Society Synergy Conference (SSC)
Volume II; Number II; Year 2025; Pages 537-542
Website:https://sinergilp.com
E-ISSN: 3048-3530

LEGALITY OF DIGITAL EVIDENCE IN CYBER CRIME PROSECUTION BETWEEN NORMATIVE RECOGNITION AND PROCEDURAL INEQUALITY

Zaikul Fuad [*1] Mhd. Azhali Siregar [*2] T. Riza Zarzani [*3]
[123] Universitas Pembangunan Panca Budi
E-mail:zakiulfuad1972@gmail.com

Abstract

The development of digital technology has created new forms of crime known as cybercrime, which requires an update to the criminal law system, especially in terms of evidence. One important instrument in proving digital crime is digital evidence. Although Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), as amended by Law Number 19 of 2016, has explicitly recognized the validity of electronic information as legal evidence, its implementation in court still faces many challenges. This study aims to analyze the legality of digital evidence in the context of the criminal evidence system in Indonesia, as well as to identify the imbalance between normative recognition and procedural application in judicial practice.

The method used in this study is a normative legal approach, using secondary data in the form of laws and regulations, court decisions, and relevant scientific literature. The results of the study indicate that although digital evidence has been recognized in positive law, the provisions in the Criminal Procedure Code have not explicitly accommodated the existence of such evidence. On the other hand, the absence of national standards governing the procedures for collecting, storing, and authenticating digital evidence has led to inequality in the cybercriminal justice process. This is exacerbated by the limited technical capacity of law enforcement officers in the field of digital forensics.

Therefore, a comprehensive revision of the criminal procedure law, the preparation of nationally binding technical guidelines on digital evidence, and the improvement of human resource capacity are needed. These reforms are important to ensure that the Indonesian criminal law system is able to guarantee justice, transparency, and protection of human rights in facing the challenges of law enforcement in the digital era.

Keywords:*digital evidence, criminal evidence, cybercrime*

INTRODUCTION

The development of information and communication technology has given rise to a new chapter in the modus operandi of crime, where perpetrators are no longer bound by the boundaries of physical space, but can carry out their actions from anywhere through digital media. Crimes in cyberspace, or what is commonly referred to as cybercrime, are increasingly complex, including criminal acts such as theft of personal data, distribution of illegal content, hacking of systems, and online fraud. This condition requires adaptation of the criminal law system, especially in the aspect of evidence, which is the main key in the criminal justice process. One of the biggest challenges is how the Indonesian criminal procedure system accommodates and regulates the legality of digital evidence as a means of evidence in court.

The Criminal Procedure Code (KUHAP), as the main regulation in Indonesian criminal procedure law, was drafted in 1981, long before the digital era developed. Article 184 of the Criminal Procedure Code only recognizes five types of evidence, namely witness statements, expert statements, letters, clues, and defendant statements. None of the five categories explicitly cover digital evidence. As a result, the existence of digital evidence in cybercrime cases often gives rise to legal debates regarding its validity and evidentiary strength (Hasibuan et al., 2024).

As a response to the development of the times, the presence of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which was later updated by Law Number 19 of 2016, has become an important milestone in the legal recognition of electronic evidence. Article 5 of the ITE Law states that "Electronic Information and/or Electronic Documents

and their printed results are valid legal evidence", and Article 44 emphasizes that this information can be used in the law enforcement process. With this recognition, the national legal system appears to have adopted digital evidence as a valid means of proof. However, this normative recognition has not been fully implemented effectively in judicial practice. Many challenges arise in terms of the authenticity of evidence, data integrity, and the chain of custody, which have not been technically regulated in the applicable procedural law (Dhadha et al., 2021).

Another problem arises when digital evidence is submitted to court, but is not supported by valid procedures, such as the process of confiscating data without court permission or collecting data from overseas servers without a valid international cooperation mechanism. In some cases, digital evidence is even rejected by judges because it is considered procedurally invalid, even though its content is relevant to the crime being charged. This inequality shows that the Indonesian legal system is not yet fully prepared to deal with the unique characteristics of digital evidence that is vulnerable to manipulation. Moreover, not all law enforcement officers have the technical capacity in the field of digital forensics, which causes the interpretation of digital evidence to be highly dependent on the interpretation of each law enforcer (Winarno, 2011).

Meanwhile, internationally, the Budapest Convention on Cybercrime (2001) has become a reference for many countries in setting digital evidence standards. Articles 14 and 15 of the convention emphasize the importance of lawful and proportionate electronic data collection procedures, as well as the protection of individual privacy rights. Unfortunately, until now Indonesia has not ratified the convention, so domestic regulations are not yet in line with global standards (Yoserwan, 2023).

Thus, this study is relevant to answer the imbalance between normative recognition and procedural reality in cybercrime evidence. Without updating the Criminal Procedure Code and detailed technical guidelines on digital evidence, as well as increasing the capacity of law enforcement human resources, the recognition of digital evidence will lose its functional power in enforcing criminal justice in the digital era.

METHOD

This study uses a normative legal approach, namely legal research that focuses on the study of applicable positive legal norms related to the legality of digital evidence in the cyber criminal evidence system in Indonesia. The data used is secondary data, including primary legal materials such as the Criminal Procedure Code (KUHAP) and Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments, as well as secondary legal materials in the form of court decisions, legal literature, and relevant scientific journals. The analysis is carried out qualitatively, by interpreting laws and regulations, comparing judicial practices, and evaluating the effectiveness of criminal procedure law in facing the challenges of digital evidence. This study also utilizes jurisprudence as an object of analysis, in order to understand how courts implement the legality of digital evidence in criminal law enforcement practices.

RESULTS AND DISCUSSION

Legal Recognition of Digital Evidence in Indonesia's Positive Legal System

Changes in the crime landscape due to advances in information technology have forced the Indonesian criminal law system to adapt to new forms of evidence, one of which is digital evidence. In this context, the legality and validity of digital evidence are central issues in law enforcement against cybercrimes. Although digital evidence has not been explicitly mentioned in the Criminal Procedure Code, its recognition has begun to appear in sectoral regulations, particularly through the

ITE Law. Article 5 paragraph (1) of the ITE Law states that electronic information and/or electronic documents and their printouts constitute valid legal evidence. Furthermore, Article 5 paragraph (2) expands the scope of this evidence as part of valid evidence according to the procedural law applicable in Indonesia. This confirms that the ITE Law provides normative recognition of digital evidence as a means of proof that can be used in criminal cases [Hasibuan et al., 2024].

However, the recognition in the ITE Law is not without legal consequences. As a lex specialis of criminal procedure law in the context of electronic transactions and information, the ITE Law needs to be harmonized with the Criminal Procedure Code which until now has not undergone substantive revision to accommodate digital evidence. In practice, digital evidence is often included in the category of written evidence (Article 184 paragraph (1) letter c of the Criminal Procedure Code), or used as a basis for instructions (letter d), depending on the form and method of presentation. This, as stated by Winarno, shows the dynamic expansion of the interpretation of procedural law, where electronic information is considered a modern form of evidence that has been previously regulated in conventional criminal procedure law [Winarno, 2011].

In addition to normative recognition, it is also important to look at the jurisprudential aspect as a reflection of the application of law in practice. In the South Jakarta District Court Decision No. 712/Pid.Sus/2020/PN JKT.SEL, the judge accepted screenshots from social media and statements from digital forensic experts as valid evidence, as long as the evidence can be verified and supports other evidence. In the decision, the court emphasized the importance of authentication and relevance of digital evidence to criminal events. Thus, the recognition of digital evidence is not only based on its existence as electronic information, but also on how the evidence was obtained, stored, and presented in court [Dhadha et al., 2021].

However, in reality, there are no nationally binding technical guidelines regarding the procedures for handling, storing, and testing digital evidence. This causes disparities in the assessment of digital evidence between cases and between jurisdictions. Many law enforcement officers, both in the police, prosecutors, and courts, do not yet have adequate technical capacity to assess and verify digital evidence, so that the position of this evidence is often debated, even rejected by judges [Yoserwan, 2023].

In the context of the Indonesian evidentiary system which adheres to a negative system according to law (negative wettelijk bewijstheorie), the position of digital evidence becomes crucial. Article 183 of the Criminal Procedure Code states that a judge can only impose a sentence if there are at least two valid pieces of evidence and it is certain that the defendant is the perpetrator. Therefore, digital evidence that is not accompanied by expert testimony or is not forensically verified, even though it is relevant, can lose its evidentiary power. In the future, it is necessary to update the Criminal Procedure Code so that it is able to explicitly regulate the existence of digital evidence as stand-alone evidence, not just an extension of the old category of evidence, and to establish standard technical procedures related to digital forensics, electronic data seizure, and chain of custody.

Procedural Inequality and Forensic Challenges in Digital Evidence in Court

Although there has been normative recognition of the legality of digital evidence in the Indonesian positive legal system, its implementation in the realm of judicial practice has not been fully in line with the principle of due process of law. This inequality is clearly visible in various stages of the legal process, especially in investigations, seizure of electronic data, testing the authenticity of evidence, and strengthening the chain of custody. These procedural challenges are what obscure the effectiveness of digital evidence as an ideal and legitimate means of proof in cybercrime cases.

First, at the investigation stage, law enforcement officers often face technical difficulties in collecting electronic data forensically. Digital evidence is volatile, easily changed, deleted, and can be modified in a very short time. Therefore, the collection process must follow strict digital forensic standards and be systematically documented. Unfortunately, in Indonesia there are no technical regulations governing the methods, tools, and standard procedures that must be used in the

confiscation and security of digital evidence. As a result, much evidence is obtained without using valid cloning or forensic imaging methods, making it vulnerable to being questioned in court (Dhadha et al., 2021).

One of the internationally recognized standards in handling digital evidence is the principle of chain of custody, namely a series of documentation of who has access to evidence from the time it was first collected until it was presented in court. If not properly documented, the validity and integrity of the evidence can be questioned. There are many cases where prosecutors cannot show in detail how the process of obtaining digital data was carried out, whether the tools were legal, who accessed it, or whether there was third party intervention. In the Surabaya District Court decision No. 261/Pid.Sus/2022/PN Sby, for example, the judge questioned the authenticity of the video files obtained from the defendant's cloud storage, because there was no evidence showing that the confiscation procedure was carried out in accordance with court permission, and there was no clear chain of control documentation (Hasibuan et al., 2024).

Second, problems also arise in the aspect of electronic seizures and searches. In the Indonesian legal system, seizures must comply with the provisions of Articles 38 to 46 of the Criminal Procedure Code which require permission from the head of the district court. However, in cybercrime practice, many seizures are carried out remotely, such as taking cloud data, emails, or server logs, without the physical presence of law enforcement officers and without a valid permit. This is problematic because according to Constitutional Court Decision Number 20/PUU-XIV/2016, the collection of digital information without court permission violates the right to privacy guaranteed by the 1945 Constitution, especially Article 28G paragraph (1) and Article 28H paragraph (4) of the 1945 Constitution (Yoserwan, 2023).

The Constitutional Court has firmly stated that wiretapping, digital seizure, and electronic data collection must comply with the principle of due process and be carried out with legal order. Without a clear legal basis and oversight mechanism, digital evidence obtained from violations of these procedures has no legal legitimacy. However, in practice, many investigators do not understand these limits, and often assume that digital information found on the perpetrator's device can automatically be used without strict legal process. In fact, in criminal procedure law which is based on the principle of fair trial, no evidence may be obtained by violating the defendant's constitutional rights.

Third, the next biggest challenge lies in testing the authenticity or authentication of digital evidence. Not all forms of digital evidence can be directly accepted by the court without a technical proof process. For example, in the case of screenshots, the defendant's lawyer can question whether the image has been edited or manipulated. Likewise with emails, instant messages, voice recordings, and other data that can be digitally modified. Therefore, the presence of a digital forensic expert is an absolute requirement in assessing the validity of evidence. However, not all courts in Indonesia have access to competent experts, or standard procedures for appointing and testing the credibility of expert witnesses (Winarno, 2011).

According to international practice, such as in the United States through the Federal Rules of Evidence (FRE), every electronic evidence must be verified for authenticity, either through digital signature methods, hash code verification, or audit trail logs. This procedure allows judges to assess whether the digital file is original, unmodified, and comes from a legitimate source. Unfortunately, Indonesia has not explicitly adopted such standards in the Criminal Procedure Code or other technical regulations, resulting in a legal vacuum that has the potential to endanger material justice (Yoserwan, 2023).

Fourth, there are legal jurisdictional challenges in digital evidence, especially when the evidence is on a foreign server or comes from international cooperation. Cybercrime is often cross-border, with perpetrators, victims, and evidence in three different countries. In this case, Indonesia does not yet have a strong legal instrument in regulating cross-border evidence, and has not ratified the Budapest Convention on Cybercrime (2001) which is the international standard in handling cybercrime. Without this legal instrument, evidence obtained from abroad often cannot be used

directly in Indonesian courts, or must go through the long and complex Mutual Legal Assistance Treaty (MLAT) procedure (Dhadha et al., 2021).

Fifth, systematically, this procedural inequality is exacerbated by the low digital literacy of law enforcement officers. Investigators, prosecutors, and even judges often do not have adequate training in understanding the characteristics of digital evidence. In a research report conducted by Hasibuan et al., it was stated that many judges still assess digital evidence conservatively, equating electronic evidence with conventional evidence without considering technical aspects such as metadata, time stamps, or source IP addresses (Hasibuan et al., 2024). As a result, the evidentiary value of digital evidence is often ignored or even considered invalid due to the lack of understanding of the officers.

This condition shows the imbalance between the speed of technological development and the readiness of the legal system to respond to it. Rigid and unrevised criminal procedure law makes it difficult for digital evidence to find a strong place before the law. In fact, without technical guidelines from the Supreme Court or the Attorney General's Office, practices between regions are very varied and not uniform. This is contrary to the principle of legal certainty guaranteed by Article 28D paragraph (1) of the 1945 Constitution.

CONCLUSION

Based on the discussion above, it can be concluded that legal recognition of digital evidence in cybercrime cases in Indonesia has been normatively recognized through the ITE Law, especially Articles 5 and 44. However, this recognition has not been followed by the readiness of procedural regulations, technical devices, and human resources in the criminal justice system, thus creating serious imbalances in the evidence process. The main challenges faced include the absence of digital forensic standards, weak chain of custody, illegal seizures, difficulty in verifying authentication, and the vacuum of cross-country laws in digital evidence.

This inequality has a direct impact on the fulfillment of the principles of justice and legal certainty. Without comprehensive reform of the Criminal Procedure Code and the establishment of national technical guidelines on digital evidence, the Indonesian criminal procedure law system will continue to lag behind in dealing with the complexity of cybercrime. Therefore, three urgent strategic steps are needed: (1) revision of the Criminal Procedure Code by explicitly including digital evidence categories and digital forensic provisions; (2) preparation of nationally binding technical guidelines for digital evidence; and (3) increasing the technical capacity of law enforcement officers through training, cross-agency cooperation, and academic collaboration.

Only with these steps can the Indonesian legal system realize a criminal justice system that is fair, adaptive, and responsive to technological advances, without sacrificing the principles of protecting human rights in the law enforcement process.

BIBLIOGRAPHY

Dhadha, Tegar Pan, Laras Atika Rahayu, Dewi Sito Resmi, & Dora Kusumastuti. (2021). The Effectiveness of the Role of the ITE Law in Protecting and Maintaining All Cyber Activities in Indonesia. Legal Standing: Journal of Legal Science, 6(1), 40–48.

Hasibuan, Aulia Rahman Hakim, Indra Utama Tanjung, & Kharisma Preety Queen Br Panjaitan. (2024). Legal Protection for Consumers from Defamation Crimes Due to Product Reviews on Social Media. In Law Synergy Conference Proceeding, 1, 337–344.

Ibrahim, Wan Nora Wan. (2021). An Empirical Study on Cybercrime: The Emerging Threat to Banking Sectors in Malaysia. Tun Abdul Razak University.

Lawalata, Jesylia Hillary, Juanrico Alfaromona Sumarezs Titahelu, & Julianus Edwin Latupeirissa. (2022). Restorative Justice Approach in Resolving Narcotics Crime Cases at the Investigation Stage. TATOHI: Journal of Legal Studies, 2(1), 91–112.

lwan Rasiwan, H., & MH SH. (2025). The Principle of Balance of the New Criminal Code Reflects Pancasila Values in Law Enforcement. Takaza Innovatix Labs.

State, Third Amendment to the Constitution. (2001). Republic of Indonesia 1945. Jakarta: Secretariat General of the MPR RI.

(nd). The Role of Telematics Law in Resolving Cybercrime Cases.

Rofiqoh, Anita Zulfiani. (nd). Examining the Phenomenon of Cybercrime in the Realm of Economic Criminal Law: Presenting New Challenges for Law Enforcement in the Digital Era.

Setiawan, M. Nanda. (2021). Criticizing the ITE Law Article 27 Paragraph (3) Viewed from the Socio-Politics of Indonesian Criminal Law. DATIN Law Journal, 2(1), 1–21.

Supriyono, R. Widodo. (2016). Indonesian Criminal Procedure Law. Jakarta: RajaGrafindo Persada.

Winarno, Wahyu Agus. (2011). A Study on the Electronic Information and Transactions Law (UU ITE). Journal of Accounting and Management Economics, 10(1).

Yam, Jim Hoy. (2022). Reflections on Mixed Method Research. EMPIRE, 2(2), 126–134.

Yoserwan. (2023). The Existence of Customary Criminal Law in National Criminal Law After the Ratification of the New Criminal Code. UNES Law Review, 5(4), 1999–2013.

Supramono, Gatot. (2014). Law of Evidence in Practice. Jakarta: Djambatan.

Budapest Convention. (2001). Convention on Cybercrime. Council of Europe Treaty Series No. 185.