Eduvest – Journal of Universal Studies
Volume 4 Number 9, September, 2024
p- ISSN 2775-3735- e-ISSN 2775-3727

THE STAND OF ELECTRONIC EVIDENCE IN CYBER CRIME LAW ENFORCEMENT IN INDONESIA

Dewic Sri Ratnaning Dhumillah
Sekolah Tinggi Ilmu Hukum IBLAM Jakarta Pusat, Indonesia
Email: dewicsri@iblam.ac.id

ABSTRACT

Crime in the cyber world certainly has a significant impact. People think that Indonesia has a Criminal Code that cannot cover crimes in cyberspace, which is a new crime. This is what makes the government have to issue regulations regarding cyber crime or cyber crime. With regard to enforcing cybercrime law, of course, a regulation is needed in positive law. It also regulates the punishment and how the evidence for cyber crimes and the position of electronic evidence are. This research method uses the normative method. The existence of electronic evidence in proving cybercrime has been alluded to in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. In Article 5 of Law Number 11 of 2008, it explicitly mandates that "Electronic Information and/or Electronic Documents and/or their printouts are valid legal evidence". This can be interpreted that electronic documents are considered legally valid according to positive law in Indonesia. However, in the amendment to the elucidation of Article 5 paragraph (1) regulated in Law Number 19 of 2016, it is explained that the existence of Electronic Information and/or Electronic Documents is binding and recognized as valid evidence to provide legal certainty for the Implementation of Electronic Systems and Transactions Electronic, especially in proving and matters relating to legal actions carried out through Electronic Systems.

KEYWORDS *Electronic Evidence, Punishment, Cyber Crime*

INTRODUCTION

In social life in society there are events that are closely related to law, so they are called legal events. Legal events are different from ordinary events, because they have legal aspects that carry certain legal consequences. In LJvan Apeldoorn's view, it is said that law is a power that regulates and compels, with no end in sight the relationships generated by human society (van Apeldoorn, 2011). Human life then has an allusion that can become a crime or an action that fulfills the elements

How to cite: Dewic Sri Ratnaning Dhumillah. (2024). The Stand Of Electronic Evidence In Cyber Crime Law Enforcement In Indonesia. Journal Eduvest. *4*(9): 7549-7559
E-ISSN: 2775-3727
Published by: https://greenpublisher.id/

of a criminal act. In this regard, in the reality of current conditions, criminal incidents do not only occur in the real world but can also occur in cyberspace or cyberspace.

This cannot be separated from the development of information and communication technology which is currently difficult to separate from human life. The development of Information Technology brings convenience to human life. One manifestation of developments in the world of information technology is internet media which can connect the world without any restrictions (Raodia, 2019). Such dynamics also bring about quite significant social, cultural and economic changes. Starting from population management to the buying and selling transaction process (Ismail, 2009).

The embeddedness of information technology in human life means that crimes or criminal acts can also be committed in cyberspace. This has become known as crime in cyberspace or commonly referred to as cyber crime (Wahyudi, 2013).This arises from inappropriate use which can result in the emergence of criminal acts which are ultimately called cyber crimes.

Of course, existing positive legal regulations also follow the dynamics of human life. Cyber crime is a new phenomenon that has emerged in the form of criminal acts which can have a direct impact in terms of the development of information technology which uses the internet as the main medium for committing these crimes. Technological developments facilitate developments in the world of crime. Plus, people are not yet very aware of developments in the world of information and technology.

With the development of technology, crime has also developed. In the past, a crime or crime was an action that involved physical contact between the victim and the perpetrator of the crime. However, nowadays criminal acts or crimes have undergone a transformation so that there is no longer any physical contact between the perpetrator and the victim. Perpetrators who commit crimes in cyberspace use technology such as the internet and other electronic tools to commit these crimes (Sari, 2021).

Internet media can indeed provide positive opportunities for society. However, on the other hand, it can also make it easier for perpetrators to commit crimes. Moreover, without any physical contact, the perpetrators can do this without having to worry about their identity being revealed by the victim. This cyber crime is more hidden and can be carried out across time and space and has a wide global reach. Only with an internet network and competent electronic equipment can criminals be able to carry out cyber crimes and prey on their victims (Alhakim & Sofia, 2021).

The development of the world of cyber crime is indeed increasingly rapid with more and more terms appearing, such as cyber money laundering, high tech white collar crime and online business crime. In the UN document there are other terms such as Dogpilling, Dixing and Doxware.

Cybercrime certainly has a significant impact. The public assumes that Indonesia has a Criminal Code that cannot cover cybercrime, which is a new crime. This is what makes the government have to issue regulations regarding cybercrime.

The Law on Information and Electronic Transactions or the ITE Law which is stated in Law No. 19 of 2016 which contains amendments to Law No. 11 of 2008

Policies regarding criminalization that use a penal approach will of course relate to criminal acts and regulate the scope of criminal law in the form of sanctions and actions (Hartanto, 2021). From a criminalization perspective, a fairly strategic policy in this non-penal facility is preventive action. And penal policies are still needed as a way of dealing with crime, which is a means of law enforcement (Galih, 2019). With regard to cyber crime law enforcement, of course a positive law regulation is needed. It also regulates the punishment and how to provide evidence for cyber crimes as well as the position of electronic evidence.

RESEARCH METHOD

The research uses normative legal methods which will focus on studies through analysis of rules in legal norms. This research will be analyzed descriptively qualitatively by comparing the formulation of legal norms in relation to phenomena that occur in the field. The collection of legal materials was carried out by reviewing statutory norms supported by a library study of relevant legal literature.

RESULT AND DISCUSSION

The research uses normative legal methods which will focus on studies through analysis of rules in legal norms. This research will be analyzed descriptively qualitatively by comparing the formulation of legal norms in relation to phenomena that occur in the field. The collection of legal materials was carried out by reviewing statutory norms supported by a library study of relevant legal literature.

Setting Up Electronic Evidence In Positive Law

The considerations for Law Number 11 of 2008 concerning Information and Electronic Transactions, starting from philosophical reasons in the form of a narrative regarding national development. The form of narrative is an ongoing process that must always be responsive to the various dynamics that occur in society. This was then continued with the presence of information globalization which has placed Indonesia as part of the world information society. Therefore, it is necessary to establish regulations regarding the management of Information and Electronic Transactions at the national level, so that the development of Information Technology can be carried out optimally, evenly, and spread to all levels of society, in order to make the nation's life more intelligent (Nugroho, 2021). As a result of the globalization of information which then influences the course of national development which should go hand in hand with the development and progress of Information Technology, it has caused changes in human life activities in various fields. As a result of this, sociological reasons emerge for the use of Information Technology to play an important role in trade and growth national economy. Development of information technology through legal infrastructure and regulations, so that the use of Information Technology is carried out safely to

prevent misuse, taking into account the religious and socio-cultural values of the Indonesian people. After explaining the philosophical and sociological reasons, this consideration is complemented and strengthened by juridical reasons, in the form of the use and utilization of Information Technology which must continue to be developed (Hamzah & Marsita, 2015).

With the aim of safeguarding, maintaining and strengthening national unity and integrity based on laws and regulations in the national interest. The amendment to Law Number 19 of 2016, the Preamble only contains juridical reasons for deficiencies in Law Number 11 of 2008. This includes ensuring recognition and respect for the rights and freedoms of other people. To fulfill fair demands in accordance with considerations of security and public order in a democratic society, it is necessary to amend Law Number 11 of 2008, Concerning Information and Electronic Transactions, in order to realize justice, public order and legal certainty.

If you read carefully the difference between Electronic Information and Electronic Documents, Electronic Information is part of Electronic Documents. Electronic Documents are definitely Electronic Information, but Electronic Documents are not necessarily Electronic Information. What makes Electronic Information Electronic Documentation is the phrase "which is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar form, which can be seen, displayed, and/or heard via a computer or system Electronic.

Article 2 of Law Number 11 of 2008, which reads "This Law applies to every person who commits legal acts as regulated in this Law, whether within the Indonesian legal territory or outside the Indonesian legal territory, which has consequences laws in the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia and are detrimental to Indonesia's interests." The author sees a legal loophole in the sound of this article where the phrase "applies to every person who commits legal acts whether within the jurisdiction of Indonesia or outside the jurisdiction of Indonesia". This norm exceeds its proper authority. Each country has its own sovereignty so that a law by one country cannot regulate legal actions outside its legal territory/jurisdiction where it is sovereign. As we understand, a legal norm can be applied when the country has entered into a bilateral or multilateral agreement. Or even adopting an international convention and having effectively ratified and enforced it. The phrase "which has legal consequences in the Indonesian jurisdiction and/or outside the Indonesian jurisdiction and is detrimental to Indonesia's interests" gives rise to a one-sided interpretation that only benefits Indonesia's interests and is not balanced. Even though Article 8 of Law Number 11 of 2008 regulates the authority to choose the law that applies to international electronic transactions, this phrase gives the impression that this law is only there to prevent losses for Indonesia, not to resolve disputes in a balanced and complete manner.

In Article 5 of Law Number 11 of 2008, it is explicitly mandated that "Electronic Information and/or Electronic Documents and/or printouts are valid legal evidence". This can be interpreted to mean that electronic documents are considered valid according to positive law in Indonesia. However, in the amendment to the explanation of Article 5 paragraph (1) regulated in Law Number 19 of 2016, it is explained that "The existence of Electronic Information and/or

Electronic Documents is binding and recognized as valid evidence to provide legal certainty for the Implementation of Electronic Systems and Electronic Transactions, especially in evidence and matters relating to legal acts carried out through Electronic Systems." This can be interpreted to mean that there is a narrowing of the use of electronic documents as evidence from the previous Law. If previously there was no limitation that the electronic document must contain a legal act, and there was also no requirement (imperative) that the electronic document, if it is the result of interception or wiretapping, or recording which is part of wiretapping, must be carried out in the context of law enforcement at the request of the police, prosecutor's office, and/or other institutions whose authority is determined by law.

Then the next paragraph mandates "Electronic Information and/or Electronic Documents and/or printouts as referred to in paragraph (1) are an extension of valid evidence in accordance with the Procedural Law in force in Indonesia." This means that electronic information and electronic documents, as well as printed results, can be equivalent to various types of evidence such as letters, witnesses, allegations, confessions and oaths in the realm of Civil Law. Likewise, electronic documents can be equated with witness statements, expert statements, letters, instructions and defendant statements in the realm of criminal law. Then further in the next paragraph "Electronic Information and/or Electronic Documents are declared valid if using an Electronic system in accordance with the provisions regulated in this Law". The author interprets that, electronic information/electronic documents/printed results can be used and are valid only if they appear as a result of an appropriate electronic system and are regulated in law. Furthermore, apart from having to use an electronic system that is regulated for proving criminal cases, evidence obtained from interception or wiretapping or recording which is part of wiretapping for law enforcement, must be at the request of the Police, Prosecutor's Office or Institutions regulated in the Law.

Enforcement of Cyber Crime Laws

According to criminal law policy and positive law, criminal acts in the field of information technology are defined as acts that violate legal provisions. Meanwhile, criminal law policy itself has a general basis which functions as direction for the government in managing and regulating problems in society as well as problems regulated in law and the application of the law.

The Criminal Code, which is the criminal justice system in Indonesia, has a conventional nature. And in it there has been no development regarding crime in the cyber world. There are several laws and regulations that regulate crimes in the cyber world and are also related to criminal acts. However, it is outside the provisions of the Criminal Code. These Legislative Regulations are:

1. UU no. 36 of 1999 concerning Telecommunications
2. UU no. 19 of 2002 concerning Copyright
3. UU no. 25 of 2003 concerning Amendments to Law no. 15 of 2002 concerning the Crime of Money Laundering
4. Law No. 15 of 2003 concerning Criminal Acts of Terrorism

5. UU no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions.

The increasing number of cyber crimes has certainly made the government issue regulations specifically regulating information technology crimes by issuing Law No. 19 of 2016. This ITE Law certainly has a hope that can be a force in overcoming cyber crimes. From a sociological perspective, society needs a regulation that can be a real and tangible legal basis and reference regarding regulations in the field of information technology. Before the issuance of this Law, the regulations in society were only related to the world of information and technology. There has been no explanation and description of criminal sanctions and a much more concrete explanation of this world. This ITE Law regulates various community activities when interacting in cyberspace (Abidin, 2015).

The ITE Law itself meets sociological and philosophical requirements. The presence of a legal basis in this philosophical field is contained in the 1945 Constitution in Article 28F which states that every community has the right to obtain, process, search for and possess and store and convey all information using all channels available within that community. This cyber crime is contained in Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 which consists of (Arief, 2006):

1. Article 27 paragraph (1) Law no. 11 of 2008, every person who intentionally distributes and/or transmits without the right to access information that violates the provisions of decency. However, in this article nothing is found regarding any activities that violate the content of decency. The amendment to the law states that cyber pornography and online prostitution are content that violate decency. (Mudadi & Barda Nawawi, 2010). And criminal penalties will be much more severe if this happens to minors.
2. Defamation, slander and insults are contained in Article 27 paragraph (3) of Law no. 11 of 2008 which states that every person intentionally and without right distributes and transmits insults and defamation by accessing electronic information and documents. This action can be found in the comments column on social media in cyberspace. Perpetrators of these crimes can receive criminal sanctions
3. Online gambling, one of the criminal acts included in cyber crime is online gambling which is regulated in Article 27 Paragraph (2) of Law no. 11 of 2008 which states that every individual who deliberately distributes and transmits so that they can access information and/or electronic documents (Abdul Wahid & Labib, 2005)
4. Cyber stalking, this criminal act is regulated in Article 29 which states that any individual who intentionally and without authorization sends information and/or electronic documents containing threats of violence and/or spreading fear to individuals or individuals. This regulation is the same as legal regulations abroad where stalking takes the form of harassment, threats and even causing fear. Starting from mail bombs, obscenity threatening emails.

5. Extortion, this criminal act is outlined in Article 27 paragraph (4) which contains every individual who knowingly and without right distributes and transmits information and/or electronic documents containing contents containing extortion.
6. Hate speech, this criminal act is regulated in Article 28 paragraph (2) which states that every individual creates feelings of hatred and/or hostility towards individuals and community groups based on SARA.
7. Hoax, the spread of false news or hoaxes is regulated in Article 28 paragraph (1) which states that every individual who intentionally or unintentionally spreads false news and misleads the public so that it can harm consumers in electronic transaction activities. (Suseno, 2012)
8. Interception, this action is regulated in Article 31 which consists of several actions, namely:
    a. Any individual who intentionally or unintentionally violates the law and intercepts information and electronic documents from individuals or institutions
    b. Any individual who carries out illegal and unlawful interception without public intent from, to and within electronic devices belonging to other parties which does not cause changes to the loss of electronic information and/or documents.
    c. Interception carried out by law enforcement at the request of law enforcement officers is permitted.
9. Illegal access, in article 30 of Law no. 11 of 2008 states several classifications of illegal access, namely:
    a. Any individual who intentionally violates the law by accessing another party's electronic devices
    b. Individuals who intentionally access electronic data with the aim of obtaining electronic information and documents
    c. Any individual who accesses documents belonging to other parties by breaking into and breaching the security system
10. Crimes against Data Interference information are outlined in Article 32 of Law No. 11 of 2008 which consists of:
    a. Any individual who violates the law by changing information and electronic documents belonging to other parties, whether individuals or the public
    b. Any individual who violates the law by transferring data and information without permission
    c. Actions that could result in the disclosure of state secrets that can be accessed by the public
11. Disturbance to cyber systems is stated in Article 33 where it is stated that every individual who violates the law with actions that can cause disruption in cyberspace so that they cannot work properly
12. Misuse of devices is stated in Article 34 in the form of changing passwords in the cyber security system and also access codes which could harm other parties. However, this action does not fall into the criminal realm if it is intended as research and testing of electronic systems.

13. Forgery and fraud are stated in Article 35 which states that any individual who deliberately manipulates, falsifies and destroys and also defrauds information and/or electronic documents that are considered authentic data.

Crime in the cyber world, also known as cyber crime, is always synonymous with computer crime. In fact, cyber crime is a computer crime that is committed illegally (Hamzah, 1989). This action is included in a criminal offense with several classifications consisting of:

This classification of crimes in cyberspace or cyber crime has several classifications determined based on the Convention on Cybercrime in Budapest, Hungary, which consists of:

1. Illegal Interception

This action is to intentionally capture the transmission and transmission of computer data that is confidential and not for public consumption.

2. Data Interference

An action carried out deliberately, such as destroying or deleting data and/or documents and electronic information on computers and cyber space.

3. System Interference

Intentionally causing interference or obstacles that cause the computer system to not run or function properly.

4. Misuse of Devive

Misuse of electronic equipment such as computer programs and passwords and access codes

5. Computer Related Forgery

An act of forgery carried out intentionally so as to change and delete authentic data to become inauthentic so that the forged data becomes data used by the public.

6. Computer Related Fraud

A criminal act of fraud intentionally and without right causes the wealth and/or goods of another party to disappear. This is done by entering and deleting data so that the computer system is disturbed with the intention of gaining personal gain.

7. Content Related Offenses

Criminal acts that are closely related to the world of pornography for minors

8. Offenses Related to Infringements of Copyright and Related Rights.

Cyber crimes are closely related to copyright infringement.

The role of virtual police and cyber police in maintaining security in cyberspace is really needed. Virtual police have a role in providing education and information to the public regarding the Information and Electronic Transactions Law. Meanwhile, the cyber police play a more important role in following up on cases circulating in society that cannot be reprimanded and warned by the virtual police. According to the rules, the virtual police will give a warning and warning first. After that, the cyber police will take action if the perpetrator does not heed the warning.

Even though we already have a cyber team and are also supported by technology, it turns out that this has not been able to help maximally in dealing with

crime in the cyber world. Often during searches and investigations, sufficient evidence is not found and the perpetrators are not caught due to the relatively easy access for the perpetrators using computers anywhere without any witnesses. Cyber police can only search for IP addresses. If the perpetrator searches from an internet cafe, the level of difficulty in tracking will be greater. The reason is that not all internet cafe service providers register. There are several obstacles in law enforcement in the form of:

1. Constraints within law enforcement

   Lack of a special team that handles crime problems in cyberspace. Added to this is the difficulty in finding out the whereabouts of the perpetrator even though the technology used is quite good. Moreover, it is easy for perpetrators to access computers from anywhere

2. External constraints

   Lack of understanding from other law enforcement officials regarding cyber crimes. Permission from the head of the court and also the public prosecutor is sometimes not optimal, causing the cyber team to lose track of the search.

The Ministry of Defense and the Indonesian National Army also support the coordination of cyber security in all sectors that are in accordance with needs and also have the nature of protecting state secrets. From this interest, anticipation is needed in cyber defense needs. One of them is the policy that is the basis for cyber defense, such as development, coordination and operations which include preparation of infrastructure and technology as well as human resources to roles and authority within the government.

Strong and effective government institutions are certainly needed in carrying out their role in government and supporting cyber defense which refers to policies in government institutions. Technology and infrastructure must support cyber defense activities so that they can be carried out effectively and efficiently. In government institutions, human resources are available who are continuously trained so that they can have special knowledge and skills in cyber defense.

There are several principles of cyber defense according to Permenhan No. 82 which consist of:

1) Have a security model that is structured and also integrated with standards and information guidelines that have been established by institutions or institutions that have authority
2) The integrity, confidentiality and availability factors are the basic principles of information security.
3) Has policy, institutional and technological elements as well as supporting infrastructure such as adequate human resources
4) The implementation of this cyber defense is supported by human resources with high quality, competence and integrity and upholds state confidentiality.
5) This is done in an effective and efficient manner so that cyber security is integrated by maximizing open technology in the context of state sovereignty and independence
6) Cyber security and defense that has superior and competent HR categories or criteria

7) Have governance principles that can realize supervision in cyber defense
8) Ensure the implementation of cyber defenses that are safe and can also withstand attacks from external parties
9) Avoid losses to computer systems
10) Developing conditions that can benefit the government.

This cyber defense is intended to prevent cyber crimes that could occur against government institutions and organizations. This cyber defense has roles and tasks consisting of;

1) Ensuring cyber security in government and society
2) Maintain confidential information resources belonging to the government
3) Maintain security of infrastructure and technology in the government environment
4) Encourage active participation with national and international networks across sectors
5) Improving capabilities and taking action against crimes in the cyber world
6) Develop effective, efficient and accountable cyber defense
7) Has the ability to maintain the confidentiality of state property and also the security of strategic networks
8) Data center model and also safe supporting facilities for maintaining strategic information.

CONCLUSION

The existence of electronic evidence in proving cyber crimes has been touched upon in Law (UU) Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

REFERENCES

Abidin, Dodo Zaenal. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Processor*, *10*(2), 509–516.

Alhakim, Abdurrakhman, & Sofia, Sofia. (2021). Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia. *Jurnal Komunitas Yustisia*, *4*(2), 377–385.

Arief, Barda Nawawi. (2006). *Tindak pidana mayantara: perkembangan kajian cyber crime di Indonesia*.

Galih, Yuliana Surya. (2019). Yurisdiksi Hukum Pidana Dalam Dunia Maya. *Jurnal Ilmiah Galuh Justisi*, *7*(1), 59–74.

Hamzah, Andi. (1989). Aspek-Aspek Hukum Pidana di Bidang Komputer. *Jakarta: Sinar*.

Hamzah, Andi, & Marsita, Budi. (2015). Aspek-Aspek Pidana di Bidang Transaksi Online. *Jakarta: Sinar Grafika*.

Hartanto, Hartanto. (2021). PERLINDUNGAN HUKUM PENGGUNA TEKNOLOGI INFORMATIKA SEBAGAI KORBAN DARI PELAKU CYBER CRIME DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE). *HERMENEUTIKA: Jurnal Ilmu Hukum*, *5*(2).

Ismail, Dian Ekawati. (2009). Cyber crime di Indonesia. *Jurnal Inovasi*, *6*(03).

Nugroho, Agus Digdo. (2021). DOKUMEN ELEKTRONIK Tantangan Transformasi Karakteristik Akta di Era Digital dan Konsekuensi Hukumnya, Yogyakarta: Sulur Pustaka, 2021. *Yogyakarta: Sulur Pustaka*.

Raodia, Raodia. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie: Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, *6*(2), 230–239.

Sari, Utin Indah Permata. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58–77.

Suseno, Sigid. (2012). *Yurisdiksi Tindak Pidana Siber*. Refika Aditama.

van Apeldoorn, L. J. (2011). *Inleiding Tot De Studie Van Het Nederlandse Recht (Pengantar Ilmu Hukum)*. Diterjemahkan oleh Oetarid Sadino, Pradnya Paramita, Jakarta.

Wahyudi, Dheny. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia. *Jurnal Ilmu Hukum Jambi*, *4*(1), 43295.