Jurnal Daulat Hukum
Volume 7 No. 4, Desember 2024
ISSN: 2614-560X
SINTA 3 Decree No. 0547/ES/DT.05.00/2024
Dated May 15, 2024

The Validity of Electronic Evidence and Its Relation to Personal Data Protection

Karina Hasiyanni Manurung[1)] & Beniharmoni Harefa[2)]
[1)] Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia, E-mail: 2110611199@mahasiswa.upnvj.ac.id
[2)] Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia, E-mail: beniharefa@upnvj.ac.id

Abstract. *An examination of electronic evidence within the context of Indonesian criminal law focuses on the evolving role of electronic evidence in criminal proceedings, highlighting the challenges arising from the absence of clear regulation in the Indonesian Criminal Procedure Code (KUHAP) and the necessity of balancing this with privacy rights under the Personal Data Protection Law (UU PDP). Electronic evidence, such as digital data and electronic documents, is increasingly recognized under the applicable laws in Indonesia, yet its practical application remains complex within the criminal justice system. This research employs a normative legal methodology, analyzing relevant legal provisions and their interplay, particularly concerning the validity of electronic evidence and data privacy. Both statutory and conceptual approaches are utilized, reviewing primary legal materials such as KUHAP, UU PDP, and related regulations. The study also examines key legal principles, including compliance, transparency, and proportionality, in the context of handling electronic evidence. Secondary data is gathered through a comprehensive literature review, including legal texts, academic books, and journals. The findings indicate significant gaps in the current legal framework, particularly regarding the procedural norms for evidence collection and the tension between privacy rights and criminal justice needs. The research concludes with recommendations for legal reforms aimed at integrating electronic evidence more effectively into KUHAP, ensuring greater consistency, safeguarding privacy, and promoting procedural fairness in criminal proceedings.*

Keywords: *Criminal; Electronic; Information; Privacy; Transactions.*

1. Introduction

The growth of digital technology in recent decades has transformed many aspects of daily life such as making information easier to access, increasing efficiency, and changing the way people interact and work.[1] However, these benefits also come with data challenges, especially given

[1] Fauzi, A. A. (2023). *Pemanfaatan Teknologi Informasi di Berbagai Sektor pada Masa Society 5.0*. PT. Sonpedia Penerbit Indonesia, p. 57.

the increasing incidents of data breaches and misuse of personal information globally.[2] These incidents have certainly triggered countries to strengthen personal data protection regulations. In the midst of rapid technological development, the issue of personal data protection has become very important and requires serious attention from all stakeholders.[3]

Article 184 of the Criminal Procedure Code (hereinafter referred to as KUHAP) recognizes five types of evidence, namely witness testimony, expert testimony, letters, instructions, and testimony of the defendant.[4] The Electronic Information and Transaction Law (hereinafter referred to as the ITE Law) provides a legal basis for the strength of electronic evidence and its admissibility in court. Article 5 paragraph (2) of the ITE Law states that electronic information and electronic documents and their printouts are an extension of legal evidence according to Indonesian procedural law.[5]

The expansion in the ITE Law has enriched the types of evidence regulated in the Criminal Procedure Code and expanded the scope of previously existing evidence of letters. These additions do not only apply in the context of the ITE Law but are also accommodated in other laws such as the Company Documents Law, the Terrorism Eradication Law, the Corruption Eradication Law, and the Money Laundering Prevention and Eradication Law. This expansion covers various forms of electronic evidence that can be used in the judicial process, thus increasing the flexibility and effectiveness of law enforcement in the face of increasingly complex and technology-based crimes.

Electronic information and documents that are used as valid evidence in Indonesian procedural law must meet formal and material requirements. Article 6 of the ITE Law states that electronic information or documents must be documents that are according to the law in written form and must be obtained by legal means.[6] This means that the document must comply with the provisions of the format and method of acquisition. If electronic evidence is obtained in an unauthorized manner, then the evidence can be ruled out by the judge or considered to have no evidentiary value by the court.[7]

Along with the increasing use of digital technology in everyday life, legal cases involving electronic evidence are increasingly common. The validity of electronic evidence is a crucial issue because it concerns the integrity of the judicial process and the protection of individual

[2] Anggita, S., & Sembiring, T. B. (2024). Reformasi Sistem Peradilan Pidana: Tantangan dan Prospek di Era Digital. *Jurnal dari Multidisiplin Internasional Penelitian, 2*(1), p. 254.
[3] Harsya, R. M. K. (2023). Undang-Undang Keamanan Siber di Era Digital: Mengatasi Tantangan dan Mengubah Perlindungan Data. *Jurnal Cahaya Mandalika*, (2), p. 2.
[4] Indonesian Code of Criminal Procedure, Article 184.
[5] Law No. 19 of 2016 Concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions, Article 5 paragraph (2).
[6] Law No. 19 of 2016 Concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions, Article 6.
[7] Constitutional Court Decision No. 20/PUU-XIV/2016, p. 96.

rights. Invalid electronic evidence can harm the parties involved, create injustice, and threaten the credibility of the judicial system. Therefore, ensuring that electronic evidence meets the formal and material requirements set out by the laws and regulations is very important.

The position of electronic evidence has not been clearly regulated in Indonesian procedural law. This creates a legal vacuum that can lead to uncertainty in the evidentiary process, considering that electronic evidence now plays an important role in law enforcement, especially in cases involving cyber crime, money laundering and corruption. The position of electronic evidence must be explicitly recognized in Indonesian criminal procedure law, by providing clear guidelines regarding the types, submission process, and assessment of the validity of electronic evidence, so as to create harmony between technological developments and legal needs in accordance with the principles of justice.

According to Eddy O. S. Hiariej, there are six important parameters in assessing evidence in criminal cases, namely the theory of evidence, the means of evidence, the presentation of evidence to judges in court, the burden of proof, the strength of proof, and the minimum evidence.[8] Especially in the submission of evidence, this process becomes very crucial because it is directly related to the validity and legitimacy of evidence before the court. In the case of electronic evidence, its submission requires proper procedures and is in accordance with applicable procedural law. The process of submitting electronic evidence to the court must ensure that the evidence submitted is authentic and not subject to manipulation.

Personal data protection in cyberspace is crucial to avoid misuse, unauthorized access, and unauthorized use of data. Personal data is individual information that must be stored, maintained and protected as confidential.[9] The right to privacy in the context of personal data allows individuals to know how their data is being used by legitimate third parties. However, this protection also brings with it the complex challenge of ensuring the necessary access for law enforcement without compromising individual privacy. This emphasizes the need for clear limitations and strict scrutiny in the applicable procedural laws on the exemptions granted so as not to excessively harm or threaten people's privacy.

In the legal context, electronic evidence has become an important component of investigations and judicial proceedings.[10] The use of electronic evidence in legal proceedings also brings its own challenges. On the one hand, electronic evidence can improve the effectiveness and efficiency of investigations and trials. On the other hand, there are concerns about the validity and reliability of such evidence, particularly in relation to how data is collected, stored and authenticated. In addition, concerns have also been raised regarding the unclear procedures for retrieving electronic evidence during an investigation or trial. The retrieval of electronic

[8] Hiariej, E. O. S. (2012). *Teori dan Hukum Pembuktian*. Erlangga, Jakarta, p. 14.

[10] Pribadi, I. (2018). Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana. *Lex Renaissance, 3*(1), https://doi.org/10.20885/JLR.vol3.iss1.art4, p. 120.

evidence involving personal data by law enforcement without the authorization of the competent authority raises important questions regarding limitations and potential misuse of data. This requires clarity in the applicable legal framework to ensure privacy protection.

Some previous studies related to this research include research conducted by Rezy Januar Wilyana, Imam Budi Santoso, and Oci Senjaya.[11] This research has examined the legal arrangements of electronic evidence regulated in the ITE Law and found that the KUHAP has not specifically regulated electronic evidence. This research identifies the gap between the provisions in KUHAP and the practices in the field that have accepted the validity of electronic evidence. Meanwhile, this latest research provides more focus on the legal position and categorization of electronic evidence in Article 184 of KUHAP and also explains the validity of the use of electronic evidence by ensuring that it does not violate individual privacy rights, such as in the context of searches.

The next research is from Made Sugi Hartono and Ni Putu Rai Yuliartini.[12] This research focuses on the process of using electronic information and documents as evidence in the context of criminal justice, this research also discusses the parameters used to determine the validity of electronic evidence. The research found that the process of validating electronic evidence by judges involves several key steps, including verification of legality, checking supporting documents through digital forensic tests. Different from this previous study, the current study emphasizes on one of the main parameters of evidence, namely bewijsvoering, which regulates how evidence is presented to the judge and also takes into account that the presentation of electronic evidence must be done without violating the privacy rights of individuals, and in accordance with the provisions of the Personal Data Protection Act.

The next research is from Nurlaila Isima.[13] This research discusses the position and definition of electronic evidence in various laws in Indonesia and shows that there is a lack of uniformity in the use of electronic evidence nomenclature in various laws and regulations without specifically considering aspects of personal data protection. In this latest research, the main focus is on analyzing the legal position and classification of electronic evidence in the Indonesian criminal procedure system. This research presents a more comprehensive view of how the regulation of electronic evidence needs to integrate aspects of personal data protection in a structured manner so that the process of obtaining and presenting evidence, such as in the case of searches, does not violate the privacy rights of individuals protected by law, so that a balance between law enforcement and privacy rights can be achieved.

[11] Wilyana, R. J., Santoso, I. B., & Senjaya, O. (2020). Pembuktian Bukti Elektronik di Persidangan. *Tinjauan Hukum Singaperbangsa (SILREV), 1*(1), 164–183.
[12] Hartono, M. S., & Yuliartini, N. P. R. (2020). Penggunaan Bukti Elektronik Dalam Peradilan Pidana. *Jurnal Komunikasi Hukum (JKH), 6*(1), 281–302.
[13] Isima, N. (2022). Kedudukan Alat Bukti Elektronik Dalam Pembuktian Perkara Pidana. *Gorontalo Law Review*, 5(1), 179–189.

Thus, this research fills the knowledge gap by exploring how the validity of the use of electronic evidence can affect and protect personal data in the context of criminal justice in Indonesia. The purpose of this study is to analyze the issues related to the validity of electronic evidence in the legal evidentiary process in Indonesia and its relationship with the protection of personal data and to examine how existing legal mechanisms can ensure the validity of electronic evidence without violating privacy rights, in accordance with the Personal Data Protection Law (PDP Law).

2. Research Methods

This study employs a normative research method aimed at analyzing and examining the application of norms within the prevailing legal provisions. The research is conducted by reviewing various formal legal regulations, such as laws and relevant legal literature, and linking them to the core issues of the study, namely the validity of electronic evidence and personal data protection as regulated by the relevant provisions. The approaches applied include statutory and conceptual approaches. The statutory approach involves analyzing various regulations, such as the Indonesian Criminal Procedure Code (KUHAP), Law No. 39 of 1999 on Human Rights, the Law on Electronic Information and Transactions and its amendments, Law No. 27 of 2022 on Personal Data Protection, and other related regulations. Meanwhile, the conceptual approach is employed to examine legal concepts such as the validity of electronic evidence, personal data protection, the principle of proportionality, and the principles of compliance and transparency. The data source for this study is secondary data, comprising primary and secondary legal materials. Primary legal materials include legislative texts, while secondary legal materials consist of books, legal journals, and other relevant documents. Data collection is carried out through a literature review, focusing on primary legal materials and related secondary materials. The data collected are analyzed descriptively, presenting the data in an organized manner to facilitate understanding and provide solutions to the issues raised. T

3. Result and Discussion

3.1. The Process of Evidence Using Electronic Evidence in Criminal Cases in Indonesia

Along with technological advances, the process of evidence using electronic evidence in criminal cases in Indonesia has experienced significant development. Based on Article 184 of the Criminal Procedure Code, Indonesian criminal procedure law only recognizes five types of evidence: witness testimony, expert testimony, documents, instructions, and statements of the accused. However, with the development of information technology, recognizing the validity of electronic evidence as part of the criminal evidence system has become more important.[14] This is manifested in various laws and regulations outside the KUHAP that recognize the validity of electronic evidence.

[14] Indonesian Code of Criminal Procedure, Article 184.

In the Indonesian criminal procedure law system, the theory of evidence used is *negatief wettelijk bewijstheorie*, which requires two things to prove the guilt of the defendant: first, there must be valid evidence in accordance with the law (*wettelijk*); second, there must be a conviction of the judge (*negatief*).[15] Article 183 of the Criminal Procedure Code stipulates that the judge may not impose a sentence unless there are at least two valid pieces of evidence and the judge has a conviction that the criminal offense actually occurred and that the defendant is the perpetrator.[16]

Electronic evidence began to be recognized after the enactment of Law No. 8 of 1997 on Company Documents. Although the term "electronic evidence" is not directly mentioned, Article 15 of the Law recognizes that data stored in microfilm or other media can be accepted as an extension of letter evidence. The term "electronic" itself is only clearly regulated in Law No. 20 of 2001, which is an amendment to Law No. 31 of 1999 on the Eradication of Corruption. In this law, electronic evidence is recognized as part of the evidence of clues.

The legal basis for the use of electronic evidence in court was further clarified after the enactment of Law No. 11 of 2008 concerning Electronic Information and Transactions which was later amended by Law No. 19 of 2016 (ITE Law). This ITE Law is considered to provide more legal certainty and expand the scope of its applicability, not only limited to criminal acts of corruption, money laundering, and terrorism. Article 1 paragraph 1 of the ITE Law stipulates that "Electronic information is one or a set of electronic data, including but not limited to writings, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed which have meaning or can be understood by a person capable of understanding them."[17]

Based on these laws, there are two perspectives regarding evidence of electronic information and electronic documents, namely the first view considers that electronic evidence is included in the category of existing evidence, meaning that it cannot stand alone. This can be seen in Law No. 8/1997 on Company Documents, which categorizes electronic evidence as an extension of letter evidence according to Article 184 of the Criminal Procedure Code. Given that electronic documents are part of company documents and company documents themselves are part of letter evidence. Furthermore, in Law Number 20 of 2001 on the Amendment to Law Number 31 of 1999 on the Eradication of Corruption, it is clearly stated that electronic evidence is an extension of legal evidence in the form of clues, as explained in the General Elucidation of Law Number 20 of 2001.

[15]Hiariej, E. O. S. (2013). *Teori dan Hukum Pembuktian* (Cet. 2). Jakarta: Erlangga.
[16]Indonesian Code of Criminal Procedure, Article 183.
[17] Law No. 19 of 2016 Concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions, Article 1 paragraph (1).

The second view states that electronic evidence is a stand-alone evidence. Electronic evidence is considered separate from the evidence that has been regulated in Article 184 of the Criminal Procedure Code. The arrangements can be found in the last four regulations, namely Law Number 15 of 2003 on the Eradication of the Criminal Acts of Terrorism, Law Number 21 of 2007 on the Eradication of the Criminal Acts of Trafficking in Persons, Law Number 35 of 2009 on Narcotics, Law Number 8 of 2010 on the Prevention and Eradication of the Criminal Acts of Money Laundering, Law Number 9 of 2013 on the Prevention and Eradication of the Financing of Terrorism, Law Number 18 of 2013 on the Prevention and Eradication of Forest Destruction, and Law Number 28 of 2014 on Copyright.

In some cases, recordings of telephone conversations or electronic messages can be used as clue evidence if supported by other evidence such as witness testimony or letters.[18] The recordings must show a relevant correlation to the criminal event being investigated, and must be analyzed by a digital forensic expert to ensure authenticity. However, this poses a problem, as in many cases, electronic evidence may be the only evidence available, especially in cases of cybercrime. Therefore, if electronic evidence is only considered as clue evidence, it cannot be used independently to prove a criminal offense. Clue evidence is indirect and abstract, in contrast to other evidence that has a concrete form such as witness testimony or letters. Thus, clue evidence can only be obtained from other legally recognized evidence, and cannot stand alone.[19]

Apart from that, CCTV recordings also often act as crucial evidence in proving criminal offenses, including cases of murder, robbery, or theft. Based on Article 1 paragraph 26 of the Criminal Procedure Code, a witness is an individual who provides information about what is seen, heard, or experienced firsthand.[20] Given that CCTV is a mechanical device that does not have human-like abilities, the recordings it produces cannot be directly categorized as witness testimony. Therefore, the validity of CCTV footage as evidence needs to be linked to other categories that have been regulated in the Criminal Procedure Code.

In order for CCTV footage to be accepted as valid evidence, it must be accompanied by expert testimony in accordance with Article 186 of the Criminal Procedure Code. This expert statement comes from someone who has specialized expertise, such as a digital forensic expert, who can ensure that the footage is authentic, not manipulated, and relevant to the case at hand in court. The testimony provided by the expert aims to authenticate the recording, ensure its validity,

[18] Parwarta, I. B. P. S., & Anak Agung Gde Oka. (2018, May 21). Legalitas Rekaman Pembicaraan Telepon Sebagai Alat Bukti Dalam Penyelesaian Perkara Pidana. *Jurnal Harian Regional*. Retrieved from https://jurnal.harianregional.com/kerthawicara/full-40683.
[19] Harefa, B., & Bazroh, N. (2022). Pembuktian Gratifikasi Seksual dalam Pemberantasan Tindak Pidana Korupsi. *Jurnal Hukum Pidana dan Kriminologi*, 3(2), 44-52.
[20] Indonesian Code of Criminal Procedure, Article 1 Paragraph 26.

and assess whether the evidence was obtained legally in accordance with applicable legal procedures.

In addition to CCTV footage, other electronic evidence that is often used is electronic messages, such as conversations via WhatsApp, email, or other digital platforms. WhatsApp messages can be categorized as letters in the context of Article 187 of KUHAP, which explains that a letter is a writing or record that can provide an explanation of certain criminal events. In the context of the digital era, electronic messages that have been printed out can also be recognized as letters, as regulated by Article 5 paragraph (1) of the ITE Law. This law emphasizes that electronic documents have the same legal force as written documents, so they can be submitted as evidence in court.

However, the validity of WhatsApp messages as mail evidence is not automatically recognized without going through a verification process. The authenticity and authenticity of the message must be checked by a telematics expert, who has the task of ensuring that the message actually originated from the intended sender's device, and has not been manipulated or altered during the transmission process. For example, in a corruption case, WhatsApp messages that show communication between the perpetrator and certain parties must be verified using digital traces or metadata that show the time of sending, the identity of the sender, and the recipient.

Electronic evidence can also function as a clue as regulated in Article 188 of the Criminal Procedure Code. A clue is an act, event, or circumstance that provides an indication that a criminal offense has occurred. The clue must be obtained from other valid evidence, and in the context of electronic evidence, data such as activity logs, metadata, or digital traces can be used as clues, provided they are supported by expert testimony or valid letters. For example, in the case of online fraud, activity logs of electronic banking transactions that show the flow of funds from the victim to the perpetrator's account can be a clue that strengthens the suspicion of criminal acts.

Electronic evidence can only be considered valid if it meets the two conditions that have been mentioned, namely material requirements and formal requirements.[21] Material requirements relate to the substance of the case which is the core of legal issues. In other words, electronic evidence needs to be able to prove facts that are relevant to the case being handled. Meanwhile, the formal requirements relate to how the evidence is obtained, which must be in accordance with applicable legal procedures. In addition, the formal requirements also include the validity of its form. Electronic evidence obtained unlawfully may not be used in court. This is related to

[21]Asimah, D. (2020). Menjawab Kendala Pembuktian Dalam Penerapan Alat Bukti Elektronik To Overcome The Constraints Of Proof In The Application Of Electronic Evidence. *Puslitbang Hukum dan Peradilan Ditjen Badan Peradilan Militer dan Tata Usaha Negara, 3*, 97–110.

the principle of due process of law, where the evidence submitted must be obtained legally so as not to violate the human rights of the defendant or related parties.[22]

Judges, when examining criminal cases, have the authority to assess the strength of electronic evidence. This assessment is carried out with consideration of whether the evidence can provide sufficient confidence to prove a criminal act. Although electronic evidence has been recognized, its strength still needs to be assessed carefully, especially in relation to other evidence.[23] Although electronic evidence has been recognized in the ITE Law, its validity in criminal procedure law is still in doubt because the Criminal Procedure Code has not expressly regulated this matter.

Regulating electronic evidence explicitly in the Criminal Procedure Code will provide various benefits, namely first, it will ensure that electronic evidence has the same legal force as other evidence, such as witness and expert testimony. Second, official recognition in the Criminal Procedure Code will minimize the possibility of debates in court regarding its validity, thereby accelerating the judicial process and providing legal certainty to all parties involved. Third, this regulation will encourage law enforcement officials to better understand and utilize technology in the process of collecting and verifying evidence.

To achieve this goal, it is necessary to revise the KUHAP by incorporating several important aspects such as the need for a detailed explanation of the definition and scope of electronic evidence, including the types of electronic information that can be accepted as valid evidence. Furthermore, the procedures for collecting, seizing and verifying electronic evidence must be clearly regulated to ensure compliance with the principles of criminal procedure law. Aspects of protecting individual privacy rights also need to be included in this regulation in order to maintain a balance between law enforcement and the protection of human rights. Overall, the regulation of electronic evidence in KUHAP does not only fulfill formal legal needs, but is also a strategic step to adapt the Indonesian criminal justice system to technological advances. The revision of KUHAP that regulates electronic evidence will provide a solid legal foundation for more effective, efficient, and fair law enforcement in the ongoing digital era proposed.

3.2. The validity of electronic evidence in ensuring that its use does not violate individual privacy rights as well as the provisions of the Personal Data Protection Act

The acceptance of electronic evidence within the criminal justice process relies not only on its legal recognition but also on ensuring that its application aligns with the protection of human rights, particularly the right to privacy. In the digital era, electronic evidence such as CCTV footage, instant messaging conversations, or electronic transaction data often contain sensitive

[22] Ilyas, A. (2021). Praktik Penerapan Exclusionary Rules di Indonesia. *Masalah-Masalah Hukum, 50*(1), 49–59.
[23] Subarzah, N. A., Wijaya, F., & Ambarita, F. P. (2023). Kekuatan Pembuktian Alat Bukti Elektronik Dalam Tindak Pidana Pencucian Uang Pada Kasus Putusan Nomor 844/Pid. Sus/2019/PN. Ptk. *Krisna Law: Jurnal Mahasiswa Fakultas Hukum Universitas Krisnadwipayana*, 5(1), 81–96.

personal information. Therefore, their use in legal proceedings must pay attention to the principles set out in the Personal Data Protection Law (PDP Law), which aims to protect individual personal data from misuse.

One of the major challenges in the use of electronic evidence is to ensure that the process of collecting, storing and presenting it does not violate the privacy rights of individuals, while still guaranteeing its credibility and validity in court.[24] Article 26 of the Law on Electronic Information and Transactions (UU ITE) provides a guarantee that every person has the right to the protection of his or her personal data, which can only be processed with the consent of the data owner, except under conditions regulated by law.[25] In addition, law enforcement should also refer to the fruit of the poisonous tree principle, which states that illegally obtained evidence is inadmissible in court. This principle, which was first applied in the case of Silverthorne Lumber Co. v. United States (1920), emphasizes that any violation of the law in the process of gathering evidence will undermine the validity of the evidence itself.

The vulnerability of electronic evidence to manipulation, alteration or even destruction further complicates the application of this principle. Therefore, if law enforcement is to prevent the contamination of evidence in the judicial process, it must ensure that all stages of electronic data collection and management are conducted lawfully and in accordance with the law. This not only preserves the integrity of the evidence, but also ensures the protection of individual privacy rights amidst the need for effective law enforcement. According to the above doctrine, if the source of evidence (referred to as the "tree") is illegally obtained, then all evidence obtained from that source (referred to as the "fruit") is also considered illegitimate and contaminated. Simply put, all evidence collected as a result of a law enforcement violation is inadmissible in court if the violation occurred during the evidence collection process.[26] This principle becomes particularly important when discussing the protection of human rights, privacy rights, and due process as it prevents the government from profiting from illegal activities. The main purpose of this doctrine is to stop individual rights violations from occurring one after another.

The right to privacy is one of the human rights generally recognized in national and international law.[27] In the realm of criminal law, this right often conflicts with law enforcement objectives,

[24] Anggraini, Y. (2024). Kekuatan hukum alat bukti elektronik dan kredibilitasnya dalam pembuktian hukum pidana. *Causa: Jurnal Hukum dan Kewarganegaraan, 6*(8), 1–10.
[25] Djafar, W., & Santoso, M. J. (2019). Perlindungan Data Pribadi. Konsep, Instrumen, dan Prinsipnya*, Lembaga Studi dan Advokasi Masyarakat (ELSAM),* Jakarta.
[26] Febriyanto, H. (2023). *Pertimbangan Jaksa dalam Mengajukan Upaya Hukum Banding terhadap Putusan Narkotika Pemidanaan yang Dituntut Rehabilitasl (Studi Kasus: Putusan Pengadilan Negeri Sei Rampah No. 716/Pid. Sus/2021, No. 287/Pid. Sus/2022, dan No. 65/Pid. Sus/2022 yang Diajukan Banding*) (Doctoral dissertation, Universitas Sumatera Utara).
[27] Fauzy, E., & Shandy, N. A. R. (2022). Hak atas privasi dan politik hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Lex Renaissance, 7*(3), 445–461.

especially when investigators need access to a person's personal information to use it as evidence in court. Article 28G Paragraph (1) of the 1945 Constitution states that "every person shall have the right to the protection of his person, family, honor, dignity, and property under his control, and shall have the right to security and protection from threats of fear to do or not to do something which is a fundamental right."[28] Protecting the privacy of every individual to protect their privacy from unauthorized interference, including from law enforcement authorities is a fundamental human right.

In order to maintain the integrity of electronic evidence and protect the privacy rights of individuals, it is important to understand the concept of "*bewijsvoering*," which describes the methods for collecting, obtaining, and presenting evidence to a judge in court.[29] Evidence has an important function as a standard in evaluating the validity of proof in the criminal justice system. When electronic evidence is obtained unlawfully or not in accordance with legal protocols, be classified as "unlawful legal evidence". This notion states that evidence obtained unlawfully cannot be the basis of the trial process. This is in line with the "fruit of the poisonous tree" theory, which states that unlawfully obtained evidence, as well as evidence resulting from such acts, has no evidentiary value and should be excluded in court.

The principle of exclusionary rules is also very important in evidentiary law, which states that evidence obtained by unlawful means should be excluded and, as a matter of law, can stop legal proceedings.[30] Herbert L. Packer stated that unlawfully obtained material should be excluded from judicial proceedings. Therefore, law enforcement authorities must adhere to legal procedures when obtaining electronic evidence, as unlawfully obtained evidence violates the privacy rights of individuals and can render a case null and void.

With the enactment of the PDP Law, challenges related to the collection of electronic evidence have become more complex. The PDP Law provides legal protection to individuals' personal data, which includes the right to know, access and control how their personal data is used. In the context of criminal law, investigators often need to access an individual's personal data for the purposes of an investigation, but this process must be done with great care to ensure that there is no violation of the individual's right to privacy. Article 1 Paragraph (1) of the PDP Law defines personal data as any information relating to a person that can be identified, either directly or indirectly.[31] This means that personal data includes all information relating to an individual's personal life, from name, address, and phone number, to financial information and

[28] Constitution of the Republic of Indonesia, Article 28G Paragraph 1.
[29] Laia, H. K. (2023). *Rekonstruksi Regulasi Sanksi Pidana Terhadap Tindak Pidana Kekerasan Seksual Bersumber Pada Nilai Keadilan Adat Nias* (Doctoral dissertation, Universitas Islam Sultan Agung).
[30] Djiwandono, D. A., Ylma, F. T., & Sella, D. Q. A. N. (2024). Prinsip Exclusionary Rules of Evidence dalam Pembuktian Tindak Pidana Narkotika. *UNES Law Review,* 6(4), 12066-12080.
[31] Law No. 27 of 2022 on Personal Data Protection, Article 1 paragraph (1).

electronic communication history. In the context of electronic evidence collection, these data are often key elements in an investigation.

One of the critical questions that arises is how to ensure that the use of electronic evidence in legal proceedings does not violate the privacy rights of individuals. For this reason, the collection and acquisition of electronic evidence must be carried out in compliance with strict procedures and in accordance with applicable regulations, in order to protect the privacy rights of individuals.[32] The Criminal Procedure Code (KUHAP) provides general guidelines on how to collect evidence, including search and seizure procedures. In terms of unauthorized searches, Article 34 Paragraph (1) of KUHAP allows for an exception in urgent situations, which allows investigators to conduct searches without permission from the President of the District Court.[33] However, this action must be reported immediately afterwards. Despite these exceptions, it is important for investigators to remain cautious when conducting searches, especially those involving electronic evidence. Failure to follow procedures may risk violating an individual's right to privacy and result in evidence being invalidated.

The PDP Law expressly stipulates that any processing of personal data, including in the context of law enforcement, must comply with the principles of privacy protection. These principles include transparency, consent, data security, and compliance with the purpose of data collection. In the case of evidence in court, personal data used as electronic evidence must be processed in accordance with these data protection principles.[34] Violations of these principles, such as unauthorized collection of personal data or processing of data that is incompatible with a legitimate legal purpose, may constitute an invasion of privacy. This may result in the evidence being declared invalid in court. For example, if law enforcement obtains personal data such as emails, browsing history, or text messages without a valid warrant or permission, the use of such data may be considered a violation of the individual's right to privacy. In this case, the violation may lead to the data being excluded as evidence at trial, in accordance with the exclusionary rules applicable in the Indonesian criminal law system.

The PDP Law establishes various mechanisms to ensure that electronic data processing, including in the context of law enforcement, is carried out in accordance with the privacy rights of individuals. One of the most important mechanisms is the principle of consent. Any processing of personal data must be based on the valid consent of the data owner, unless there is another legal basis that justifies the processing, such as public interest or law enforcement. In the case of electronic evidence, if data is obtained without consent or a valid legal basis, then the data cannot be used as valid evidence. In addition, the principle of transparency is also

[32] Satria, M. K., & Yusuf, H. (2024). Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Intelek Dan Cendikiawan Nusantara*, 1(2), 2442-2456.
[33] Indonesian Code of Criminal Procedure, Article 34 Paragraph 1.
[34] Gultom, O., Saputra, A. F., & Aziz, M. F. (2021). Perlindungan Data Pribadi Di Indonesia Menyikapi Liberalisasi Ekonomi Digital. *Indonesia for Global Justice*, 1-135.

crucial. Every individual has the right to know how their data is collected, used, and stored. In the context of law enforcement, this means that authorities must provide individuals with a clear explanation of how their data will be used as evidence. For example, when law enforcement accesses an individual's communication data or digital recordings, they must have a clear and understandable legal basis that can be conveyed to the individual.

The PDP Law also sets out provisions regarding data security. Personal data used as electronic evidence must be protected by a strict security system to prevent manipulation, damage, or theft. In this context, chain of custody, which includes recording every step in the capture and handling of electronic evidence, is very important. This aims to ensure that the evidence remains original and uncontaminated. If the personal data captured as electronic evidence is not adequately protected or manipulated, the validity of the evidence may be questioned at trial. The recognition of electronic evidence in the Indonesian legal system reflects an effort to adapt the law to the development of information technology. In this modern era, electronic evidence, such as data from digital devices or electronic communications, has become an essential component in the process of proving criminal cases, especially in cases involving cyber crime or technology-based crime. Although the ITE Law has provided a legal basis relating to electronic evidence, there are still various challenges in its application. In particular, there are legal gaps in the KUHAP and potential conflicts with the PDP Law that need to be addressed.

The KUHAP, as the legal basis for the criminal justice process in Indonesia, does not yet clearly regulate electronic evidence. In Article 184 of the Criminal Procedure Code, there are five types of evidence that are recognized, namely witness testimony, expert testimony, letters, instructions, and testimony of the defendant. However, electronic evidence - such as digital recordings, communication data, or electronic documents - is not specifically mentioned.[35] This lack of clarity raises legal doubts, especially regarding the categorization and evaluation of electronic evidence in court. For example, evidence in the form of instant messages, such as WhatsApp or emails, are often considered as "letters" due to their communicative function. However, this interpretation remains contentious, especially as the KUHAP does not provide clear guidelines on how such evidence should be obtained, verified and presented. Similarly, CCTV footage or forensic data usually requires expert analysis for its validity, so it can be included in the category of "expert testimony." However, in the absence of firm rules, the Criminal Procedure Code does not provide clear guidelines on how such evidence should be obtained, verified and presented. However, in the absence of firm rules, the use of electronic evidence is often a source of legal disputes, especially in terms of the validity and reliability of such evidence.

One issue that needs special attention is the search and seizure of electronic evidence. Article 43 of the ITE Law, paragraphs (3) and (4), states that searches and seizures of electronic systems must be conducted in accordance with criminal procedure law, while maintaining the public

[35]Ibid, p.2.

interest.[36] However, this provision faces challenges when implemented as KUHAP does not regulate specific procedures for the search and seizure of electronic devices. Articles 33 to 38 of KUHAP focus on general guidelines for search and seizure, but they are geared more towards physical items, such as documents or other tangible objects. The distinctive characteristics of electronic systems-such as the digital nature that is susceptible to alteration, copying or deletion-are not covered by these provisions. As a result, investigators are often faced with the dilemma of determining the appropriate procedures to handle electronic evidence without violating the rights of the parties involved.

To illustrate, the seizure of digital devices such as cell phones or computers usually requires forensic techniques to ensure that relevant data remains intact and verifiable. However, if the search is conducted without a valid warrant or without permission from the chief justice, the action risks violating the principle of due process of law. In addition, illegally obtained data may be considered the "fruit of the poisonous tree", and therefore cannot be used as evidence in court. The PDP Law also provides important protection to individuals' rights to personal data. In Article 15 of the PDP Law, there are exceptions to the rights of personal data subjects in the context of law enforcement, including the search and seizure of electronic evidence.[37] While these exceptions are deemed necessary to support investigation and evidence in criminal cases, there remains a risk of infringement of individuals' privacy rights if the process is not conducted properly.

Article 5 to Article 13 of the Personal Data Protection Law (PDP Law) regulates the various rights that personal data subjects have. These include the right to obtain information regarding the use of personal data, the right to rectify inaccurate data, and the right to object to data processing deemed unauthorized. However, in the context of law enforcement, these rights are often overlooked, especially when data collection is carried out without adequate notice or consent. This can create tension between law enforcement efforts and the protection of human rights. When searches and seizures of electronic systems are conducted without authorization from the chief justice or do not comply with applicable legal principles, such actions not only violate the KUHAP and PDP Law, but can also undermine the credibility of the evidence produced. Therefore, law enforcement needs to ensure that every step in the electronic evidence collection process is in line with the principles of accountability, transparency and proportionality as stipulated in Article 46 of the PDP Law.

However, Article 15 of the PDP Law provides for exceptions to some rights of personal data subjects, especially in the context of law enforcement.[38] Certain rights, such as the right to erase data (Article 8), withdraw consent (Article 9), restrict processing (Article 11), and transfer data

[36] Law No. 19 of 2016 Concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions, Article 43.
[37] Law No. 27 of 2022 on Personal Data Protection, Article 15.
[38] Law No. 19 of 2016 Concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions, Article 15.

to another controller (Article 13), are excluded if the interests of the law enforcement process require it. This means that an individual's right to their personal data can be sacrificed to support law enforcement purposes. The exceptions stipulated in Article 15 of the PDP Law aim to provide flexibility to law enforcement officials in accessing personal data that is relevant to an investigation or other legal process. However, disregarding the rights of personal data subjects in law enforcement proceedings may pose a number of risks, especially if the data collection or use procedures are unauthorized.

For example, searches of personal data conducted without the permission of the chief justice, as stipulated in KUHAP for physical searches, may raise questions about the lawfulness of such actions. In the context of personal data, unauthorized searches or searches without a clear legal basis not only violate the principle of due process of law, but also have the potential to set a bad precedent that undermines individual rights. Furthermore, this exclusionary provision opens room for potential abuse of authority by law enforcement officials. In certain cases, personal data may be accessed or used for purposes that are not relevant to the ongoing legal process. This may contradict the principles of transparency and accountability as stipulated in Article 5 of the PDP Law.

To prevent the misuse of personal data and to ensure that exceptions to the rights of data subjects are not exploited, it is essential to establish clear and robust procedural standards for managing personal data in law enforcement activities. This necessitates more detailed regulations concerning the mechanisms for searching and seizing personal data, as outlined in Article 43 of the ITE Law. Currently, the Criminal Procedure Code lacks specific guidelines for executing searches and seizures of digital or personal data.

These shortcomings can be addressed by harmonizing the PDP Law, KUHAP, and ITE Law. For example, searches of personal data should be conducted with the permission of the court, except in clearly defined urgent circumstances, such as an immediate threat to national or public security. This is crucial to prevent the misuse of the claim of "law enforcement interests" as a pretext to ignore individual rights. When the rights of personal data subjects are excluded in the interest of law enforcement, it is necessary to ensure that the process takes place with high accountability. Any access or processing of personal data for legal purposes should be recorded in detail, including the identity of the officer conducting the search, the legal basis for the action, and the data accessed. Good documentation allows for more effective oversight and prevents possible abuse.

Furthermore, violations of personal data management procedures in the context of law enforcement should be subject to strict sanctions. Article 12 of the PDP Law already regulates the right of data subjects to obtain redress for violations of personal data processing, but the implementation of this provision requires an efficient complaint system, so that individuals can report violations without feeling pressured or facing obstacles. The application of Article 15 of UU PDP, which excludes certain rights of personal data subjects in the interest of law

enforcement, exposes the dilemma between the protection of individual rights and the interests of the state. On the one hand, this flexibility is necessary to support investigations and trials, especially in serious cases that threaten national security or public interest. However, on the other hand, waiving individual rights without clear procedures can undermine public trust in the legal system and create injustice.

The dilemma can be resolved by stricter oversight required in every step involving personal data, from its collection to its use in court proceedings. More precise regulations are also required to ensure that exceptions to the rights of personal data subjects are only made in truly exigent circumstances and in accordance with applicable legal principles. In conclusion, while the exceptions to the rights of personal data subjects in the PDP Law are necessary to support law enforcement, this must be balanced with the protection of individual rights. With clearer procedural standards, harmonization with KUHAP and ITE Law, and effective oversight, the Indonesian legal system can ensure that law enforcement is conducted lawfully and fairly, without compromising the privacy rights of individuals.

A meticulously documented chain of custody process is an essential step to ensuring the integrity and authenticity of electronic evidence. This approach is particularly necessary given the instability and ease of manipulation of electronic evidence which demands careful handling procedures. In addition, capacity building of judges also needs to be considered through continuous socialization and training. This is so that they can better understand digital technology and be able to interpret electronic evidence in court, while respecting privacy rights and applicable evidentiary principles.

4. Conclusion

The process of presenting electronic evidence in criminal cases in Indonesia continues to encounter challenges, primarily because the Criminal Procedure Code lacks clear guidelines on the types and procedures for utilizing such evidence. While the recognition of electronic evidence is addressed in the ITE Law and the PDP Law, these regulations remain uncoordinated, leading to potential overlaps and vulnerabilities in the legal framework. The validity of electronic evidence relies heavily on compliance with criminal procedural law procedures and privacy protections. Unfortunately, practices such as search and seizure often have the potential to violate individuals' privacy rights if not conducted properly. This creates a dilemma between effective law enforcement and the protection of human rights guaranteed by the PDP Law. The revision of KUHAP is needed to explicitly regulate electronic evidence, including its acquisition and management procedures, in order to harmonize with the ITE Law and PDP Law. With clearer and more integrated regulations, Indonesia's legal system can ensure fair, efficient, respectful of individual privacy, and non-overlapping law enforcement.

5. References

Journals:

Asimah, D. (2020). Menjawab kendala pembuktian dalam penerapan alat bukti elektronik. *Puslitbang Hukum dan Peradilan Ditjen Badan Peradilan Militer dan Tata Usaha Negara, 3*, 97–110.

Anggita, S., & Sembiring, T. B. (2024). Reformasi Sistem Peradilan Pidana: Tantangan dan Prospek di Era Digital. *Jurnal dari Multidisiplin Internasional Penelitian,* 2(1), 254.

Harefa, B., & Bazroh, N. (2022). Pembuktian gratifikasi seksual dalam pemberantasan tindak pidana korupsi. *Jurnal Hukum Pidana dan Kriminologi, 3*(2), 44–52.

Djiwandono, D. A., Ylma, F. T., & Sella, D. Q. A. N. (2024). Prinsip Exclusionary Rules Of Evidence Dalam Pembuktian Tindak Pidana Narkotika. *UNES Law Review.*

Fauzy, E., & Shandy, N. A. R. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Lex Renaissance*, 7(3), 445–461.

Harsya, R. M. K. (2023). Undang-Undang Keamanan Siber di Era Digital: Mengatasi Tantangan dan Mengubah Perlindungan Data. *Jurnal Cahaya Mandalika*, (2), 2.

Hartono, M. S., & Yuliartini, N. P. R. (2020). Penggunaan Bukti Elektronik Dalam Peradilan Pidana. *Jurnal Komunikasi Hukum* (JKH, 6)(1), 281–302.

Ilyas, A. (2021). Praktik penerapan exclusionary rules di Indonesia. *Masalah-Masalah Hukum, 50*(1), 49–59.

Isima, N. (2022). Kedudukan Alat Bukti Elektronik Dalam Pembuktian Perkara Pidana. *Gorontalo Law Review,* 5(1), 179–189.

Parwarta, I. B. P. S., & Anak Agung Gde Oka. (2018, May 21). Legalitas rekaman pembicaraan telepon sebagai alat bukti dalam penyelesaian perkara pidana. *Jurnal Harian Regional.* Retrieved from https://jurnal.harianregional.com/kerthawicara/full-40683.

Pribadi, I. (2018). Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana. *Lex Renaissance*, 3(1), 120. https://doi.org/10.20885/JLR.vol3.iss1.art4.

Putra, D. (2020). Pembuktian Tindak Pidana Zina Berdasarkan Bukti Petunjuk: Analisis Putusan Pengadilan No. 506/Pid. B/2017/PN Smn. *Lex Renaissance,* 5(2), 272–286.

Satria, M. K., & Yusuf, H. (2024). Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Intelek dan Cendikiawan Nusantara,* 1(2), 2442–2456.

Subarzah, N. A., Wijaya, F., & Ambarita, F. P. (2023). Kekuatan pembuktian alat bukti elektronik dalam tindak pidana pencucian uang pada kasus putusan No. 844/Pid. Sus/2019/PN. Ptk. *Krisna Law: Jurnal Mahasiswa Fakultas Hukum Universitas Krisnadwipayana, 5*(1), 81–96.

Wilyana, R. J., Santoso, I. B., & Senjaya, O. (2020). Pembuktian Bukti Elektronik Di Persidangan. Tinjauan Hukum Singaperbangsa *(SILREV,* 1)(1), 164–183.

Books:

Fauzi, A. A. (2023). *Pemanfaatan Teknologi Informasi Di Berbagai Sektor Pada Masa Society 5.0.* PT. Sonpedia Penerbit Indonesia.

Gultom, O., Saputra, A. F., & Aziz, M. F. (2021). *Perlindungan Data Pribadi Di Indonesia Menyikapi Liberalisasi Ekonomi Digital.* Indonesia For Global Justice.

Hiariej, E. O. S. (2013). *Teori dan Hukum Pembuktian (Cet. 2).* Jakarta: Erlangga.

Regulation:

Indonesian Code of Criminal Procedure.

Law No. 19 of 2016 Concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions.

Law No. 27 of 2022 on Personal Data Protection.

Constitutional Court Decision No. 20/PUU-XIV/2016.

Government Regulation No. 71 of 2019 Concerning the Implementation of Electronic Systems and Transactions.

Others:

Fauzi, A. A. (2023). *Pemanfaatan Teknologi Informasi Di Berbagai Sektor Pada Masa Society 5.0.* PT. Sonpedia Penerbit Indonesia.

Febriyanto, H. (2023). *Pertimbangan Jaksa dalam Mengajukan Upaya Hukum Banding terhadap Putusan Narkotika Pemidanaan yang Dituntut RehabilitasI (Studi Kasus: Putusan Pengadilan Negeri Sei Rampah No. 716/Pid. Sus/2021, No. 287/Pid. Sus/2022, dan No. 65/Pid. Sus/2022 yang Diajukan Banding)* (Doctoral dissertation, Universitas Sumatera Utara).

Laia, H. K. (2023). Rekonstruksi Regulasi Sanksi Pidana Terhadap Tindak Pidana Kekerasan Seksual Bersumber Pada Nilai Keadilan Adat Nias. *Universitas Islam Sultan Agung.*