AHMAD DAHLAN INDONESIAN LAW JOURNAL
Vol. 1. No.1, June 2023, pp 11-19
10.12928/adil.v1i1.572
ISSN 3031-030X

ORIGINAL RESEARCH PAPER

OPEN ACCESS

Legality of Electronic Evidence in Cyber Crime Cases

July Wiarti

Islam Riau University, Riau, Indonesia
julywiarti@law.uir.ac.id
Submitted: December 20, 2022 | Revised: May 01, 2023 | Accepted: May 21, 2023

ABSTRACT

The rapid development of technology is currently a double-edged sword in the world of law, one side has a positive impact but on the other side it can also have a negative impact. The most clearly seen negative impact is the emergence of various kinds of criminal acts in the use of technology known as Cyber Crime. Electronic evidence is important in proving Cyber Crime, considering that in Indonesia itself the defendant is declared guilty if there are at least two valid pieces of evidence, and electronic evidence is vulnerable to being tampered with and so on. Then, what is the legality of electronic evidence in proving Cyber Crime cases? The results obtained are that whether electronic evidence is valid or not is determined by the material and formal requirements regulated in the ITE Law. Apart from that, digital forensics and expert witnesses also have an important role in proving Cyber Crime. Therefore, law enforcement officials should have a good understanding of this matter, so they can handle Cyber Crime cases better.

Keywords: Cyber Crime, Electronic Evidence, Legality

INTRODUCTION

As time goes by, humans will certainly experience developments in their lives. Likewise, the law must be able to cover human development within legal provisions, so that it can guarantee order, tranquility and peace for humans in living their lives in accordance with the purpose of the law. Regarding the law, it must follow the development of society, in accordance with von Savigny's teachings. The essence of his teaching is that: "das Recht wird nicht gemacht, est ist und wird mit dem Volke - law is not made, but grows and develops with society." (Lili & Ira, 2010:63)

Advances in science and technology or what is known as science and technology are currently growing rapidly. Advances in science and technology have now become an important part of human life. One of these developments is in the field of information technology such as the internet. As stated by Ermansjah in his book: "The advance of science and technology has accelerated the flow of information to all corners of the world. "What happens in other parts of the world will be known in a matter of minutes in other parts of the world." (Djaja, 2010:27)

This development certainly has a positive impact, namely making it easier for people to live their lives, but on the other hand, it can also have a negative impact, namely when it is misused to commit crimes. "Crimes that arise as a negative impact of the development of internet applications are called cyber crimes." (Wahid & Labib, 2010:39)

To prevent this negative impact from occurring, the Indonesian government has created a special legal regulation that regulates this, namely Law Number 11 of 2008 concerning

Electronic Information and Transactions which has been updated with Number 19 of 2016, which will hereinafter be referred to as Law ITE. The problem does not end there, because it turns out that in terms of overcoming cyber crime itself there are still obstacles. One of them is regarding the method of proof itself.

"Evidence is about whether or not the defendant actually committed the act charged, which is the most important part of criminal proceedings. In this case, human rights are at stake." (Hamzah, 2008: 249) So when carrying out this proof, great attention must be paid. The scope of cyber crime proof certainly concerns electronic information and/or documents, therefore one of the weaknesses of this is that electronic evidence is easy to change, manipulate and delete. Law enforcement officials have difficulty handling cyber crime cases, especially in providing evidence. (Sugiarto & Siregar, 2022: 217)

An example of a case that shows the difficulty of proof in a cyber crime case is what happened in Surakarta, the case of breaking into an email password, but the expert witness presented by the victim was unable to provide proof of this, so the defendant ended up acquitted. (Handoko, 2016:3)

So a good method of proof is needed, so that people who are truly guilty can be punished. This is what the author will examine in this article. Based on the background above, the problem that the author raises in this article is what is the legality of electronic evidence in proving cyber crime?

RESULTS AND DISCUSSION

1. Cyber Crime and its Regulation

Cyber crime is one of the dark sides of technological progress which can have a negative impact on modern life today. This concern was expressed in the cyber crime paper presented by ITAC (Information Technology Association of Canada) at the International Information Industry Congress (IIIC) 2000 Millennium Congress in Quebec on September 19 2000. This concern is also because it is closely related to economic crimes and organized crime . This matter regarding cyber crime has been on the agenda twice at the UN congress, namely at VIII/1990 in Havana and at Congress X/2000 in Vienna. (Arief, 2007:1)

"Terminologically, crimes based on information technology using computer media as currently occurring can be called by several terms, namely computer misuse, computer abuse, computer fraud, computer-related crime, computer-assisted crime, or computer crime." (Widodo, 2009:23) According to Barda Nawawi Arief, the meaning of computer-related crime is the same as cybercrime. (Arief, 2007:3)

Barda Nawawi in his book also contains several nicknames for this crime, including cyber crime, a new dimension of high tech crime, a new dimension of transnational crime, and a new dimension of white collar crime. (Arief, 2007:2)

Regarding the definition of cyber crime itself, there are differences of opinion from each expert. The following is the definition of cyber crime according to experts:

a. "Cyber crime is a crime committed by a person or group of people by using computer or internet services." (Djaja, 2010:32)

b. These crimes are divided into two categories: (Widodo, 2009:24)

    1) Cyber crime in the narrow sense, crime against computer systems;

    2) Cyber crime in a broad sense, includes crimes against computer systems or networks and crimes that use computer facilities.

c. Cyber crime is a new form or dimension of contemporary crime that has received widespread attention in the international world, as well as one of the dark sides of technological progress which has a very broad negative impact on all areas of modern life today. (Arief, 2007: 4)

d. Criminals see the characteristics of the internet as an opportunity or means for them to carry out evil intentions through various acts which are better known as cyber crimes. (Sitompul, 2012: 36)

e. Crimes that arise in cyberspace are known as cyber crimes. (Arief, 2010:77)

f. According to the British police, cyber crime is all kinds of use of computer networks for criminal purposes and/or high-tech crimes by abusing the convenience of digital technology. (Wahid & Labib, 2010:40)

g. The US Department of Justice defines computer crime as "any illegal act requiring knowledge of computers for its perpetration, investigation, or prosecution", meaning "any unlawful act that requires knowledge of computers to handle, investigate and prosecute." (Wahid & Labib, 2010:40)

h. Organization of European Community Development, namely "any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data", meaning "any illegal, inappropriate, unauthorized behavior relating to data processing and/or transmission data." (Wahid & Labib, 2010:40)

i. In the UN congress report computer. (Wahid & Labib, 2010:40)

j. "The broadest definition of cyber crime is all criminal acts that use means or with the assistance of electronic systems." (Aldriano & Priyambodo, 2022: 2172)

The regulation of cyber crime itself begins with the existence of an international instrument, namely the Convention on Cybercrime. The only international instrument that regulates cyber crime is the Convention on Cybercrime which was signed in Budapest (Hungary) in 2001. As of October 2004, this convention had been signed by 32 countries, and ratified or accessed by 8 member countries of the Council of Europe. Each country that signed and ratified agreed to implement the convention in criminal law in each country through legal harmonization. This convention is used as a minimum standard (Standard Minimum Rules) in the preparation of criminal law that regulates computer-related crimes. (Widodo, 2009:83)

This international instrument also serves as a guideline for drafting laws relating to cyber crime, namely Law Number 11 of 2008 concerning Electronic Information and Transactions. Two major contents are regulated in the ITE Law, namely regarding the regulation of electronic transactions and regarding cyber crimes. The substance of the regulation of cyber criminal acts in the ITE Law includes material criminal law, namely the criminalization of actions that fall into the category of cyber criminal acts and includes formal criminal law specifically to enforce cyber criminal law. .(Sitompul, 2012:36)

2. Evidence in the Criminal Justice System in Indonesia

Criminal procedural law aims to find material truth, in contrast to civil procedural law which is quite satisfied with formal truth. Finding material truth is not easy. The evidence available according to law is very relative. (Hamzah, 2008: 249-250)

Evidence is the provisions that contain outlines and guidelines regarding the methods permitted by law to prove the guilt of the accused. Evidence is an effort to provide confidence to the judge in the arguments put forward in a case by the parties in a criminal

case, namely by the public prosecutor and the defendant accused of committing a crime or the legal advisor who accompanies him. (Harahap, 2007: 260)

Evidence in criminal cases is aimed at finding the real truth or at least close to the real truth. Evidence is also a provision that regulates the evidence permitted by law which the judge may use to prove the guilt of the accused. Court trials must not be arbitrary and arbitrarily prove the defendant's guilt. (Harahap, 2007: 260)

There are four types of systems or theories in terms of proof. Indonesia adheres to a negative system of evidence based on law, the sentence is based on double evidence (dubbel en grondslag, said D. Simons), namely on statutory regulations and on the judge's belief, according to the law the judge's belief is based on regulations. law. (Prodjodikoro, 2019: 256) The provisions of the evidentiary system can also be seen in Article 183 of the Criminal Code, hereinafter abbreviated to KUHAP, "Article 183 of the KUHAP states that a judge may not impose a crime on a person, except if at least "With the lack of two valid pieces of evidence, he is convinced that a criminal act has actually occurred and that the defendant is guilty of committing it."

So, in deciding whether a defendant is guilty or not, there must be at least two pieces of evidence, and with this evidence the judge can be confident.

Regarding valid evidence itself, it is regulated in the provisions of Article 184 paragraph 1 of the Criminal Procedure Code:

1) Witness testimony
2) Expert testimony
3) Letter
4) Instructions
5) Statement of the defendant

3. Electronic Evidence in Cyber Crime Cases

Evidence has an important role in the criminal justice process, because this is the stage that most determines whether a person can be proven to be the perpetrator of a crime so that he can be sentenced or not. In addition, cyber crime cases use electronic evidence, which, as the author previously explained, is that electronic evidence is very vulnerable to being changed, manipulated, deleted and so on, making it difficult to prove it.

To carry out this proof, in theory there are several types, but in Indonesia, especially the Criminal Procedure Code, it adheres to a system or theory of proof based on negative law (negatief wettelijk), and this is the proof system used in the criminal justice system in Indonesia to this day.

Evidence has an important role in proof, because as stated above, the defendant's guilt is determined by a minimum of two valid pieces of evidence, and it is with this evidence that the judge can form his belief regarding the defendant's guilt or innocence. This is also in line with what Ni Made Trisna Dewi said in her writing that digital evidence has a very important position in the evidentiary process at trial, this evidence also determines whether the defendant is guilty or not. (Made, et al, 2021:21)

For the use of electronic evidence here the author only looks at the ITE Law, but in other laws provisions for electronic evidence are also regulated. The process of proving cyber crime is no different from conventional criminal acts, but cyber crime mainly uses electronic matters as described in article 5 of the ITE Law. (Lestari, 2018:52)

The regulation of electronic evidence in the ITE Law is regulated in Article 5 and Article 44, which contains the expansion of evidence, namely by legalizing or accepting electronic evidence in evidence in Indonesia. Among them are Electronic Information and/or Electronic Documents and/or printed results.

Proving using electronic evidence is difficult, because it is vulnerable to being changed, manipulated, deleted and so on. In accordance with the provisions of the ITE Law, there must be testing equipment for electronic evidence so that electronic evidence can be declared valid in court as with other evidence, namely meeting formal and material requirements. These requirements are determined based on the type of electronic evidence referred to (in the original). (Sitompul, 2012: 280)

This is in line with what Andrew Christian Banjarnahor said in his writing that technological developments have had legal impacts, including regarding evidence in criminal procedural law. Evidence is said to be valid if it meets the material and formal requirements. (Banjarnahor & Faridah, 2023: 33-47)

Several things about electronic evidence: (Sitompul, 2012: 280-281)

a. Electronic evidence expands the scope of evidence

For example, a letter, the essence of which is a collection of punctuation marks in a particular language that have meaning. This essence is the same as the printout of Information or Electronic Documents, so it is categorized as a letter in Article 187 of the Criminal Procedure Code and can be used as evidence if the results are related to the contents of other evidence.

b. Electronic evidence as another form of evidence

Article 44 of the ITE Law regulates that Electronic Information or Documents are other means of evidence. Information or Electronic Documents in original form is evidence apart from being regulated in the Criminal Procedure Code, considering that Information or Electronic Documents in original form are important because they can contain information that cannot be obtained if printed.

c. Electronic evidence as a source of clues

Article 188 paragraph (2) regulates that the sources of guidance are witness statements, letters and defendant statements. Electronic evidence can be used as a source of guidance, namely printouts of information or electronic documents which are categorized as letters as explained above.

Material requirements are intended to ensure data integrity, availability, security, authenticity and access to information and/or electronic documents in the process of collecting and storing them in the investigation and prosecution process, as well as presenting them at court hearings. (Sitompul, 2012: 282) So scientific discipline is needed in the form of digital forensics. Material requirements are regulated in Article 5 paragraph (3), Article 6, Article 15 to. 16 of the ITE Law.

Electronic evidence can only be said to meet the material requirements if the Electronic Information and/or Electronic Documents use an Electronic System that is appropriate for its use, safe, responsible, the information can be displayed in its entirety, can protect the integrity and authenticity of the data, and is accompanied by procedures. On the other hand, if you do not use an electronic system as explained above, it will not fulfill the material elements and cannot be used as valid electronic evidence.

The formal requirements are regulated in Article 5 paragraph (4) and Article 43 of the ITE Law, namely that it cannot be used as electronic evidence if the evidence is something

that must be realized in the form of a written letter and notarial deed or must be made by an official making the deed, as well as in during searches and seizures must be based on existing procedures. If these conditions are met, the electronic evidence is in accordance with its original form, and can be declared valid and can be used in court. In terms of strength and evidentiary value, its essence is the same as evidence in 184 of the Criminal Procedure Code, namely that it is free and not binding or determining. (Sitompul, 2012: 287)

Digital forensics has a big role in evidence that uses electronic evidence, because with the help of this scientific discipline you can find valid electronic evidence, and from that evidence the judge can base his belief. Digital forensic procedures, namely: .(Sitompul, 2012:291-294))

1) Retrieval, because it is easy to change, it is necessary to secure the original electronic evidence. The method can be based on the initial conditions where electronic evidence was found or the tool/device that stores electronic evidence.
2) Examination and analysis, examination using hardware and software specifically created for digital forensic purposes to examine original and copied evidence. Then analyze, interpret the information that has been extracted and determine information related to criminal acts.
3) Documentation and presentation, every action taken in collecting and examining electronic evidence is documented accurately and thoroughly.

In carrying out this digital procedure, officials are needed who are truly competent in their field, so that they can prepare electronic evidence as appropriate and can be used during the trial.

This is also in line with what I Komang said in his writing, "Demonstrating electronic evidence requires information and technology expertise as well as a computer system testing laboratory to carry out validity as digital evidence. Expert reports are very helpful in solving crimes where electronics are used as evidence because judges can consider expert information when deciding cases." (Sudawirawan, 2023: 187) Techniques for obtaining cyber crime evidence so that it can be used as evidence requires the digital forensics profession. . (Darwis, 2019:36)

The proof process at trial, at the stage determined by the public prosecutor to show evidence, electronic evidence will be displayed according to the characteristics of the digital evidence. Based on Article 181 paragraph (1) of the Criminal Procedure Code, the presiding judge shows evidence and asks whether the defendant is familiar with the evidence which must also be based on Article 45. In paragraph (2) the judge can also show evidence to witnesses, as well as in paragraph (3) if necessary, the presiding judge at the trial reads or shows the letter or minutes to the defendant or witness and asks for information as necessary. (Widodo, 2013: 156)

In this regard, expert witnesses are needed who really understand electronic evidence. Because the presence of experts can also be used to provide confidence in electronic evidence, namely, as stated in the ITE Law, someone who has special expertise in the field of information technology who can be held accountable both academically and practically regarding this knowledge. This can cause problems in practice, because the phrase being academically accountable seems to require that you have an educational background in the field of information technology and electronic transactions and practically have to have a job in that field. However, in general cyberists have the ability to learn self-taught, so that the level of expertise cannot only be determined by a diploma/certificate but also by the recognition of the community. So academically an expert must have his knowledge capacity tested and practically it must be proven by experience of his activities in the ITE field. (Wisnubroto, 2011:228-229)

Proving disclosure in cyber crime cases still has difficulties due to: (Wisnubroto, 2010:136-137)

1) Limited ability of law enforcement officials in handling cases related to high-technology;
2) Limited availability of technological facilities to uncover cases related to high-technology; for example, the limited existence of computer forensic laboratories in Indonesia;
3) The role of expert witnesses in the criminal justice process cannot yet be utilized optimally;
4) Low awareness of victims to report criminal cases that occur on their computer security systems, especially their willingness to act as main witnesses.

This obstacle was also explained by Miftakhur Rokhman: (Rokhman & Liviani, 2020: 420)

> *"Law enforcement against cybercriminals is still hampered by several aspects, namely: law enforcement officers lack the skills or quality to combat cyber crackers, limited tools (media) and the latest equipment owned by the Police. Like a tool that should be available in every Regional Police to speed up detection and prediction of the whereabouts of crackers in action, namely a cyber crime laboratory. However, only the National Police Headquarters and the Police in several large cities have this laboratory, so there are obstacles to delays and high budgets in every cybercrime investigation process in Indonesia, as well as victims who are reluctant to report crimes that have happened to them due to privacy, economic reasons, or because the victim does not trust the expertise and dedication of the police in solving the case."*

Seeing the problems above, the government should pay more attention, this can be done by preparing law enforcement officers who are able to understand cyber crime, improving facilities at existing agencies, and preparing expert witnesses who are competent in their fields who can help uncover cases. cyber crime, so that it can simplify the proof process considering that proof using electronic evidence is not an easy thing to do. Apart from that, judges can impose sentences on people who are truly guilty and give sentences appropriate to their guilt based on evidence. In the end, it can create a good judicial process in efforts to overcome cyber crime.

CONCLUSION

Based on the discussion above, it can be concluded that proof of cyber crime in the Indonesian criminal justice system is by adhering to a system or theory of evidence based on negative law (negatief wettelijk). The defendant's guilt is determined by a minimum of two valid pieces of evidence, and with this evidence the judge can form his or her belief as to whether the defendant is guilty or not. Proof uses electronic evidence because it is vulnerable to being changed, manipulated, deleted, so for the electronic evidence to be valid so that it can be accepted as electronic evidence, it must meet the formal and material requirements regulated in the ITE Law. Digital forensics has a big role in evidence that uses electronic evidence, because with the help of this scientific discipline you can find valid electronic evidence, and from that evidence the judge can base his belief. The proof process at trial, at the stage determined by the public prosecutor to show evidence, electronic evidence will be displayed according to the characteristics of the digital evidence. The existence of expert witnesses is also an important part of proving cyber crime.

The difficulty in proving cyber crime is that it is easy for electronic evidence to be changed, manipulated and deleted, so the author suggests providing officers who are truly

able to understand this field, so they can determine which electronic evidence is valid and which is not, so that it can help in the proof process itself. Apart from that, in terms of facilities, the government must also be able to accommodate facilities related to the evidentiary process, namely a forensic laboratory, so as to facilitate the performance of the authorities in uncovering cybercrime cases.

AUTHORS' DECLARATION

Author contribution	:	The authors made substantial contributions to the conception and design of the study. The authors took responsibility for data analysis, interpretation, and discussion of results. The authors read and approved the final manuscript.
Funding statement	:	None of the authors have received any funding or grants from any institution or funding body for the research.
Availability of data and materials	:	All data are available from the authors.
Conflict of interest	:	The authors declare no conflict of interest.
Additional information	:	No additional information is available for this paper

REFERENCES

Books

Arief, Barda Nawawi. *Tindak Pidana Mayantara: Perkembangan Kajian cyber crime di Indonesia*. Jakarta: PT RajaGrafindo Persada, 2007.

Djaja, Ermansjah. *Penyelesaian Sengketa Hukum Teknologi Informasi dan Transaksi Elektrik*. Yogyakarta: Pustaka Timur, 2010.

Hamzah, Andi. Hukum Acara Pidana Indonesia. Jakarta: Sinar Grafika, 2008.

Harahap, M. Yahya. *Pembahasan Pemasalahan dan Penerapan KUHAP Penyidikan dan Penuntutan*. Jakarta: Sinar Grafika, 2007.

Rasjidi, Lili & Ira Thania Rasjidi. *Pengantar Filsafat Hukum*. Bandung: CV. Mandar Maju, 2010.

Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2012.

Wahid, Abdul dan Mohammad Labib. *Kejahatan Mayantara (Cyber Crime)*. Bandung: PT Refika Aditama, 2010.

Widodo. *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta: Aswaja Pressindo, 2013.

Widodo. *Sistem Pemidanaan dalam Cyber Crime*. Yogyakarta: Laksbang Mediatama, 2009.

Wisnubroto, Al. *Konsep Hukukm Pidana Telematika*. Yogyakarta: Universitas Atma Jaya Yogyakarta, 2011.

Wisnubroto, Al. *Strategi Penanggulangan Kejahatan Telematika*. Yogyakarta: Universitas Atma Jaya Yogyakarta, 2010.

Journals

Agustina, Shinta. et. al. "Harmonisasi Hukum Pengaturan Cyber Crime dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik", *Jurnal Mahkamah*, Edisi No. 1 Vol. 2, (2010).

Aldriano, Muhammad Anthony. and Mas Agus Priyambodo. "Cyber Crime Dalam Sudut Pandang Hukum Pidana," Jurnal Kewarganegaraan, Vol. 6, No. 1 (2022), https://doi.org/10.31316/jk.v6i1.2947

Banjarnahor, Andrew Christian. and Hana Faridah. "Tinjauan Yuridis Dalam Proses Pembuktian Cyber Pornography Yang Dilakukan Melalui Media Sosial Berdasarkan Hukum Positif Indonesia," Jurnal Analisis Hukum 6, no. 1 (April 25, 2023): 33–47, https://doi.org/10.38043/jah.v6i1.3998.

Darwis, Nurlely. "Kriminology Pada Bidang Kebijakan 'Cyber Securty,'" Jurnal Ilmiah Hukum Dirgantara, Vol 9 No. 2, Maret (2019).

Dewi, Ni Made Trisna. and Reido Lardiza Fahrial. "Suatu Kajian Yuridis Terhadap Penggunaan Alat Bukti Elektronik Dalam Kejahatan Cyber Dalam Sistem Penegakan Hukum," Jurnal Hukum Saraswati, Vol 3 No 2, (2021), https://doi.org/10.36733/jhshs.v2i2.

Handoko, Cahyo. "Kedudukan Alat Bukti Digital Dalam Pembuktian Cyber Crime Di Pengadilan," Jurnal Jurisprudence 6, no. 1 (March 2016).

Lestari, Anis Dewi., et al., "Cakupan Alat Bukti Sebagai Upaya Pemberantasan Kejahatan Siber (Cyber Crime)" Jurnal Al-Ahkam Jurnal Ilmu Syari'ah dan Hukum, Vol. 3 No 1, (2018): 201

Rokhman, Miftakhur. and Habibi-Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia"Jurnal Al-Qanun, Vol 23, no. 2, Desember (2020).

Sudawirawan, Komang et al., "Kekuatan Alat Bukti Dalam Pembuktian Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime)" Jurnal Konstruksi Hukum, Vol 4, no. 2 (2023): 184–89, https://doi.org/10.55637/jkh.4.2.6798.184-189.

Sugiarto, Fredy. and Datir Siregar. "Pembuktian Hukum Dalam Kejahatan Dunia Maya Berdasarkan Hukum Pidana," Jurnal Ilmiah Publika 10, no. 1 (January 2022).

Regulations

Undang-Undang U No. 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektonik