principles and legal synchronization apply to the legal protection of victims of cybercrime in Indonesia. The approaches used are a conceptual approach, a normative approach and a case law approach. In this case, it concerns legal protection for victims of cybercrime in Indonesia.

D. Discussion

1) Legal Protection for Cybercrime Victims in Indonesia.

Cybercrime or cybercrime is a term that refers to criminal activities involving computers or computer networks which become tools, targets or places where crimes occur Law in principle is a regulation of the attitudes (behavior) of a person and society for which violators are given sanctions by the state. Even though the cyber world is a virtual world, laws are still needed to regulate people's attitudes, in at least two things, namely:

Firstly, society in the virtual world is society in the real world, society has values and interests, both individually and collectively, that must be protected.

Second, even though they occur in cyberspace, transactions carried out by the public have an influence in the real world, both economically and non-economically.

Currently the regulation used as the legal basis for cybercrime cases is Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE). With the ITE Law, it is hoped that it can protect people who use information technology in Indonesia, this is important considering the number of internet technology users is increasing from year to year. The increasing use of the internet on the one hand provides many conveniences for humans in carrying out their activities, on the other hand it makes it easier for certain parties to commit criminal acts, progress this technology also influences human lifestyles and thought patterns, in fact currently many crimes occur using information technology. Cybercrime, which spreads rapidly regardless of borders, requires caution because its characteristics are very different from those of general crimes. The use of information technology plays an important role in the country's trade and economic growth to achieve social welfare, the government should support the development of information technology through legal and regulatory frameworks to make good use of information technology . Abuse of Indonesian people's religious and social values and caution. According to the provisions of article 4, paragraph 2 of the ITE Law, the government will protect the interests of the public from all types of interference arising from electronic communications and the misuse of electronic information that is harmful to people's lives. Legal requirements. These malicious acts of information technology, which can cause harm to other people, countries and countries that use computer equipment and Internet facilities, may be carried out by groups of criminals or businessmen or, without the knowledge of the person who was affected by it, will cause damage to people, property and body. Loss due to destruction. Data generated by hackers. Eradicating cybercrime requires law enforcement to be knowledgeable and technologically savvy. The problems victims face are due to ignorance, computer and internet literacy, so if there are victims, they cannot report all the dangers they face, which means it's a problem for all of us. The purpose and purpose of this law is that the use of information technology and electronic communications is carried out in accordance with the principles of legal security, interest, prudence, good faith and freedom of choice or non-technological. Therefore, the use of information technology and electronic transactions can be interpreted as expected to have legal validity, benefit, prudence, good faith, freedom to choose technology and neutrality. In response to the needs and challenges of global communication through the Internet, the law aims to answer all legal issues related to global

technological development, and all problems are expected to arise, including the negative effects of Internet misuse. Users may be confused.

There are several other positive laws that apply generally and can be imposed on cybercrime perpetrators, especially for cases that use computers as a means, including:

a. Criminal Code
b. Law Number 11 of 2008 concerning ITE
c. Law Number 44 of 2008 concerning Pornography
d. Law Number 36 of 1999 concerning Telecommunications.
e. Law Number 5 of 1999 concerning Prohibition of Monopoly Practices and Unfair Business Competition.
f. Law Number 8 of 1999 concerning Consumer Protection.
g. Law Number 19 of 2002 concerning Copyright.
h. Law Number 8 of 1997 concerning Company Documents
i. Law Number 25 of 2003 concerning Amendments to Law Number 15 of 2002 concerning the Crime of Money Laundering
j. Law Number 15 of 2003 concerning Eradication of Terrorism

Maintaining and protecting the technology user community requires cooperation and seriousness from all parties considering that information technology, especially the internet, has been used as a means to build a society with an information culture. It is hoped that the existence of laws regulating cybercrime can protect and provide a sense of security for those who use technology as a forum for carrying out transactions or carrying out economic activities. In taking action against those who abuse technological developments, quality human resources are needed who have the ability and expertise in the field of technology. Law enforcement is influenced by at least several factors, namely the legal rules themselves or the law, the implementing apparatus of these rules, namely the law enforcement officers, and the legal culture itself, namely the community itself which is the target of the law. The electronic information and transaction law (UU ITE) or what is called cyberlaw, is used to regulate various legal protections for activities that use the internet as a medium, both transactions and use of information. The ITE Law also regulates various kinds of punishments for crimes via

the internet. ITE Law accommodates the needs of business people on the internet and society in general to obtain legal certainty by recognizing electronic evidence and digital electronic signatures as valid evidence in court. The ITE Law itself is new in Indonesia and was ratified by the DPR on March 25 2008. The ITE Law consists of 13 chapters and 54 articles which examine in detail the rules of life in cyberspace and the transactions that occur in it. With the ITE law, it is hoped that it can provide a sense of security and protect those who use technology. Apart from that, in certain and dangerous circumstances, those who are victims of technology crimes are also entitled to legal protection, this is stated in Law Number 13 of 2006 concerning Witness and Victim Protection (UU PSK). In the provisions of Article 5 of the PSK Law, it is stated that:

1) A witness and victim have the right to:

a. Obtain protection for personal, family and property security the object, and free from threats relating to testimony which he will, is, or has given;

b. Participate in the process of selecting and determining the form of protection and security support;

c. Provide information without pressure;

d. Get a translator;

e. Free from ensnaring questions;

f. Obtain information regarding case developments;

g. Obtain information regarding court decisions;

h. Know if the convict is released;

i. Getting a new identity;

j. Obtaining a new residence;

k. Obtain reimbursement for transportation costs according to needs;

l. Obtain legal advice and/or;

m. Get temporary living expenses assistance until the protection period ends.

2) The rights specified in paragraph (1) are granted to witnesses and/or victims of criminal acts in certain cases according to the decisions of the LPSK. In addition, Article 1, paragraph 2 of the PSK Law states that "any person who suffered physical, mental or economic suffering as a result of a criminal act". The victim in this case refers to a person who has suffered material

damage or harm as a result of a cybercrime. There are two models of legal protection for victims of cybercrime: the customary rights model and the services model :

1). Procedural Rights Model In the procedural rights model, cybercrime victims have the right to file criminal complaints, assist prosecutors, or appear at all levels of justice when information is required. In this model, victims are given the opportunity to "recoup" the perpetrator of the harm they have suffered. In this procedural model, victims are asked to be more proactive in helping law enforcement officers handle their cases, especially those involving new cyber activities. The presence of the authorities can restore the confidence of those who have been harmed by the person responsible (the perpetrator), and it is also something that prosecutors can take into account if they oppose and very simple assumptions. .

2). Service Model (Service Model)

This service model addresses the need to create standards for the development of victims of cybercrime. This model views victims as people who need the services of the police and other law enforcement officers. If law enforcement officers do a good job of dealing with victims of cybercrime, it will have a positive effect on law enforcement, especially cybercrime, because victims of these developments will have more confidence in technology for their businesses. By providing services to victims, law enforcement officers help victims feel that their rights and interests are protected. During the trial period, especially when it comes to proving cyber crimes, many cases arise due to the development of information technology. It is necessary for law enforcement officers to have access to reliable personnel who are knowledgeable and technologically aware, considering that cybercrime is a new crime that deserves to be punished. Governments are paying more attention to crime in cyberspace because of its global implications. Act No. 11 of 2008 is expected to help law enforcement officers protect those who use the technology. While providing legal protection to victims of cybercrime, law enforcement agencies, especially the police, have taken steps to curb the rise in cybercrime. One is support for the technology user community and victims. Cybercrimes: You can report scams you've experienced by reporting them to us email address is cybercrime@polri.go.id. If you include the attacker's account and phone number in the report, you can track them immediately. To overcome this increase in crime, fraud, online selling etc. The National Police

sends a special email to receive complaints related to cyber activity. The importance of legal protection for victims of cybercrime is important not only in the framework of law enforcement, but also in the preventive measures taken by officers to reduce or prevent the occurrence of victims of cybercrime. Of course, it's not just a news jar, it's supposed to lead to real action by law enforcement to keep those who use technology to conduct their business online safe.

2) The provisions of the Penal Code of Law No. 11 of 2008 on Electronic Information and Communications (UU ITE).

As a constitutional state, the government's duty to protect all citizens from acts harmful or harmful to society is a duty of legal protection. Laws, technologies, and technologies that a country provides to people using technology have different words, but they influence each other and affect people's own lives. Indonesia's law on technical crimes (cybercrime) can be viewed in two methods: the general method and the narrow method. Basically, cybercrime is any crime that uses any means or is facilitated by electronic systems. This means that all crimes can be included in the Penal Code (KUHP), if they use assistance or methods, such as terrorism or human trafficking. In a general sense, they are categorized into online banking, banking services and money laundering. However, the cybercrime law in a strict sense is included in Law 11 of 2008 on Electronic Information and Activities (UU ITE). The ITE Law classifies certain crimes in the category of cybercrime.

a. Criminal acts related to illegal activities, namely:

1) Distribution or dissemination, transmission, accessibility of illegal content consisting of:

a) Morality (Article 27 paragraph (1) of the ITE Law);

"Every person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents which have content that violates decency."

b) Gambling (Article 27 paragraph (2) of the ITE Law);

"Every person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that have gambling charges."

c) Insults and defamation (Article 27 paragraph (3) of the ITE Law);

"Every person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents which contain insulting and/or defamatory content."

d) Extortion or threats (Article 27 paragraph (4) of the ITE Law); "Every person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents which contain blackmail and/or threats"

e) Fake news that misleads and harms consumers (Article 28 paragraph (1) of the ITE Law);

"everyone intentionally and without right spreads false and misleading news which results in consumer losses in electronic transactions"

f) Causing feelings of hatred based on SARA (Article 28 paragraph (2) of the ITE Law);

"everyone intentionally and without right disseminates information aimed at creating feelings of hatred or enmity towards certain individuals and/or groups of people based on ethnicity, religion, race and inter-group (SARA)"

g) Sending information containing threats of violence or intimidation aimed at you personally (Article 29 of the ITE Law); "every person intentionally and without authorization sends Electronic Information and/or Electronic Documents that contain threats of violence or intimidation aimed at personally"

2) By any means by means of illegal access (Article 30 of the ITE Law):

a) Any person intentionally and without authorization and unlawfully accesses another person's computer and/or electronic system in any way.

b) Every person intentionally and without right or against the law accesses a computer and/or electronic system in any way with the aim of obtaining electronic information and/or Electronic Documents.

c) Any person intentionally and without or against the law accesses the Computer and/or Electronic System in any way by violating, breaking through, surpassing, or breaching the security system.

3) Illegal interception of electronic information or documents and systems electronic (Article 31 of the ITE Law)

a) Every person intentionally and without right or against the law intercepts or intercepts Electronic Information and/or Electronic

Documents on a computer and/or certain Electronic System belonging to another person.

b. Criminal acts related to interference

1) Interference with Information or Electronic Documents (data interference Article 32 of the ITE Law)

"Any person intentionally and without right or against the law in any way changes, adds, reduces, transmits, damages, deletes, moves, hides electronic information and/or electronic documents belonging to other people or public property."

2) Interference with Electronic Systems (system interference Article 33 of the Law ITE)

"Any person intentionally and without right or against the law carries out any action which results in disruption of the Electronic System and/or causes the Electronic System to not work properly"

c. Criminal act of facilitating prohibited acts (Article 34 of the ITE Law)

1) Every person intentionally and without right or against the law produces, sells, reproduces for use, imports, distributes, provides, or possesses:

a) Computer hardware or software designed or specifically developed to facilitate the actions as intended in Articles 27 to Article 33;

b) Password via computer, access code or something similar intended to make the Electronic System accessible with the aim of facilitating actions as intended in Article 27 to Article 33.

d. Criminal act of falsifying electronic information or documents (Article 35 of the ITE Law)

"Every person intentionally and without right or against the law manipulates, creates, changes, deletes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are treated as if they were authentic data."

e. Additional criminal offenses (accessory to Article 36 of the ITE Law)

"every person intentionally and without right or against the law commits acts as referred to in Articles 27 to Article 34 which result in harm to other people." In addition, the ITE Law also regulates very serious criminal provisions for perpetrators of cyber crimes that are regulated in Articles 45 to Article 52 the criminal threat ranges from 6 (six) years to 12 (twelve) years in prison and a fine starting from Rp. IDR 600,000,000.00 (six hundred million rupiah) up to IDR 12,000,000,000.00 (twelve billion rupiah). Apart from regulating material cyber crimes, the ITE Law also regulates formal criminal acts, especially in the field of investigations. Article 42 of the ITE Law regulates that investigations into criminal acts in the ITE Law are carried out based on the provisions in Law Number 8 of 1981 concerning Criminal Procedure Law (KUHAP) and provisions in the ITE Law. This means that the investigation provisions in the Criminal Procedure Code remain in effect as long as they are not regulated otherwise in the ITE Law. With the existence of material and formal regulations that regulate crime in cyberspace, it can at least help law enforcement officials in dealing with crimes that occur in cyberspace, both conventional crimes and modern crimes. With the hope of providing a sense of security for people who use information

technology considering that this technological crime knows no time and space and can happen to anyone at any time.

E. Conclusion

To provide legal protection to victims of cybercrime, the government enacted the Electronic Communications (ITE) Act No. 11 of 2008. The ITE Act also provides for various penalties for crimes committed on the Internet. The ITE Act follows the needs of Internet entrepreneurs and the entire community to ensure the integrity of the law by recognizing electronic evidence and digital electronic signatures as valid evidence in court. The ITE Law consists of 13 chapters and 54 articles that describe the rules of being online. And the transactions that take place in it. Prohibited acts (cybercrimes) are explained in Chapter 7 (Articles 27-37). In addition, if necessary in specific cases, victims of cybercrime may request assistance from the LPSK, which is also established in Law No. 13 of 2006 on the Protection of Witnesses and Victims (UU PSK) regarding the legal protection of witnesses and the crime . make sacrifices There are two avenues available for legal protection for victims of cybercrime. These are: 1) a model for the authorities that will strengthen the role of victims and help prosecutors to carry out trials and the right to participate in all stages of the judicial process; and police officers and other law enforcement officers; Victims of cybercrime and international support should be offered at all stages of the investigation, starting with the investigation, trial and post-trial.

DAFTAR PUSTAKA

A. Buku

Andi Hamzah, 1990, Aspek-aspek Pidana di Bidang Komputer, Sinar Grafika,Jakarta.
Arif Gosita, 2004, Masalah Korban Kejahata, PT Bhuana Ilmu Populer, Jakarta
Barda Nawawi Arief, 2000, Perlindungan HAM dan Korban dalam Pembaharuan Hukum, Citra Aditya Bakti, Bandung.
Dikdik M Arief Mansyur dan Elisatris Gultom, 2008, Urgensi Perlindungan Korban Kejahatan, PT Raja Grafindo Persada, Jakarta.

J.E Sahetapy, 1987, Viktimologi Sebuah Bunga Rampai, cet.I, Pustaka Sinar Harapan, Jakarta.

Josua Sitompul, 2012, Cyberspace, cybercrime, cyberlaw, Tinjauan Aspek Hukum Pidana, PT. Tatanusa, Jakarta.

Muladi dan Barda Nawawi Arif, 1992, Bunga Rampai Hukum Pidana, Alumni,Bandung.

B. Undang-undang

Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.

C. Akses Internet

http://id.wikipedia.org/wiki/Kejahatan_dunia_maya.

http://alwaysahabat.blogspot.com/2012/11/artikel-cybercrime.html

www.tribun-timur.com.

www.kompas.com