Asy Syar'iyyah: Jurnal Ilmu Syari'ah dan Perbankan Islam – ISSN 2089-7227 (p) 2598-8522 (e)
Vol. 9, No. 2, Desember 2024, pp. 191 - 207

THE EVIDENTIARY POWER OF ELECTRONIC DOCUMENTS AS AN EXTENSION OF LEGAL EVIDENCE ACCORDING TO ELECTRONIC INFORMATION AND TRANSACTIONS LAW (UU ITE)

Sonia Ramadani[1], Reski Anwar[2*], Nagia Duwi Safitri[3]
[1 2 3] IAIN Syaikh Abdurrahman Siddik Bangka Belitung

*Corresponding author: reskibelitong@iainsasbabel.ac.id

Abstract

The development of information technology has changed the method of proof in criminal law, especially regarding electronic evidence. In the Indonesian criminal justice system, electronic evidence is now recognized as a type of valid evidence, as regulated by Law no. 11 of 2008 concerning Electronic Information and Transactions which has been amended by Law no. 19 of 2016. However, the use of electronic evidence in criminal cases still experiences various difficulties, including in terms of validity, authenticity and effectiveness of evidence before a judge. The aim of this research is to legally analyze the validity of electronic evidence in criminal cases, including the legal basis underlying it, its position in the evidence system, and the challenges faced in practice in court. The methodology used is a normative approach by examining relevant regulations, court decisions and legal theory. Research findings show that electronic evidence has legal force equivalent to other conventional evidence, as described in Article 184 of the Criminal Procedure Code. However, its validity is greatly influenced by the validity of the collection process and the authentication carried out on the electronic document. In addition, there are still differences in understanding regarding its application between law enforcement officials and the courts, which can have an impact on the effectiveness of electronic evidence in proving criminal acts. Therefore, efforts are needed to harmonize regulations and increase the knowledge of law enforcement officers regarding digital technology so that electronic evidence can be utilized optimally in the criminal justice process.

Keywords: *Electronic Evidence, Evidence, Criminal Cases, Criminal Procedure Law, ITE Law*

Abstrak

Perkembangan teknologi informasi telah mengubah cara pembuktian dalam hukum pidana, terutama mengenai bukti elektronik. Di dalam sistem peradilan pidana Indonesia, bukti elektronik kini diakui sebagai salah satu jenis bukti yang sah, sebagaimana diatur oleh Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-undang No. 19 Tahun 2016. Namun, penggunaan bukti elektronik dalam kasus pidana masih mengalami berbagai kesulitan, termasuk dalam hal keabsahan, autentisitas, dan efektivitas pembuktian di depan hakim. Tujuan dari penelitian ini adalah untuk menganalisis secara hukum mengenai validitas bukti elektronik dalam kasus pidana, termasuk landasan hukum yang mendasarinya, posisinya dalam sistem pembuktian, dan tantangan yang dihadapi dalam praktik di pengadilan. Metodologi yang dipakai adalah pendekatan normatif dengan menelaah regulasi, putusan pengadilan, dan teori hukum yang relevan. Temuan penelitian menunjukkan bahwa bukti elektronik mempunyai kekuatan hukum yang setara dengan bukti konvensional lainnya, seperti yang diuraikan dalam Pasal 184 KUHAP. Namun, keabsahannya sangat dipengaruhi oleh sahnya proses pengumpulannya serta autentikasi yang dilakukan terhadap dokumen elektronik tersebut. Di samping itu, masih terdapat perbedaan pemahaman dalam penerapannya antara aparat penegak hukum dan pengadilan, yang bisa berdampak pada efektivitas bukti elektronik dalam membuktikan tindakan pidana. Oleh karena itu, diperlukan usaha untuk menyelaraskan regulasi dan meningkatkan pengetahuan aparat penegak hukum mengenai teknologi digital agar bukti elektronik dapat dimanfaatkan secara maksimal dalam proses peradilan pidana.

***Kata Kunci**: Alat Bukti Elektronik, Pembuktian, Perkara Pidana, Hukum Acara Pidana, UU ITE*

A. Introduction

The existence of technology, now every individual has a supporting tool in completing his or her tasks, and the relationship between humans and technology is getting closer and more interdependent. Technology has come as a significant innovation, which is very beneficial for human work thanks to the advancement of science and technology. One of the results is information technology, which continues to facilitate interaction between people from

various communities.[1]

One of the advances in information and communication technology is technology known as cyberspace or the internet. As a conduit for information and communication electronically, the internet has been widely used in a variety of activities, including browsing, searching for information and news, exchanging messages via email, communicating on social media platforms, as well as for trading activities.[2]

However, although technology is one of the innovations that provides convenience, on the other hand, technology has also created new problems and serves as a tool that triggers illegal actions. Referring to J.E. Sahetapy's view, he stated that there is a close relationship between crime and culture. In this context, it means that the more advanced a culture is, the more crime patterns will develop.

One type of crime that arises due to the widespread use of technology is cybercrime. This term refers to criminal acts that are generally carried out through a computer network. Cybercrime activities are not as easy as they seem, especially in the context of law enforcement, from the existing rules to which courts have the authority to handle the case. Cybercrime is regulated in the Criminal Code (KUHP) as well as in Regulation No. 11 of 2008 concerning Digital Data and Transactions and Regulation No. 19 of 2016 which has been updated by Regulation No. 11 of 2008 concerning Digital Data and Transactions (hereinafter summarized as the ITE Law). The ITE Law serves as an initial legal basis to regulate digital transaction activities in Indonesia, as well as provide legal updates with the intention of protecting the interests of the public in

[1] Santa Maria Hutapea dan I Wayan Bela Siki Layang, "*Kajian Terhadap Kekuatan Hukum Pembuktian Alat Bukti Elektronik dalam Penyelesaian Perkara Pidana," Kertha Desa: Journal Ilmu Hukum, Vol* 12, no. 3 (2023). hlm 2.

[2] Iskandar, Taufik; Mauluddin; Rudi; Marsudi Utoyo. "*Kekuatan Pembuktian Alat Bukti Elektronik Berdasarkan Undang-undang Nomor 19 Tahun 2016 Tentang Informasi Transaksi Elektronik (ITE)*." Lex Stricta: Jurnal Ilmu Hukum, vol. 2, no. 1 (2023). Hlm. yang benar 2 (hlm tercetak 24).

obtaining legal certainty when conducting transactions through digital media.[3]

Various types of cybercrimes that appear in society include: falsification of information, fraud, data theft, provocation, pornography, online gambling, copyright infringement, and others. On the other hand, the relevance of digital forensics in providing evidence for cases that occur in cyberspace that have unique characteristics can be recognized. This is due to the inherent nature of computer technology that allows criminals to hide from their actions. Therefore, one strategy to uncover cybercrime involves analyzing the system with the role of an investigator, not just an ordinary user. Cybercrime is a challenge that must be faced through this method.[4] The proof system for this cybercrime, electronic documents serve as the main evidence that can be directly submitted in court. Given that technology-related crimes inevitably leave a digital footprint, electronic documents and their prints become invaluable as prime evidence and formidable evidence.[5]

Based on the ITE Law, Article 1 number 3 of Information Technology is a technique for collecting, preparing, storing, processing, announcing, analyzing, and/or disseminating information. In the legal framework related to information technology, the term information technology refers to the use of information technology and communication based on computers.

Article 1 number 14 of the ITE Law defines "Computer" as a tool for processing electronic, magnetic, optical, or system data that performs logic, arithmetic, and storage functions.[6] The definition of a computer in this context includes not only hardware such as PCs, laptops, and servers, but also a broader range of systems, including computer networks and electronic systems that support various data processing functions. In the world of law and

[3] Hamdi, Syaibatul; Suhaimi; Mujibussalim. "*Bukti Elektronik dalam Sistem Pembuktian Pidana*." Jurnal Ilmu Hukum, vol. 7, no. 4 (2013). hlm. yang benar 2 (hlm tercetak 42).

[4] Tria, A. *Cyber Crime Dalam Perspektif Hukum Pidana*. Surakarta: UMS. (2010).

[5] Logi dan Informasi (*Cyber Crime*)." Kertha Wicara: Journal Ilmu Hukum, vol. 8, no. 6 (2019). Hlm 10.

[6] Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

cybercrime, this definition also includes information technology infrastructure, such as cloud computing, data centers, and network-based systems that allow the electronic exchange of information.

Computers in the ITE Law are also closely related to electronic systems, which are defined as one or more electronic devices that work together to process information, such as those found in banking systems, e-commerce, and various digital applications that manage user data.

However, because Cyber Wrongdoing uses a medium, namely Cyber Space , to commit crimes and uses information and telecommunication technology as a tool for victims, based on the UN General Assembly Resolution (Determination of the General Assembly of States - Joined States) No. A/RES/55/63 dated January 12, 2001 concerning Response to Information Technology Processing (Combating the Crime of Prior Data Misuse), which is the relevant term for The follow-up of cyber breaches is related to information technology and telecommunications.[7]

With the rapid development of the use of the internet and information technology as a tool for online transactions and communication, our efficiency and speed have increased. However, there are also serious impacts that arise due to the increase in cybercrime. Data security and digital transactions and cybercrime have always been in the fight regarding various issues related to information and digital transactions.[8]

Thus, the understanding of criminal law in the information technology sector here includes criminal rules that are relevant to the actions of individuals who use computers and computer networks in cyberspace. This includes activities such as collecting, preparing, storing, processing, announcing,

[7] Makalah di sampaikan di Seminar "Penegak Hukum Tindak Pidana Mayantara", Kepolisian RI Polda Jateng Semarang.

[8] Mantik, Vogen L. M. T.; Watulingas, Ruddy R.; Muaja, Harly Stanly. " *Tinjauan Yuridis tentang Kedudukan Alat Bukti Digital dalam Tindak Pidana Kejahatan Mayantara (Cyber Crime)*." Lex Privatum, Vol. 10, No. 2 (2022). hlm. 1.

analyzing, and sharing information in various forms, including data, sound, and images.[9]

B. Research Findings and Discussion

This section will describe about findings of the research, then complete with discussion. It must consist elaborated between 1500 – 4500 words (4 – 8 pages). Research Findings is the explanation about the result of the research based on analysis of the data whether it is in qualitative or quantitative approaches.

In the Indonesian dictionary, the term proof is defined as a process or method used to show whether the defendant is right or wrong during the trial. M. Yahya Harahap stated that from a legal perspective, evidence is related to rules that provide limits and directions regarding methods that can be used in accordance with the law to prove the error addressed to the defendant. Evidence also includes regulations on evidence allowed by law and establishes the types of evidence that can be used by the judge to ascertain the guilt of the defendant. The court is not allowed to act arbitrarily in proving the guilt faced against the defendant.[10]

The law regarding evidence is part of the criminal law procedure that regulates the various types of evidence that are legally recognized, the methods applied in the evidentiary process, the provisions and steps in presenting the evidence, and the authority of the judge to accept, reject, and evaluate an evidentiary process.[11]

[9] Widodo, *Hukum Pidana Di Bidang Teknologi Informasi Cybercrime Law*, Aswaja Pressindo, Yogyakarta, 2013.

[10] Ramiyanto. (2017). "*Bukti Elektronik Sebagai Alat Bukti yang Sah dalam Hukum Acara Pidana*." Jurnal Hukum dan Peradilan, Vol. 6, hlm. yang benar 4 (hlm tercetak 446).

[11] Hanafi dan Muhammad Syahrial Fitri, *Implikasi Yuridis Kedudukan Alat Bukti Elektronik dalam Perkara Pidana Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016*, *Al'Adl*, Vol. XII No. 1, (Januari 2020), hlm yang benar 2 (hlm tercetak 102).

Proof acts as a provision that provides direction related to legally permissible techniques to prove the fault assigned to the defendant. In addition, proof also refers to regulations that regulate the category of evidence that is legal according to the law and can be used by judges to prove the alleged wrongdoing.

The following is an interpretation of the meaning of proving which includes several understandings, as follows:

1. In the logical aspect, proving means providing guarantees that are fully applicable to each individual and do not allow for any other form of proof;
2. In a more general sense, proof provides certainty, but not absolute certainty, but rather relative or comparative certainty, with the following categories of properties:
    a. Certainty that is intuitive and based only on feelings, which can be called intimate conviction; and
    b. Certainty based on rational analysis, known as conviction raisonnee.
3. Evidence in the realm of legal evidence, which is evidence that gives confidence to the judge about the facts that actually happened.[12]

Criminal law is one of the tools used by the state to carry out its responsibilities in protecting the right of every individual to feel safe, especially from the threat of crime. When compared to other types of law, criminal law has a unique feature that lies in the existence of very clear sanctions in the form of suffering. Therefore, the criminal justice system needs to be reviewed, restructured, harmonized, and updated carefully and appropriately, through a thorough understanding and thinking so that, on the one hand, it is effective in dealing with the development of crime but on the other hand does not threaten human rights, honor, and dignity.[13]

[12] Subarzah, Nasya Ardhani; Wijaya, Firman; Ambarita, Folman Paulus. "*Kekuatan Pembuktian Alat Bukti Elektronik dalam Tindak Pidana Pencucian Uang pada Kasus Putusan Nomor 844/Pid.Sus/2019/PN.Ptk.*"Jurnal Krisna Law, Vol. 5, No. 1 (2023). hlm. yang benar 4-5 (hlm tercetak 84-85).

[13] Aloysius Wisnubroto, *Konsep Hukum Pidana Telematika*, Universitas Atma Jaya, Yogyakarta, 2011, hlm. 1.

In general, the main purpose of the law is to build an organized coexistence in a way that can expand opportunities for individuals to pursue their aspirations. In essence, the law aims to safeguard the interests of the community in the community, ensure the implementation of human rights, and realize justice in social interactions within the community.[14]

Overall, the role of law is to create a cohabitation that is structured in such a way that these conditions can support the growth of each individual in achieving life goals. Basically, the role of law is to protect the collective interests in the community, protect individual rights, and realize justice in social interactions in society.[15]. Regarding the role of law, Lawrence M. Friedman stated that the role of law includes being a tool to supervise or regulate society, resolve conflicts, and build social structures and innovation. On the other hand, Soerjono Soekanto argued that the role of law is to provide direction to the community on how to behave and behave, maintain social unity, and provide guidelines for implementing social control.[16] Based on article 1 of the Criminal Code, it can be concluded that there is a principle of legality in criminal law in Indonesia.

The principle of legality indicates that there must be legal provisions that are officially established before actions can be accounted for. After that, actions by individuals who are proven to meet the criteria of criminal conduct may be subject to sanctions. In other words, this principle emphasizes that legal regulations cannot be applied retroactively, providing a guarantee of legal certainty.

The ITE Law also adheres to the principle of legality (as a fundamental principle in criminal law), which is as seen in Article 54 paragraph (1) that this

[14] Wicaksono, Bayu; Yulianto, Irwan; Hadiyanto, Ide Prima. "*Tinjauan Yuridis Kekuatan Alat Bukti Elektronik dalam Pembuktian Perkara Pidana Menurut Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana*." Jurnal Ilmiah AKSES, Vol. 2, No. 1 (2024). hlm. yang benar 8 (hlm tercetak 26).

[15] The Huijbers, *Philosophy of Law in the Trajectory of History,* Kanisius, Jakarta, 1988, p. 285.

[16]Soerjono Soekanto, *Principles of Legal Sociology*, Raja Grafindo Persada, Jakarta, 2003, p. 9.

Law comes into force on the date of promulgation. This means that the legal provisions contained in the ITE Law will be implemented after its implementation comes into effect on April 21, 2008.[17]

This principle of legality has a very important role in determining whether an action can be considered a criminal act or not, especially in the context of technology-based crime, whether it is related to legal or ethical issues. Therefore, the existence of the principle of legality as the main basis for assessing actions that are classified as criminal acts is very necessary. Article 184 of the Criminal Code paragraph 1 regulates the legal evidence, namely:

1. Witness statements.
2. Akli's caption.
3. Letter.
4. Instructions.
5. Defendant's statement[18]

In order for Information and Electronic Documents to be used as legal evidence, the ITE Law stipulates that there are formal and material requirements that must be met. Formal requirements are regulated in Article 5 paragraph (4) of the ITE Law, namely that information or electronic documents will be valid and have legal force as long as they are not documents or letters that according to laws and regulations must be in written form. Meanwhile, material requirements are regulated in Article 6, Article 15, and Article 16 of the ITE Law, which basically stipulate that information and electronic documents must be guaranteed to be authentic, complete, and available. These three elements are very important so that information or electronic documents can have legal force.[19]

[17] Pribadi, Insan. "*Legalitas Alat Bukti Elektronik dalam Sistem Peradilan Pidana*." Lex Renaissance, vol. 3, no. 1 (2019). Hlm. yang benar 8 (hlm tercetak 116).

[18] Rusyadi. "*Kekuatan Alat Bukti dalam Persidangan Perkara Pidana*." Jurnal Hukum Prioris, Vol. 1, No. 2. 2016. Hlm. yang benar 3 (hlm tercetak 130).

[19] Manope, Indra Janli. "Kekuatan Alat Bukti Surat Elektronik dalam Pemeriksaan Perkara Pidana." Lex Crimen, vol. 6, no. 2 (2017). Hlm. yang benar 5 (hlm tercetak 111).

Electronic Document is any Electronic Information created, transmitted, transmitted, received, or stored in analogue, digital, electromagnetic, optical, or similar form, which may be viewed, displayed, and/or heard through a Computer or Electronic System, including but not limited to writing, sound, image, map, design, photograph or the like, letters, signs, numbers, Access Codes, symbols or perforations that have any meaning or significance or are understandable by the person who able to understand it.[20]

The existence of electronic evidence as legal evidence is further strengthened by the issuance of the ITE Law article 5 paragraph (1) and paragraph (2) of the ITE Law which[21] reads:

1. Electronic Information and/or Electronic Documents and/or their printed results are valid legal evidence
2. Electronic Information and/or Electronic Documents and/or their printed results as intended in paragraph (1) are an extension of valid evidence in accordance with the applicable procedural law in Indonesia.

Article 5 paragraph (3) of the ITE Law, namely Electronic Information and/or Electronic Documents is declared valid if using the Electronic System in accordance with the provisions stipulated in this Law. Furthermore, the Electronic System is regulated in Articles 15 to 16 of the ITE Law and from these two articles, more detailed requirements can be obtained, namely that the Electronic System:

1. Reliable, secure, and responsible.
2. Can display the Information or Electronic Document in its entirety.
3. Can protect the availability, completeness, authenticity, confidentiality, and accessibility of Electronic Information.
4. Equipped with procedures or instructions and can operate according to the procedures or instructions that have been set.

[20] Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[21] Yusandy, Trio. "*The Position and Evidentiary Power of Electronic Evidence in Civil Procedure Law in Indonesia*." Journal of Serambi Akademica, Vol. 10, No. 1 (2022). True p. 4 (printed p. 648).

Meanwhile, the formal requirements for electronic evidence are regulated in Article 5 paragraph (4) and Article 43 of the ITE Law, namely:

1. Such Information or Electronic Document shall not:
   a. A letter that according to the Law must be made in written form; and
   b. The letter and its documents according to the Law must be made in the form of a notarial deed or a deed made by the deed making official.
2. The search or seizure of the Electronic System must be carried out with the permission of the chairman of the local district court.
3. Seizure or confiscation and maintaining the preservation of the interests of public services with the 16 ITE Law and from these two articles, a more detailed discussion can be obtained, namely that the Electronic System.

In the Indonesian legal system, electronic evidence is recognized as legitimate evidence, especially through the regulation in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE). Although the Criminal Procedure Code (KUHAP) does not explicitly mention electronic evidence, the ITE Law provides a legal basis for the acceptance of electronic evidence in judicial proceedings.

Types of Recognized Electronic Evidence:

1. Electronic Information: Data or information created, sent, received, or stored electronically, such as email, text message, or other digital data.
2. Electronic Documents: Any document created or stored in electronic format, including digitally stored text, image, audio, or video documents.
3. Printed Results of Information or Electronic Documents: Physical printouts of information or electronic documents that can be used as evidence of letters in judicial proceedings.

The Ministry of Communication and Information Technology (Kemenkominfo) classifies several types of electronic evidence, which the classification submitted to the Scientific Working Group on Digital Evidence in 1999. The types of electronic evidence are:

1. E-mail, E-mail address (e-mail)
2. File Word Processor/Spreedsheet

3. Software Source Code
4. Image files (jpegs, tips, etc.)
5. Web Browser Bookmarks, Cookies
6. Calendar, to-do list.

The Association of Chief Police (ACPO), in its Good Practice, Guide for Computer Based Electronic Evidence, categorizes the types of electronic evidence, namely:

1. Computers,
2. Network,
3. Video & Closedcircuit Television (CCTV)
4. Mobile phone[22]

The criminal justice system has two main goals: to protect the public and to enforce the law. In addition, the system has several important functions, including:[23]

1. Preventing crime.
2. Taking action against perpetrators of criminal acts by providing understanding to them when prevention is not effective.
3. Conduct a review of the legality of prevention and enforcement measures.
4. Issuing a court decision to determine whether or not a person is detained.
5. Provide an appropriate disposition for a person who is found guilty.
6. Administer correctional institutions by the tools of the state approved by the community against their behavior that violates criminal law.

It is stated that one of the main criteria for electronic evidence to be accepted in court is that information or documents in electronic form must be guaranteed its availability, completeness, and authenticity. In an electronic transaction, there will be a large amount of information recorded or stored on various devices and devices. If electronic information and documents are not

[22] Sari, Indah. "*Kekuatan Keabsahan Alat Bukti Elektronik dalam Penyelesaian Perkara Pidana di Indonesia.*" JSI (Jurnal Sistem Informasi) Universitas Suryadarma, vol. 11, no. 2, (2020). Hlm. yang benar 4-5 (hlm tercetak 106-107).

[23] Tollib Effendi, *Sistem Peradilan Pidana*, Buku Seru, Jakarta, 2013, hlm. 13.

properly managed, they have the potential to change, become corrupted, or even lost.

The Association of Chief Police Officers (ACPO) provides four principles in handling electronic evidence, namely:[24]

1. All handling of electronic evidence (i.e. data obtained from computers or storage media, or other electronic tools and devices) by law enforcement officials must not result in alteration or damage to the data in order to be admissible in court.
2. In circumstances where a person must access the original data contained in a computer or storage media, the person in question must have the competence to do so, and must be able to provide an explanation of the relevance of his actions to the data and the consequences of his actions.
3. That there should be clear procedures and processes in place to collect and analyze electronic evidence. The procedure in question contains the handling of electronic evidence starting from the discovery of evidence containing electronic evidence, packaging of evidence, examination, analysis and reporting.
4. There must be a party or official responsible for ensuring the implementation of activities in accordance with laws and regulations and the entire process and procedures in question.

Another thing that needs to be considered in the collection of evidence that stores electronic evidence is that there are so many types of tools and media that store information. Considering that there are so many types of information storage media and technology, the handling also has its own characteristics. In general, digital forensics is divided into:[25]

1. Computer forensics, which is forensics carried out on computers, laptops, or hard disks and similar storage media.
2. Mobile forensics, which is forensic work carried out on mobile phones.
3. Network forensics, which is forensic work carried out on computer networks.
4. Forensic audio, which is forensic work done on sound.
5. Forensic image, which is forensic work carried out on images.
6. Forensic video, which is forensic work carried out on video and CCTV.

[24] Good Practice Guiede for Computer-Based Electronic Evidence, hlm. 4.

[25] Muhammad Nuh Al-Azhar, *Digital Forensic Panduan Praktis Investigasi Komputer*, hlm. 25-26.

In terms of evaluation and investigation, the analysis of original electronic evidence is usually carried out using hardware and software specifically designed for digital forensic purposes. This process includes extraction, which is taking all information from the data storage medium, including data that has been previously deleted. The examiners also make use of the write blocker tool, which serves to protect the original data from rewriting.

Checking copies of the original electronic evidence also allows for the creation of additional copies as materials for work. All of these processes must be documented appropriately and thoroughly. In addition to the actions when conducting digital forensics, any actions related to the process, such as the handover of computers from the goods pick-up officer at the scene to the forensic examiner, must also be recorded. The report of the results of the inspection should include the steps and processes undertaken, as well as the equipment and devices used. In addition, the report is also required to include information about the total data obtained and data related to the crime being investigated.

In practice, investigations are carried out by police officers who are allowed by law to carry out investigations in accordance with the expertise possessed by the investigator. If the case handled by the investigator is related to a crime involving information technology, then the investigation and investigation stage requires the use of information technology knowledge to explain a case. One of the crucial ways for the law enforcement process is to apply digital forensic science.

C. Conclusion

The regulation regarding the legality of electronic evidence has been clearly stated in Article 5, Article 6, as well as through affirmation in Law Number 11 of 2008 which has been amended by Law Number 19 of 2016

concerning Electronic Information and Transactions. This electronic evidence is indispensable in the Criminal Justice System to provide a decision for defendants faced in cases related to technological crimes, by making electronic evidence a valid form of evidence in the criminal justice process. In addition, the provisions regarding electronic evidence in the ITE Law mentioned above are a development of the type of evidence that has been regulated in Article 184 of the Criminal Code.

This electronic evidence has an important role in the criminal case justice system to determine decisions for defendants faced in technology-based crime cases by making electronic evidence as official evidence in the court process. In addition, the regulation of electronic evidence in the ITE law mentioned earlier, as well as the function of digital forensics in the processing of evidence, are strategic steps needed so that electronic evidence can be used as evidence in court.

Digital forensics is a branch of forensic science that includes the search and investigation of digital information contained on electronic devices for the purpose of legal evidence. In conducting the investigation and interrogation process, it is important to identify the type of crime based on the technology used, as this has an impact on the investigation process carried out through various digital forensic sciences.

REFERENCES

Effendi, Tollib. (2013), *Criminal Justice System*, Buku Seru, Jakarta.

Huijbers, The. (1988). *Philosophy of Law in the Trajectory of History*, Kanisius, Jakarta.

Good Practice Guiede for Computer-Based Electronic Evidence.

Nuh Al-Azhar, Muhammad Nuh Al-Azhar, Digital Forensic Practical Guide to Computer Investigation.

Sitompul, Joshua. (2012). *Cyberspace, Cybercrimes, Cyberlaw: A Review of Criminal Law Aspects,* Jakarta: Tatanusa.

Soekanto, Soerjono. (2003). *Principles of Legal Sociology*, Raja Grafindo Persada, Jakarta.

Tria, A. (2010). *Cyber Crime in the Perspective of Criminal Law,* Surakarta: UMS.

Huijbers, The. (1988). *Philosophy of Law in the Trajectory of History*, Kanisius, Jakarta.

Widodo. (2013). *Criminal Law in the Field of Information Technology Cybercrime Law*, Aswaja Pressindo, Yogyakarta.

Wisnubroto, Aloysius. (2011). *Concept of Telematics Criminal Law*, Atma Jaya University, Yogyakarta.

Seminar Papers

The paper was presented at the Mayantara Criminal Law Enforcement Seminar, Indonesian Police Central Java Police.

Laws and Regulations

Law Number 11 of 2008 concerning Information and Transactions.

Journal

Janli Manope, Indra. (2017). "Kekuatan Alat Bukti Surat Elektronik dalam Pemeriksaan Perkara Pidana." Lex Crimen, vol. 6, no. 2.

Isima, Nurlaila. (2024). "Kedudukan Alat Bukti Elektronik dalam Pembuktian Perkara Pidana." Gorontalo Law Review, vol. 5, no. 1.

Gusti Ayu Shabaina Jayantari, I; Sugama, I Dewa Gede Dana. (,2019). "Kekuatan Alat Bukti Dokumen Elektronik dalam Tindak Pidana Berbasis Teknologi dan Informasi (Cyber Crime)." Kertha Wicara: Journal Ilmu Hukum, vol. 8, no. 6.

Pribadi, Insan. (2019). "Legalitas Alat Bukti Elektronik dalam Sistem Peradilan Pidana." Lex Renaissance, vol. 3, no. 1.

Sari, Indah. (2020). "Kekuatan Keabsahan Alat Bukti Elektronik dalam Penyelesaian Perkara Pidana di Indonesia." JSI (Jurnal Sistem Informasi) Universitas Suryadarma, vol. 11, no. 2

Iskandar, Taufik; Mauluddin; Rudi; Marsudi Utoyo. (2023). "Kekuatan Pembuktian Alat Bukti Elektronik Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Transaksi Elektronik (ITE)." Lex Stricta: Jurnal Ilmu Hukum, vol. 2, no. 1.

Hamdi, Syaibatul; Suhaimi; Mujibussalim. (2013). "Bukti Elektronik dalam Sistem Pembuktian Pidana." Jurnal Ilmu Hukum, vol. 7, no. 4.

Rusyadi. (2016). "Kekuatan Alat Bukti dalam Persidangan Perkara Pidana." Jurnal Hukum Prioris, Vol. 1, No. 2.

Yusandy, Trio. (2022). "Kedudukan dan Kekuatan Pembuktian Alat Bukti Elektronik dalam Hukum Acara Perdata di Indonesia." Jurnal Serambi Akademica, Vol. 10, No. 1.

Mantik, Vogen L. M. T.; Watulingas, Ruddy R.; Muaja, Harly Stanly. (2022). "Tinjauan Yuridis tentang Kedudukan Alat Bukti Digital dalam Tindak Pidana Kejahatan Mayantara (Cyber Crime)." Lex Privatum, Vol. 10, No. 2.

Ardhani Subarzah, Nasya; Wijaya, Firman; Ambarita, Folman Paulus. (2023). "Kekuatan Pembuktian Alat Bukti Elektronik dalam Tindak Pidana Pencucian Uang pada Kasus Putusan Nomor 844/Pid.Sus/2019/PN.Ptk." Jurnal Krisna Law, Vol. 5, No. 1.

Ramiyanto. (2017). "Bukti Elektronik Sebagai Alat Bukti yang Sah dalam Hukum Acara Pidana." Jurnal Hukum dan Peradilan, Vol. 6.

Wicaksono, Bayu; Yulianto, Irwan; Hadiyanto, Ide Prima. (2024). "Tinjauan Yuridis Kekuatan Alat Bukti Elektronik dalam Pembuktian Perkara Pidana Menurut Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana." Jurnal Ilmiah AKSES, Vol. 2, No. 1.

Hanafi dan Muhammad Syahrial Fitri. (2020). *Implikasi Yuridis Kedudukan Alat Bukti Elektronik dalam Perkara Pidana Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016*. *Al'Adl*, Vol. XII No. 1

Maria Hutapea, Santa. (2024). "Kajian Terhadap Kekuatan Hukum Pembuktian Alat Bukti Elektronik dalam Penyelesaian Perkara Pidana." *Jurnal Kertha Desa* 12, no. 5.