International Journal of Educational Review, Law & Social Sciences (IJERLAS)

International Journal of Educational Review, Law And Social Sciences (IJERLAS Journal) | ISSN (e): 2808-487X
Volumes 5 No. 6 (2025)

TREATMENT OF ELECTRONIC EVIDENCE AFTER A JUDGE'S DECISION WHICH HAS PERMANENT LEGAL FORCE IN CRIMINAL CASES

Fanidia Tumanggor[1], Faizin Sulistio[2], Patricia Audrey[3]
[1]Program Magister Ilmu Hukum Fakultas Hukum Universitas Brawijaya, Malang
[2 3]Fakultas Hukum Universitas Brawijaya, Malang
Correspondent Email: 1) fanidia44@gmail.com

Received	: 01 September 2025	Published	: 01 November 2025
Revised	: 15 September 2025	DOI	: https://doi.org/10.54443/ijerlas.v5i6.4362
Accepted	: 10 October 2025	Link Publish	: https://radjapublika.com/index.php/IJERLAS

Abstract

Advances in information and communication technology have significantly influenced legal developments, particularly in the area of evidence in criminal justice processes. The use of electronic evidence as evidence in various criminal cases poses challenges related to the clarity and adequacy of the legal framework in Indonesia. This study aims to examine the extent to which Indonesian law accommodates the existence of electronic evidence and how judges determine its legal status and treatment after a criminal verdict has become final and binding. The study focuses on the question of whether it is sufficient to seize electronic data together with the electronic device or whether a normative separation between the physical device and the electronic data within it is necessary, as is the practice in the Netherlands and France. In this context, it is important to analyze whether existing legal provisions provide legal certainty and strike a balance between the interests of law enforcement and the protection of individuals' rights to personal data, information, and/or electronic documents contained in seized electronic devices. Through a normative juridical and comparative legal approach, this study finds that legal regulations in Indonesia do not specifically regulate the treatment of electronic data in court decisions. Therefore, regulatory reform is needed to ensure the protection of each individual's constitutional rights and strengthen the integrity of the evidentiary system in electronic-based criminal cases.

Keywords: ***electronic evidence, judge's decision, data protection, legal certainty***

BACKGROUND

The development of technology and information has brought significant changes to all aspects of society, including the legal field and the enforcement of justice in Indonesia. One important change in the Indonesian criminal justice system is the recognition of the existence of electronic evidence in the criminal trial process. Electronic evidence such as voice recordings, video recordings, instant messages, electronic mail (e-mail), and even activity logs have become crucial evidence in proving criminal acts.whether the defendant is proven guilty or not of committing the crime that the public prosecutor charged him with in court.[1]

The Criminal Procedure Code (KUHAP) regulates that valid evidence consists of (a) witness statements, (b) expert statements, (c) letters, (d) instructions and (e) statements from the defendant.[2]However, current digital developments have presented new forms of evidence, namely electronic information, electronic documents and/or electronic printouts known as electronic evidence.[3]ApprovedLaw Number 8 of 2011 concerning Electronic Information and Transactions in conjunction with Law Number 1 of 2024 concerning the Second Amendment to Law Number 8 of 2011 concerning Electronic Information and Transactions (ITE) has placed electronic evidence in the form of Electronic Information and/or Electronic Documents as valid evidence in the evidence process in court.[4]

[1]Mohammad Taufik Makarao and Suhasril, Criminal Procedure Law in Theory and Practice, Ghalia Indonesia, Bogor, 2010, p. 2.

[2]Article 184 paragraph 1 of the Criminal Procedure Code

[3]Article 5 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

[4]Ibid

Article 1 number 1 and Article 1 number 4 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions regulate that electronic evidence refers to data in the form of electronic information or electronic documents, whether printed or still in digital format. However, it is necessary to understand that the electronic data is stored in an electronic media or device, so that to obtain data that will become electronic evidence, investigators or prosecutors must first access the electronic media or device, to then extract the data contained in the media using accountable forensic methods.[5]

There are various types and categories of electronic evidence in information and communications technology (ICT). Internally and externally installed electronic devices, as well as other electronic devices found at crime scenes, can hold important information useful as evidence in criminal investigations.[6]In principle, ICT can be divided into three components, namely hardware, software and brainware.[7]Hardware is the physical equipment, software is the data within a computer, and brainware is the thing that initiates the operation of information and communication technology. Electronic devices and the data stored within them can be used as electronic or digital evidence.[8]

The recognition of electronic evidence in the criminal procedural law system has not been fully accompanied by comprehensive legal regulations, particularly regarding the mechanism for treating electronic evidence after a judge's decision has been rendered and has obtained permanent legal force.(inkracht van gewijsde).The provisions of Article 194 paragraph (1) of the Criminal Procedure Code require the judge to determine the formulation of the mechanism for treating evidence for a crime being handled and decided in his/her decision. Determining the treatment of evidence in the judge's decision will provide legal certainty regarding the treatment and actions that must be taken with regard to the evidence.

Electronic evidence used in investigations and trials often contains personal data or confidential information that has the potential to become evidence for other cases, so that determining the status of electronic evidence is much more complex than physical evidence as referred to in Article 39 of the Criminal Procedure Code. In relation to the confiscation of evidence, in the confiscation of electronic evidence there are two (2) objects that can be confiscated, namely the electronic evidence storage device and the information/documents in the device. However, the Criminal Procedure Code and technical regulations related to electronic evidence do not explain the relationship between the two confiscated objects. This condition has the potential to cause problems in determining the treatment of electronic evidence, especially regarding the unclear status of data or information stored in a device—whether its status follows the legal status of the device as determined by the judge in the decision, or whether it has a different status and is independent from the storage device. This data or information essentially has a different and equal status to the device that stores it. Therefore, the judge's determination of how to treat electronic evidence should not affect the treatment of the data or information stored on the device. Therefore, the judge must still determine the treatment or status of the electronic data or information in his or her decision.[9]

One example of a decision at the Medan District Court is the Medan District Court decision Number 579 / Pid.B / 2023 / PN Mdn, the classification of a letter forgery case in which the Defendants in the case were proven to have made fake STNK and fake motor vehicle taxes using a laptop and printer. And in the verdict, the judge determined that electronic evidence in the form of 1 (one) silver Dell brand laptop, 1 (one) Canon Type MG2570s printer, 1 (one) purple Oppo type F9 brand cellphone with sim card number: 082169008388 and 1 (one) gray Wiko cellphone without a sim card, were confiscated for destruction. The judge did not determine whether the electronic evidence intended to be destroyed in this decision was electronic information or electronic documents related to the forgery of letters contained in the confiscated electronic devices or what was destroyed was only the electronic devices. Based on the decision, it is clear that there is a lack of clarity in the relationship and clear separation between electronic evidence storage devices and the data or information stored therein, so that judges in determining electronic evidence in their decisions will create doubt and uncertainty. Based on this, it is important to conduct a more in-depth study regarding the formulation of the treatment of electronic evidence in the criminal justice system, especially after the judge's decision has been rendered and has permanent legal force.

---

[5] Justitia Avila Veda, Directorate of Terrorism and Transnational Crimes, and Counter-Trafficking and Labor Migration Unit IOM, Guidelines for Handling the Crime of Human Trafficking, 2021.

[6]Michael B. Mukasey, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, US Department of Justice, Washington, 2008, p. 1.

[7]*Ibid*

[8]Ibid

[9]Article 194 of the Criminal Procedure Code.

LITERATURE REVIEW

The literature review includes an analysis of previous research that discusses the validity of electronic evidence in criminal procedure law and the role of digital forensics in proving criminal acts. Although there have been many studies related to the existence of electronic evidence, this study specifically highlights the treatment of electronic evidence after the judge's decision in a criminal case has become legally binding. In comparative practice, Dutch law through the provisions of Article 354 Paragraph (2) in conjunction with Article 351 of the Wetboek van Strafverordering essentially regulates that the status of data and information in electronic devices is separate from the storage device, so that the status of the data must be specifically determined in a court decision with the formulation of a specific treatment mechanism.[10]Likewise in France, throughArticle 56 of the French Code of Criminal Procedure (French Criminal Procedure Code) as last amended by Law Number 2024-582 dated June 24, 2024, emphasizedthat there is a clear separation between electronic devices and electronic documents/information contained in the electronic devices.[11] Therefore, with the current regulations in Indonesia, further research is needed to determine whether the determination of the treatment of electronic evidence after a judge's decision has permanent legal force has followed the developments and needs of a dynamic society.

RESEARCH METHODS

This research uses a normative juridical method by means ofexplain the law, interpret the meaning and give value to the law with normative stepsin order to find solutions to the problems being studied.[12]This study examines and analyzes the concept of electronic evidence based on Law of the Republic of Indonesia No. 1 of 2024 in conjunction with Law of the Republic of Indonesia No. 11 of 2008 concerning Electronic Information and Transactions and the formulation of the mechanism for treating electronic evidence based on Article 46 and Article 194 of the Criminal Procedure Code. This study uses a legislative approach by analyzing the 1945 Constitution, Electronic Information and Transactions, the Criminal Code (KUHP) and other regulations related to the handling of Electronic Evidence. In addition, a conceptual approach is used to explore and test the theoretical framework related to the handling and treatment of electronic evidence. This study also utilizes a comparative approach to compare the concept of determining the status of electronic evidence in criminal decisions in Indonesia with legal practices in other countries. Furthermore, the primary legal materials collected come from statutory provisions, while secondary legal materials include scientific literature or non-official legal publications. This research uses library study and documentary study methods with grammatical interpretation analysis techniques to find the implied meaning in the provisions of the laws and regulations being studied, so that rational and accountable legal solutions can be formulated.

RESULTS AND DISCUSSION

Regulation of Electronic Evidence in Criminal Procedure Law in Indonesia

Electronic evidence is a type of evidence obtained from crimes involving the use of technology, either in the form of electronic data stored on hardware such as computers, memory cards, diskettes, SIM cards, or other similar media, or printed copies of such data. This evidence is produced or processed by technological devices and reflects a digital trail of their use.[13] Referring to the provisions of Article 184 of the Criminal Procedure Code, electronic evidence is not explicitly included in the category of valid evidence according to criminal procedural law. However, the Supreme Court, through its letter to the Minister of Justice Number 39/TU/88/102/Pid dated January 14, 1988, emphasized that electronic media such as microfilm and microfiche can be used as valid evidence in criminal cases in court, replacing written evidence, provided that the microfilm is guaranteed to be authentic and can be traced through official registration or minutes. Based on the Supreme Court's interpretation, electronic evidence in the form of microfilm or microfiche is valid evidence in court whose legal standing is equal to written evidence.[14]

[10]Maxius, Wetboek van Strafvordering- Article 354.https://maxius.nl/wetboek-van-strafvordering/artikel354

[11]Code de procédure penale [Code of Criminal Procedure]. (2024, June 26). Article 56. Legislation.https://www.legifrance.gouv.fr/codes/id/LEGIARTI000049778813/2024-06-26

[12]Bahder Johan, Legal Science Research Methods, CV. Mandar Maju, Bandung, 2008, p. 87.

[13] Pandoe Pramoe Kartika, "Electronic Data as Valid Evidence in Proving Money Laundering Crimes," Indonesian Journal of Criminal Law 1, no. 1 (May 24, 2019): 33–46, https://doi.org/10.31960/ijocl.v1i1.146.

[14] Daniel David et al., "Development of Electronic Evidence Regulations in Criminal Procedure Law (Legal Study on Cyber Crime)," UNSRAT Faculty of Law Journal 12, No. 4 (2024).

The provisions in other articles of the Criminal Procedure Code also do not provide explicit recognition of the existence of electronic documents as evidence.Developments in information and communication technology have encouraged the recognition of a new form of evidence not yet explicitly regulated in the Criminal Procedure Code (KUHAP): electronic evidence. Although not explicitly regulated in the KUHAP, the recognition and existence of electronic evidence are regulated in several specific laws and regulations in Indonesia, including:

- Law Number 8 of 1997 concerning Company Documents;[15]
- Law Number 31 of 1999 concerning the Eradication of Criminal Acts of Corruption as amended by Law Number 20 of 2001;[16]
- Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism;[17]
- Law Number 32 of 2009 concerning Environmental Protection and Management;[18]
- Law Number 8 of 2010 concerning the Prevention and Eradication of the Crime of Money Laundering.[19]

One of the important contributions of the ratification of the ITE Law is the legal recognition of the existence of electronic evidence in the judicial process, which applies generally to all types of crimes, except those specifically regulated in other laws and regulations. The only extension of evidence from Article 184 of the Criminal Procedure Code is electronic evidence. Although the ITE Law does not explicitly use the term "electronic evidence," this concept is still recognized and enforced within the legal framework of evidence in Indonesia.[20]Electronic evidence in the ITE Law can be explained as electronic information and electronic documents as regulated in Article 5 of the ITE Law. Electronic Information is “one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail (electronic mail, telegram, telex, telecopy or similar), letters, signs, numbers, Access Codes, symbols, or perforations that have been processed that have meaning or can be understood by people who are able to understand them”. For Electronic documents, it is explained as “any Electronic Information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar form, which can be seen, displayed, and/or heard via a Computer or Electronic System, including but not limited to writing, sound, images, maps, designs, photographs or similar, letters, signs, numbers, Access Codes, symbols or perforations that have meaning or significance or can be understood by people who are able to understand them”.[21]

Furthermore, the provisions of Article 6 of the ITE Law also state that the conditions for electronic evidence to be accepted as evidence in court are as follows:[22]

a. Accessible
b. Can be displayed
c. Guaranteed integrity
d. Can be accounted for so that it explains a situation

The obligation to fulfill the requirements for the validity of electronic evidence is absolute, as stated in Article 5 paragraph (3) of the ITE Law. Therefore, if one of these requirements is not met, the electronic evidence will be invalid as evidence in court.The determination of these requirements is based on the different characteristics of electronic evidence compared to conventional or non-electronic evidence. The main differences are:Electronic evidence is vulnerable to change, destruction and deletion, so that errors in handling it can result in the loss of

[15]Law Number 8 of 1997 concerning Company Documents. Article 15 paragraph (1)

[16]Law Number 31 of 1999 concerning the Eradication of Criminal Acts of Corruption. Article 26A

[17]Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism. Article 27.

[18]Law Number 32 of 2009 concerning Environmental Protection and Management. Explanation of Article 96 letter f.

[19]Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering. Article 38.

[20] Noor Rahmad et al., “The Effectiveness of Electronic Evidence in the ITE Law as an Expansion of the Evidence System in the Criminal Procedure Code,” Proceedings of the 16th Urecol: Education and Humanities Series, 2022, 96–111.

[21]Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

[22]Al-Azhar, MM, Digital forensics: Practical Guidelines for Computer Investigation, Puslabfor Mabes Polri, Jakarta, 2012, pp. 66-67.

evidence of crime or damage to data integrity.[23] Recognition of electronic information and/or electronic documents as electronic evidence is based on the binding nature of such information, which is legally recognized as valid evidence. This provides legal certainty in the implementation of electronic systems and electronic transactions, particularly in proving legal acts conducted through electronic media.[24] Based on this definition, electronic evidence is data/documents stored and/or transmitted via an electronic device, network, or communications system. This data is then used to prove whether a crime has occurred in court. It is not the physical form of the electronic device, such as a cell phone, laptop, hard drive, and so on, but the contents of the electronic device related to the crime that occurred.

Legal Loopholes Regarding the Treatment of Electronic Evidence Following a Judge's Decision in Criminal Cases

Article 44 of the Criminal Procedure Code stipulates that objects that have been confiscated or seized objects are stored in a confiscated objects storage house and the person responsible is an authorized official according to the level of the judicial examination process and the confiscated objects are prohibited from being used by anyone.[25]In the examination of a case in court, the status of confiscated objects or evidence is determined in the verdict. In accordance with Article 46 paragraph (2) of the Criminal Procedure Code, it is stated that:

> "When the case has been decided, the object subject to confiscation is returned to the person or persons mentioned in the decision unless according to the judge's decision the object is confiscated for the state, to be destroyed or damaged until it can no longer be used or if the object is still needed as evidence in another case."

From the text of Article 46 paragraph (2) of the Criminal Procedure Code, the evidence or confiscated objects are determined as follows:

1. returned to the person or persons mentioned in the verdict;
2. confiscated for the state;
3. confiscated to be destroyed or damaged until it can no longer be used;
4. returned to the investigator or public prosecutor if it is still used for other cases.

The Criminal Procedure Code (KUHAP) currently does not explicitly regulate the treatment of electronic evidence after a judge renders a verdict in a criminal case. Article 46 of the KUHAP only generally regulates the status of physical evidence, as referred to in Article 39 of the KUHAP, namely whether the evidence will be returned to the rightful party, destroyed, or confiscated for the state.

Electronic evidence, including electronic information or documents, hardware, and other data storage media, presents more complex challenges in terms of handling and treatment than conventional forms of evidence. However, the Criminal Procedure Code (KUHAP) does not yet provide clear provisions regarding how judges should decide and determine the treatment of such electronic evidence. Therefore, legal reform is needed that can provide clear and comprehensive guidelines for the handling of electronic evidence after a judge's decision has become legally binding, in order to maintain the integrity of the judicial system and protect the rights of all parties involved.

Formulation of the Mechanism for the Treatment of Electronic Evidence After a Judge's Decision Has Permanent Legal Force in Criminal Cases

A judge's decision in a criminal case is not limited to proving or disproving the defendant's guilt, but also includes the obligation to determine the legal status and treatment of evidence. This is an integral part of the judge's authority in resolving the case. Therefore, every court decision, whether imposing a criminal sentence or acquitting the defendant of all legal charges, must include a determination regarding the legal status of the evidence, as stipulated in Article 194 of the Criminal Procedure Code. This provision emphasizes the importance of legal certainty regarding the status of evidence after the decision has obtained permanent legal force.

---

[23]Partnership for Governance Reform, Advocacy Study Institute for Judicial Independence (LeIP), Analysis of Regulatory Gap Concerning the Acquisition, Examination, and Management of Electronic Evidence, Jakarta, 2019, p. 17.

[24] I Made Wirawan, Oheo K. Haris, and Handrawan Handrawan, "The Legality of Expanding the Use of Electronic Evidence in Indonesian Criminal Law Enforcement," Halu Oleo Legal Research 2, no. 1 (2020): 75, https://doi.org/10.33772/holresch.v2i1.10604.

[25]Wasis Priyanto, Development of Evidence Status in Criminal Cases, 2011, accessed December 13, 2024.

In the context of electronic evidence, after a court decision has obtained permanent legal force (inkracht van gewijsde), the handling of electronic evidence enters a crucial stage that must be carried out in an orderly manner and in accordance with legal provisions. At this stage, the judge is obliged to firmly determine the legal status of the electronic evidence used during the trial process. This determination becomes the legal basis that determines the direction of treatment of the evidence, whether it is returned to the entitled party, confiscated for the state, destroyed, or used for other purposes that are lawful according to law. Evidence that is no longer needed in the evidentiary process in court must be returned to the rightful owner, as stipulated in Article 46 paragraphs (1) and (2) of the Criminal Procedure Code. The judge has a responsibility to consider the principles of justice and proportionality, especially for parties who have a legal relationship with the evidence.[26]The return of evidence is not merely administrative but also closely related to the protection of each person's property rights, which are part of human rights. Mistakes in determining the party with the most rights to evidence have the potential to give rise to disputes or objections from the rightful owner, requiring judges to be meticulous, objective, and cautious in making decisions regarding this matter to ensure legal certainty and justice.[27]

The return of evidence in criminal cases is carried out based on the provisions for the implementation of court decisions that have permanent legal force. The implementation of court decisions that have permanent legal force is handed over to the Prosecutor based on the provisions of Article 30 paragraph (1) letter b of Law Number 16 of 2004 concerning the Prosecutor's Office of the Republic of Indonesia, Article 270 of the Criminal Procedure Code, and Article 54 paragraph (1) of Law Number 48 of 2009 concerning Judicial Power. The Prosecutor is obliged to follow the established procedures, including issuing a Letter of Order for the Implementation of Court Decisions (P-48), compiling a Minutes of the Implementation of Court Decisions (BA-8), and implementing other administrative provisions. This procedure is intended to guarantee legal certainty, accountability for the implementation of decisions, and protection of ownership rights over evidence.[28] The execution of a judge's decision begins after the court clerk submits a copy of the legally binding decision to the District Attorney's Office. The Chief Prosecutor will then assign one or more prosecutors to execute the decision. In practice, the execution is generally delegated to the Section Head in charge of the relevant case. The Section Head will review the contents of the decision to be executed and prepare a written order for the execution of the judge's decision. This letter will be accompanied by a report on the judge's decision and related decisions, as well as evidence of the implementation of the judge's decision relating to evidence, criminal penalties, and court costs.[29]

No	Case Number	Classification of Cases	Electronic Evidence/Electronic Evidence	Treatment of Electronic Evidence
1	Medan District Court Decision Number 522/Pid.B/2020/PN Mdn	Letter Forgery	- 1 (one) unit of black LG brand computer monitor; - 1 (one) unit of black CPU, Basic; - 1 (one) unit of black Epson L-300 printer; - 1 (one) unit of black Jedel brand keyboard;	Used in the case of Jhonson Chandra Tarigan
2	Medan District Court Decision Number 580/Pid.B/2023/PN Mdn	Letter Forgery	- 1 (one) unit of Vivo brand cellphone type Y12i	Seized for destruction
3	Medan District Court Decision Number 1103/Pid.B/2021/PN Mdn	Letter Forgery	1 (one) computer unit consists of: a. Samsung brand monitor; b. Libera brand CPU; c. Arech brand keyboard; d. genius brand mouse;	Returned to the Public Prosecutor for use in the

[26]Angelica, "A Review of the Judgment" 12, no. 1 (2024):39–47, https://doi.org/10.20956/verstek.v7i2.xxxx., Op.Cit.

[27]Ibid

[28] Nuraini Nuraini and Olivia Nindy Kartika, "The Role of Public Prosecutors in Returning Evidence to Victims of Crimes in the Jurisdiction of the East Tanjung Jabung District Attorney's Office," Wajah Hukum 8, no. 1 (2024): 395, https://doi.org/10.33087/wjh.v8i1.1461.

[29]Ibid

			e. Toshiba 4 GB flash disk; - 1 (one) unit of Oppo A1K brand cellphone, black; - 1 (one) unit of Oppo brand cellphone, type CPH 1909, black;	Rizal Dasuki case;
4	Medan District Court Decision Number 123/Pid.Sus-TPK/2023/PN Mdn	Criminal Act of Corruption	1. Oppo brand mobile phone type CPH 2217; 2. LCD monitor computer brand Lenovo serial number 3M04625B43200300450AB1 type model D186WA October 2011 color black; 3. CPU brand Leonovo H330 CPU G360 2.7 Machine type 10070 Configuration number 5730463 color black; 4. Epson brand printer type LQ2190 model PA31A serial No. MK4Y179911 gray color; 5. Leonovo brand keyboard;	Returned to the Public Prosecutor
5	Medan District Court Decision Number 579/Pid.B/2023/PN Mdn	Letter Forgery	1 (one) BCA Bank ATM card An Fran Mudigdo, 1 (one) grey Oppo brand mobile phone with sim card number: 081367461800, 1 (one) silver Dell brand laptop, 1 (one) Canon brand printer Type MG2570s, 1 (one) purple Oppo brand mobile phone type F9 with sim card number: 082169008388 and 1 (one) grey Wiko mobile phone without sim card	Seized for destruction

Table 1. Treatment of Electronic Evidence in Judge's Decisions
Source: Medan District Court Case Tracking Information System

Based on the examples of decisions above, it can be seen that the determination of the status of electronic evidence in the verdicts by judges still shows ambiguity, particularly in distinguishing between electronic devices and documents or electronic information stored therein. In these decisions, not a single verdict is found that explicitly determines the legal status of electronic documents or information as referred to in the Electronic Information and Transactions Law (UU ITE). Instead, all decisions only contain provisions regarding the treatment of electronic evidence in the form of the physical electronic device itself, such as a mobile phone or computer, without considering the content of the electronic data contained therein. This reflects a gap or at least a lack of clarity in criminal justice practice regarding the treatment of non-physical elements of electronic evidence, which is an essential part of proving information technology-based crimes.

As explained previously, electronic evidence is data or information contained in a device or medium that stores electronic evidence, not the device or medium itself. This data or information essentially has a different and equal status to the device that stores the data or information. Therefore, the judge's determination of the formulation of treatment for electronic evidence devices should not affect the treatment of data or information stored in the device. Therefore, the judge must still determine the treatment or status of the electronic data or information in his decision. If the judge decides to destroy the electronic evidence storage device, the treatment of the data or information should not follow the treatment of the device that is destroyed, so that the destruction of the device does not result in the status of the data or information being destroyed. If the judge considers destroying the data or information, the judge must specifically state the destruction of the data or information in his decision. This also applies to determining the status of other electronic evidence, for example, if the judge wants to return data or information to its owner, this cannot be done by simply returning the data or information storage device; rather, the judge must specify the return of the data or information in his decision.[30] Jan M. Otto in his article entitled "Real Legal Certainty in Developing Countries" argues that legal certainty does not only cover the legal aspect alone, but also includes certain conditions that require judges in court to be independent, self-reliant and impartial in consistently enforcing the law when resolving disputes they handle, as well as in conditions where court decisions

[30]Article 194 of the Criminal Procedure Code.

can be implemented concretely.[31]The unclear treatment of electronic evidence demonstrates the failure to achieve an independent and consistent judiciary in upholding the law. This reduces the effectiveness of court decisions, which not only make them potentially difficult to implement effectively but can also raise public doubts about the integrity and certainty of the law itself. Regarding the protection of personal data as stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), electronic evidence in the form of documents and/or electronic information contained in electronic devices is closely related to an individual's personal data. Article 1 number 1 of the PDP Law states that "Personal Data is data about an individual who is identified or can be identified individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems." In the context of law enforcement, personal data contained in electronic devices seized as evidence occupies a very important position in its handling.

Based on the provisions of Articles 20, 21, and 22 of the PDP Law, the processing of personal data must be carried out with the explicit, valid consent of the personal data subject and the fulfillment of protection of the personal data subject's vital interests. In addition to facing technical and legal challenges, privacy and data protection issues are also a concern in the context of the use of electronic evidence. When a person's personal information is used as evidence in a case, concerns arise that the individual's right to privacy may be threatened. In a number of cases, the collection and use of personal data as evidence creates a conflict between the protection of privacy rights and the interests of law enforcement.[32]Improper handling of electronic evidence and the unclear legal status of electronic evidence in the judge's decision can give rise to the potential for serious problems, such as data leaks, unauthorized access to information, and misuse of data contained in electronic devices that can cause harm to the individual concerned.[33]Therefore, courts and law enforcement officials are required to carefully balance the protection of individual rights with the need for the use of electronic evidence in the judicial process.

Problems related to electronic evidence often arise due to the lack of a clear separation between electronic devices as physical objects and the digital data they contain, which is of a personal nature. In judicial practice, several judges' decisions indicate that the process of obtaining, presenting, or using electronic evidence is often not accompanied by mechanisms that guarantee the protection of the personal data contained therein. The absence of such mechanisms has the potential to violate the principles of personal data protection as stipulated in the PDP Law, particularly regarding the right to privacy and control of data subjects over their personal information. The absence of explicit and technical regulations regarding the treatment of personal data in electronic evidence can lead to the neglect of legal standards for personal data protection. Therefore, it is crucial for law enforcement officials, including judges, to integrate personal data protection principles into every stage of the judicial process involving electronic evidence. In this regard, court decisions should not be solely oriented toward evidentiary aspects but must also ensure maximum protection of personal data to prevent negative impacts such as information misuse and data leaks that could violate citizens' constitutional rights.

Under personal data protection law, data subjects have a number of rights, such as the right to information, transparency, and access to their personal data. However, these rights are often not optimally utilized due to a lack of public understanding of their existence and implementation mechanisms. Even when recognized, these rights can be restricted if an investigation or inquiry is still underway in a criminal case. This demonstrates the tension between protecting individual privacy and law enforcement's interest in obtaining and processing electronic evidence. When compared with legal practices in other countries, such as the Netherlands, as stipulated in Article 354 paragraph (2) jo. Article 351 Wetboek van Strafvordering, regulates that "In de gevallen, bedoeld in article 353 eerste lid neemt de rechtbank tevens een beslissing over de met toepassing van*article 125ontoegankelijk gemaakte gegevens indien de desbetreffende maatregelen nog niet zijn opgeheven*(Meaning: In the cases mentioned inArticle 353 paragraph (1), the court also made a decision regarding data that cannot be accessed based onArticle 125o, if the relevant action has not been revoked." This provision clearly separates the legal status of electronic devices as physical devices from

[31]Jan M. Otto. (2012). Real Legal Certainty in Developing Countries, In AW Bedner, S. Irianto, & TD Wirastri, Socio-Legal Studies, Jakarta: Pustaka Larasan; University of Indonesia; Leiden University; University of Groningen, 115–156, accessed fromhttps://hdl.handle.net/1887/20633, March 23, 2025

[32] Yuli Anggraini, "The Legal Power of Electronic Evidence and Its Credibility in Criminal Law Proof," Journal of Law and Citizenship 6, no. 8 (2024): 0–11.

[33] Jonathan Matthew Pakpahan, "Awareness of the Urgency of the Role of Personal Data Controllers and Processors in the Context of Protecting Individual Personal Data Based on Law Number 27 of 2022 Concerning Personal Data Protection," To-Ra Law Journal: Law to Regulate and Protect Society 10, no. 1 (2024): 119–37, https://doi.org/10.55809/tora.v10i1.331.

the electronic data or information contained therein. This provision requires the court to specifically determine the treatment of electronic data in the decision, through a clear and measurable mechanism. Meanwhile, in France,Article 56 of the Code of Criminal Procedure (French Criminal Procedure Code) as in the latest amendment through Law Number 2024-582 dated 24 June 2024 concerning Increasing the Effectiveness of the Criminal Asset Confiscation and Forfeiture System states "Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatives aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal….." (Meaning: If the nature of the crime allows for evidence by confiscating letters, documents, computer data, or other objects owned by the person suspected of participating in the crime or keeping documents, information, or objects related to the facts charged, then the judicial police officers are obliged to immediately go to the suspect's house to conduct a search and make a report...). This provision also expressly regulates that there is a clear separation between electronic devices and electronic documents/information contained in the electronic devices.[34].

The seizure of computer data required to reveal the truth in a criminal case is carried out by placing the physical media containing the data, or a copy thereof, into the legal possession of a competent authority. The making of copies must be done in the presence of witnesses who directly witnessed the search process, in order to ensure the accountability and integrity of the seizure procedure. In the case of making electronic copies of data, upon the instruction of the public prosecutor, computer data obtained, owned, or used unlawfully, or which has the potential to endanger the safety of life or property, may be permanently deleted from the original physical media, as long as the media is not in court custody.[35] The treatment of electronic evidence should not stop at the confiscation and analysis stage alone, but should also be explicitly reflected in the judge's decision. The judge's decision should clearly establish the legal status of the physical device and the electronic data contained therein, including whether the evidence will be destroyed, returned to its owner, stored for other purposes, or permanently deleted. The ambiguity in the judge's decision regarding the treatment of electronic evidence stems from the lack of a clear separation between the electronic device as a physical device and the electronic data and/or documents stored therein, particularly personal or sensitive digital data.

This situation has the potential to violate the right to privacy and contradicts the principles of personal data protection as guaranteed by law. Without clarity regarding the status and treatment of such data, the court's decision risks disregarding the constitutional rights of data subjects, particularly in the context of the control, use, and dissemination of personal information that should be legally protected. Therefore, the formulation of the judge's decision, which encompasses both technical and legal aspects regarding the treatment of electronic evidence, is crucial to ensuring legal certainty, procedural fairness, and the protection of citizens' constitutional rights. Accordingly, it is necessary to update and refine regulations, both in criminal procedural law and related implementing regulations, so that courts or judges, when deciding criminal cases that use electronic evidence in the evidentiary process, have a legal basis for determining the treatment of electronic data separately from the electronic devices. This formulation must include technical provisions explaining the procedures for the destruction, return, or storage of electronic data or documents.

This is to ensure that electronic information or electronic documents irrelevant to the criminal case are securely destroyed to prevent future leaks or misuse, and to ensure the return of data or electronic devices to their rightful owners, while taking into account the rights of data subjects and maintaining the integrity of the evidence. The Draft Criminal Procedure Code (KUHAP) currently under revision should include explicit technical provisions regarding the handling of electronic data after a judge's decision, whether the data will be returned, stored, destroyed, or legally blocked. These provisions should also align with the objectives of the enactment of Law Number 27 of 2022 concerning Personal Data Protection, which regulates the rights of data subjects, such as the right to access, delete, and limit data processing, to safeguard citizens' constitutional rights in the digital era. Furthermore, the presence of digital forensic experts at every stage of the investigation, prosecution, and trial is crucial to ensuring the evidence-gathering process is fair and professional. Therefore, integrating data protection into the criminal

[34]Code de procédure penale [Code of Criminal Procedure]. (2024, June 26). Article 56. Legislation.https://www.legifrance.gouv.fr/codes/id/LEGIARTI000049778813/2024-06-26

[35]French Business Law. Article 56 of the French Code of Criminal Procedure. Retrieved July 30, 2025, fromhttps://french-business-law.com/french-legislation-art/article-56-of-the-french-code-of-criminal-procedure

procedure framework is a crucial foundation for maintaining a balance between law enforcement and human rights protection. This reformulation will ultimately strengthen legal certainty and procedural fairness in the digital age.

CONCLUSION

Digital transformation has had a significant impact on the evidentiary system in criminal law, particularly with the emergence of electronic evidence as a primary instrument of proof in modern criminal cases. Although the Indonesian legal system has recognized the existence and legality of electronic evidence through Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, this recognition has not been accompanied by adequate technical regulations. This gap is particularly evident in the treatment of electronic data after a court decision has become legally binding, where there are no clear legal guidelines regarding the legal status of electronic data separately from its storage device. To achieve a balance between law enforcement and the protection of subjects' rights in criminal cases, harmonization of criminal law and data protection law, which have previously operated separately, is necessary. Therefore, a reformulation of criminal procedural law or institutional policies is needed that can provide a legal basis for judges in determining the treatment of electronic data or documents, whether in the form of destruction, return, storage, or blocking of data. This is necessary to ensure the security of information irrelevant to the case, prevent data leaks or misuse, and ensure the return of electronic devices or data to their rightful owners. Furthermore, these regulations must take into account the rights of data subjects and the principles of personal data protection. Thus, the criminal justice system in Indonesia will have a stronger, more modern, and more responsive legal basis to technological developments, while guaranteeing the protection of citizens' constitutional rights in the digital era.

REFERENCES

Buku:

Al-Azhar, M. M. (2012). *Digital forensik: Practical guidelines for computer investigation*. Puslabfor Mabes Polri.

Bahder, J. (2008). *Metode penelitian ilmu hukum*. CV. Mandar Maju.

Makarao, M. T., & Suhasril. (2010). *Hukum acara pidana dalam teori dan praktek*. Ghalia Indonesia.

Jurnal Ilmiah:

Angelica. (2024). Tinjauan semula dalam amar putusan. *Verstek, 12*(1), 39–47. https://doi.org/10.20956/verstek.v7i2.xxxx

Anggraini, Y. (2024). Kekuatan hukum alat bukti elektronik dan kredibilitasnya dalam pembuktian hukum pidana. *Jurnal Hukum dan Kewarganegaraan, 6*(8), 0–11.

David, D., et al. (2024). Perkembangan pengaturan alat bukti elektronik dalam hukum acara pidana (kajian hukum tentang cyber crime). *Jurnal Fakultas Hukum UNSRAT, 12*(4).

Kartika, P. P. (2019). Data elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana pencucian uang. *Indonesian Journal of Criminal Law, 1*(1), 33–46. https://doi.org/10.31960/ijocl.v1i1.146

Nuraini, N., & Kartika, O. N. (2024). Peranan jaksa penuntut umum dalam pengembalian barang bukti kepada pihak korban tindak pidana di wilayah hukum Kejaksaan Negeri Tanjung Jabung Timur. *Wajah Hukum, 8*(1), 395. https://doi.org/10.33087/wjh.v8i1.1461

Pakpahan, J. M. (2024). Kesadaran urgensi peran pengendali dan prosesor data pribadi dalam rangka pelindungan data pribadi individu berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Jurnal Hukum To-Ra: Hukum untuk Mengatur dan Melindungi Masyarakat, 10*(1), 119–137. https://doi.org/10.55809/tora.v10i1.331

Wirawan, I. M., Haris, O. K., & Handrawan, H. (2020). Legalitas perluasan penggunaan alat bukti elektronik dalam penegakan hukum pidana Indonesia. *Halu Oleo Legal Research, 2*(1), 75. https://doi.org/10.33772/holresch.v2i1.10604

Dokumen Pemerintah / Undang-Undang:

Republik Indonesia. (1981). Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

Republik Indonesia. (1997). Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan.

Republik Indonesia. (1999). Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi.

Republik Indonesia. (2003). Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme.

Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Republik Indonesia. (2009). Undang-Undang Nomor 32 Tahun 2009 tentang Perlindungan dan Pengelolaan Lingkungan Hidup.
Republik Indonesia. (2010). Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.
Republik Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Republik Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Laporan/Manual/Panduan:
Kemitraan & LeIP. (2019). *Analisis kesenjangan pengaturan tentang perolehan, pemeriksaan, dan pengelolaan bukti elektronik (electronic evidence)*. Kemitraan.
Mukasey, M. B. (2008). *Electronic crime scene investigation: A guide for first responders* (2nd ed.). U.S. Department of Justice.
Veda, J. A., Direktorat Tindak Pidana Terorisme dan Tindak Pidana Lintas Negara, & IOM. (2021). *Panduan penanganan tindak pidana perdagangan orang*.

Sumber Web/Kode/Artikel Internasional:
Code de procédure pénale [Code of Criminal Procedure]. (2024, June 26). Article 56. Legifrance. https://www.legifrance.gouv.fr/codes/id/LEGIARTI000049778813/2024-06-26
French Business Law. (2025, July 30). Article 56 of the French Code of Criminal Procedure. https://french-business-law.com/french-legislation-art/article-56-of-the-french-code-of-criminal-procedure
Maxius. (n.d.). *Wetboek van Strafvordering*, Artikel 354. https://maxius.nl/wetboek-van-strafvordering/artikel354
Otto, J. M. (2012). Kepastian hukum yang nyata di negara berkembang (Real legal certainty in developing countries). In A. W. Bedner, S. Irianto, & T. D. Wirastri (Eds.), *Kajian socio legal (Socio legal studies)* (pp. 115–156). Pustaka Larasan. https://hdl.handle.net/1887/20633