Society Synergy Conference (SSC)
Volume II; Number II; Year 2025; Pages 529-536
Website:https://sinergilp.com
E-ISSN: 3048-3530

LEGALITY OF DIGITAL EVIDENCE IN PROVIDING CYBER CRIMES IN COURT

Khairul Huda Rizka*1 Fitri Rafianti*2 Mhd. Azhali Siregar*3
[123] Universitas Pembangunan Panca Budi
E-mail:hudarizka12@gmail.com

Abstract

The development of crime in the digital era has given rise to new challenges in the criminal justice system, especially in terms of evidence. Digital evidence is now a central element in cybercrime cases, replacing the dominance of conventional evidence. Although positive Indonesian law, through Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendment in Law Number 19 of 2016, has explicitly recognized electronic information and/or electronic documents as valid legal evidence, this normative recognition has not been fully effective in court practice. This article examines the legal basis for recognizing digital evidence, the challenges of its application in the criminal justice process, and the need for regulatory updates and strengthening institutional capacity. Using a normative legal approach and analysis of a number of jurisprudence, it was found that digital evidence is very vulnerable to issues of integrity, authenticity, and procedural deviations, such as ignoring the chain of custody. The lack of uniformity in technical procedures in criminal procedure law also worsens the position of digital evidence before judges. Therefore, a comprehensive revision of the Criminal Procedure Code and the establishment of digital forensic technical guidelines are needed to ensure the legality and effectiveness of evidence in cybercrime cases. This study shows that without the support of adaptive regulations and digitally competent officers, the recognition of digital evidence will lose its functional power in upholding criminal justice.

Keywords: Digital Evidence, Criminal Evidence, Cybercrime, Criminal Procedure Law.

INTRODUCTION

The development of information and communication technology has brought about major changes in various aspects of life, including in the way crimes are committed. Crimes are now no longer only occurring in the real world (physical), but have also penetrated into cyberspace, known as cyberspace. This phenomenon marks a paradigm shift in the world of crime, where perpetrators of criminal acts are no longer limited by space and time to carry out their actions. One of the crucial consequences of the presence of cybercrime is the challenge in the aspect of proof, especially in the use of digital evidence in the realm of criminal justice.(Rofiqoh, nd)

In the Indonesian criminal law system, evidence is a fundamental aspect in determining whether or not someone is guilty of a crime. Article 184 paragraph (1) of the Criminal Procedure Code (KUHAP) specifically mentions five valid forms of evidence, namely: witness statements, expert statements, letters, clues, and statements from the accused. This provision, which was drafted in an era before the massive presence of digital technology, certainly does not explicitly regulate the existence and validity of digital evidence. This raises a legal problem: can digital evidence be categorized as one of the five valid forms of evidence mentioned in the KUHAP?(Iwan Rasiwan and SH 2025)

Based on these doubts, there is an urgency to review how criminal procedure law in Indonesia responds to the presence of digital evidence, especially in the context of law enforcement against cybercrimes. These crimes include hacking, malware distribution, personal data theft, online fraud, to illegal content involving child pornography and hate speech on the internet.

Amidst the limitations of the Criminal Procedure Code in regulating digital evidence, the presence of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendment in Law Number 19 of 2016 is an important milestone. Article 5 of the ITE Law emphasizes that electronic information and/or electronic documents, as well as their printouts, are

valid legal evidence. This provision is further emphasized in Article 44 of the ITE Law which states that electronic information and/or electronic documents can be used as evidence in the law enforcement process.(Setiawan 2021)

However, the problem does not end with the recognition of the legality of digital evidence alone. There are still problems in the aspects of procedural validity and acceptance of digital evidence in court. One of the main issues is regarding the integrity, authenticity, and chain of custody of the digital evidence. The collection, storage, and presentation of digital evidence must be carried out forensically so as not to raise suspicions of possible engineering, deletion, or alteration of data.

In judicial practice, the validity of digital evidence is often challenged by the defense. For example, in cases of cyber fraud or the spread of hoax content, the defendant's lawyer can question the authenticity of screenshots, conversation recordings, or server logs submitted as evidence. This shows that even though there is normative recognition in the ITE Law, factual recognition at the court level is still full of challenges. Various jurisprudence has shown the complexity of proof in cybercrime cases. One example is the decision of the South Jakarta District Court Number 712/Pid.Sus/2020/PN JKT.SEL, which tried a perpetrator of defamation through social media. In this case, the main evidence was screenshots from social media and the testimony of a digital forensics expert. However, the judge continued to emphasize that the evidence must be verified for authenticity and supported by other related evidence.

In addition, the Constitutional Court Decision Number 20/PUU-XIV/2016 also emphasizes the importance of protecting electronic evidence from misuse, especially in the context of citizens' right to privacy. The Constitutional Court stated that every act of collecting electronic information must be subject to legal procedures, including requests for legitimate digital wiretapping and searches from law enforcement officers. Therefore, the legality of digital evidence also depends heavily on the suitability of the collection procedure with the principle of due process of law.(Aulia Rahman Hakim Hasibuan, Tanjung, and Panjaitan 2024)At the international level, many countries have more specific legal instruments in regulating the legality of digital evidence. The Budapest Convention on Cybercrime (2001), which is the first international reference in combating cybercrime, pays special attention to digital evidence. Articles 14 and 15 of the convention emphasize the importance of lawful electronic data collection and its proportional application. Unfortunately, Indonesia has not yet ratified the Budapest Convention, so national regulations are not fully in line with international standards.

In this context, there is an urgent need to review and evaluate the effectiveness of national laws in regulating the legality and procedures for proving digital evidence, especially in cybercrime cases. The gap between increasingly digital investigative practices and the still conventional legal system must be immediately bridged through regulatory reform and increased capacity of judicial institutions.(Dhadha et al. 2021)

The revision of the Criminal Procedure Code that has long been drafted by the government and the DPR is expected to be a turning point in the renewal of criminal procedure law that is able to accommodate digital reality. The draft of the Criminal Procedure Code Bill that was once discussed explicitly includes provisions regarding electronic evidence as valid evidence, and opens up space for the recognition of forensic digital investigation methods. However, until now, the draft has not been enacted. On the other hand, the understanding and capacity of law enforcement officers, including investigators, prosecutors, judges, and advocates, are also crucial factors. Handling digital evidence is not enough to rely only on regulations, but also requires technical competence and a deep understanding of information technology. Cooperation with digital forensic experts is a necessity in proving cyber cases.

With this background, this study aims to analyze in depth how the legality of digital evidence is recognized and applied in the criminal justice process in Indonesia. The focus of the study will be directed at three main aspects: (1) the legal basis for recognizing digital evidence in the Indonesian legal system; (2) the procedure for collecting and presenting digital evidence in accordance with the principles of justice and criminal procedure law; and (3) a jurisprudential analysis of the acceptance

of digital evidence in cybercrime cases. This study is expected to provide conceptual and practical contributions to the renewal of Indonesian criminal procedure law, especially in responding to the challenges of criminal evidence in the digital era. In addition, the results of this study can be input for the government and legislative institutions in formulating legal policies that are adaptive to technological developments, as well as strengthening a fair, transparent, and accountable criminal justice system.

METHOD

The research method used in this study is a normative legal approach,(Yam 2022)namely legal research that focuses on the study of positive legal norms that apply regarding the legality of digital evidence in the Indonesian criminal justice system. The data used are secondary data obtained through literature studies, including laws and regulations such as the Criminal Procedure Code, the ITE Law, court decisions, as well as relevant jurisprudence documents and scientific literature. The analysis is carried out qualitatively with an emphasis on legal interpretation and application of norms to the problem of evidence in cybercrime. This approach was chosen to explore the accuracy and adequacy of legal norms in responding to the challenges of digital evidence in the information technology era.

RESULTS AND DISCUSSION

Legal Recognition of Digital Evidence in Indonesian Positive Law

The development of crime in the digital era requires the criminal law system to be able to adapt responsively to new realities, especially in the aspect of evidence. If previously conventional evidence such as letters, witness statements, or physical objects were dominant, then in cybercrime, the main evidence actually comes from electronic data, digital recordings, metadata, and forensic image results of electronic devices. This situation creates an urgent need for legal recognition of digital evidence, both in terms of legality, authenticity, and its proof before a judge.(Aulia R Hakim Hasibuan, Tanjung, and Panjaitan 2024)

As part of the evidentiary system in criminal procedure law, the legality of digital evidence must refer to the main normative instruments, namely the Criminal Procedure Code (KUHAP) and relevant sectoral regulations. However, because the KUHAP was drafted before the digital era, in many cases, its provisions have not been able to accommodate the existence of information technology-based evidence. Therefore, this study will discuss the extent to which Indonesian positive law recognizes the existence of digital evidence as valid evidence, as well as its legal position in the criminal evidentiary system. In general, the evidentiary system in Indonesian criminal procedure law adopts a negative evidentiary system according to law (negatief wettelijk bewijstheorie). This is emphasized in Article 183 of the KUHAP which states that "A judge may not impose a sentence on a person unless with at least two valid pieces of evidence he obtains the conviction that a crime has actually occurred and that the defendant is guilty of committing it."

Article 184 paragraph (1) of the Criminal Procedure Code regulates in a limited manner the types of valid evidence in criminal cases, namely:

1. Witness testimony;
2. Expert testimony;
3. Letter;
4. Instruction;
5. Defendant's statement.

In this context, digital evidence is not explicitly mentioned as a separate category of evidence. This raises legal problems when cybercrime is handled using conventional evidentiary instruments.

However, legal experts agree that digital evidence can be reconstructed into the category of letters, clues, or even expert testimony, depending on the form and substance of the evidence. For example, in the case of the spread of hate speech through social media, screenshots showing the content of the speech can be used as written evidence, while metadata explaining the upload time, device used, and IP address can be used as clues or the basis for the testimony of a digital forensic expert.(Dhadha et al. 2021)A major step in explicit recognition of digital evidence emerged through the ratification of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Article 5 paragraph (1) of the ITE Law states:

"Electronic Information and/or Electronic Documents and/or printouts thereof constitute valid legal evidence."

Furthermore, Article 5 paragraph (2) emphasizes that:

"Electronic Information and/or Electronic Documents referred to in paragraph (1) are an extension of valid evidence in accordance with the procedural laws applicable in Indonesia."

These articles are important because they show that Indonesian law has consciously recognized new forms of evidence in the digital realm, and even stated it as an extension of the evidence mentioned in the Criminal Procedure Code. This means that the existence of electronic information does not shift or add to the category of evidence formally, but rather broadens the interpretation of existing evidence.

Furthermore, Article 44 of the ITE Law also states that:

"Electronic information and/or electronic documents and/or printouts thereof can be used as valid evidence in accordance with the provisions of applicable laws and regulations, including criminal procedure law."

On this basis, digital information such as emails, WhatsApp chats, server activity logs, digital video recordings, and even social media posts can be used as evidence as long as its authenticity, its relevance to the criminal event, and its acquisition in a legally valid manner can be ascertained. One of the important issues in recognizing the legality of digital evidence is how to harmonize the provisions of the ITE Law with the Criminal Procedure Code as the lex generalis of criminal procedure law. Because the Criminal Procedure Code does not explicitly recognize digital evidence, the approach used is interpretive expansion.

This approach is apparent in judicial practice, which is beginning to accept digital evidence as part of a letter (if in the form of a digital document) or as an indication (if used to trace elements of a criminal event), or even as expert testimony if there is technical analysis from a digital forensic expert.(Winarno 2011)According to R. Widodo Supriyono, digital evidence can be included in the category of documentary evidence as long as it meets the requirements as an electronic document that has a structure and context that can be legally verified (Supriyono, Indonesian Criminal Procedure Code, 2016). Likewise, digital evidence can also be part of the instructions as regulated in Article 188 of the Criminal Procedure Code, namely as a combination of witness statements, letters, and circumstances that are interconnected with each other.

This is where the judge's legal understanding is important in assessing the weight of digital evidence, because the validity of evidence is not only determined by its form, but also by how the evidence was obtained and its logical relevance to the charges.

Even though normative recognition has occurred, the issue of the legality of digital evidence often faces challenges in procedural aspects, especially in terms of:

- The legality of the process of obtaining digital evidence (lawful collection);
- Authenticity of digital evidence (authenticity);
- Integrity and absence of manipulation (integrity);
- Chain of custody of evidence.

Digital evidence is very vulnerable to modification, engineering, or deletion. Therefore, the process of collecting digital evidence must be carried out with forensic methods that comply with international standards. Institutions such as the Cyber Crime Directorate of the National Police Criminal Investigation Unit usually carry out a forensic cloning process on the device, then an analysis is

carried out by a digital forensic expert using software such as EnCase or FTK Imager, so that it can guarantee the integrity of the evidence.

However, not all law enforcement officers or judicial institutions in Indonesia have the capacity and infrastructure to ensure this. This has led to several cases where digital evidence has been rejected or its validity questioned in court.(Ersya 2017)A number of court decisions have tested the legality of digital evidence in cybercrime cases. For example:

- South Jakarta District Court Decision No. 712/Pid.Sus/2020/PN JKT.SEL, in a case of defamation on social media. The judge in this case accepted screenshots and digital forensic analysis as valid evidence because they were supported by expert testimony and direct links to the defendant's account.
- Surabaya District Court Decision No. 261/Pid.Sus/2022/PN Sby, which decided the case of the distribution of immoral content. The judge assessed the validity of digital video evidence obtained from cloud storage, and emphasized the importance of chain of custody to prove that the file has not been changed.
- Constitutional Court Decision No. 20/PUU-XIV/2016, although not in a criminal case, the Constitutional Court emphasized the importance of legal procedures in the collection and use of electronic information, especially related to citizens' privacy rights. This also has an impact on the limits of digital evidence collection by investigators so as not to violate the constitutional rights of suspects.

Although there has been explicit recognition of digital evidence in the ITE Law, this recognition has not been balanced with technical regulations in criminal procedure law that regulate in detail the procedures for collecting, verifying, and using digital evidence. As a result, there is a gap between the needs of practice and the norms available.

Revisions to the Criminal Procedure Code are urgently needed to explicitly accommodate the category of digital evidence, while also regulating technical provisions regarding digital forensics, confiscation of electronic devices, data security, and presentation of evidence in court.(Ibrahim 2021)In addition to regulatory updates, increasing the capacity of human resources in the criminal justice system is also an urgent need. Judges, prosecutors, and lawyers need to be equipped with the knowledge and skills to understand and assess digital evidence, so that there are no errors in assessment due to a lack of legal digital literacy.

Application of Digital Evidence in Cyber Criminal Justice Practices in Indonesia

As crimes in the digital space become increasingly complex, Indonesian criminal justice is faced with new challenges in terms of evidence. Cybercrime includes crimes committed using information technology, either as a tool or as the object of the crime itself. Unlike conventional crimes which generally have physical traces or direct witnesses, cybercrime often leaves traces in digital form, such as log files, metadata, digital footprints, and recordings of online activity. Therefore, digital evidence is central to the evidence process, and its role cannot be underestimated. However, how it is applied in criminal justice practices in Indonesia still has a number of important problems that require further study.(Nurdin1 et al., nd)

Normatively, legal recognition of digital evidence has been granted through Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), as amended by Law Number 19 of 2016. As discussed in the previous chapter, Article 5 and Article 44 of the ITE Law explicitly state that electronic information and/or electronic documents, as well as their printouts, can be used as valid legal evidence. However, in practice, this normative recognition often faces various challenges in terms of implementation, both in the investigation, prosecution, and trial stages.

At the investigation stage, the main challenge in using digital evidence is the limited tools and technical capabilities of law enforcement officers. The process of obtaining digital evidence cannot be equated with the collection of conventional evidence. The procedure must be carried out with the right digital forensic method so that the evidence is not damaged, changed, or even deleted. Collecting evidence haphazardly, without following a strict chain of custody, can cause the digital evidence to

be considered invalid or its integrity to be questioned before the panel of judges. Chain of custody is a documentation procedure that explains who holds, accesses, or manipulates evidence from the time it is first obtained until it is submitted to the court. If this procedure is not carried out properly, the potential for misuse or manipulation of evidence is wide open.(Lawalata, Titahelu, and Latupeirissa 2022)In addition, the procedure for confiscating and searching electronic devices is also often a source of dispute. In general criminal cases, confiscation must be carried out with a court warrant, as regulated in Articles 38 to 46 of the Criminal Procedure Code. However, in the practice of handling cybercrime, there are often actions to take data online (remotely) which are difficult to control physically. This raises the question: is the confiscation of cloud data or data on online servers also subject to the same mechanism? Can the actions of officers in accessing email, online storage folders, or personal servers without court permission be legally justified? In this case, the Constitutional Court in Decision Number 20/PUU-XIV/2016 has emphasized that any form of taking personal information through digital devices, whether in the form of wiretapping, electronic searches, or confiscation of digital data, must go through a legal process and cannot be done unilaterally.

In the trial process, the challenge that arises is how judges assess digital evidence as valid and convincing evidence. According to the negative evidence system according to the laws adopted by Indonesia, judges are not sufficient to only accept evidence formally, but must also obtain confidence that the evidence truly reveals the material truth of a criminal event. This requires the judge to be careful and have the technical ability to understand the characteristics of digital evidence. Problems arise when digital evidence submitted by the public prosecutor, such as WhatsApp chat recordings, screenshots of social media accounts, or digital CCTV recordings, is considered weak if not supported by forensic verification and expert testimony.

Several cases have provided a concrete illustration of this problem. In the case of spreading hate speech via Facebook which was tried at the South Jakarta District Court, case number 712/Pid.Sus/2020/PN JKT.SEL, the main evidence presented by the prosecutor was a screenshot of the defendant's social media account containing hate speech based on SARA. However, the defense filed an objection because there was no digital hash or forensic verification to ensure that the screenshot had not been modified. Therefore, the judge did not only base the verdict on the evidence alone, but also on the statements of digital forensic experts and witnesses who saw the content directly. Another challenge in the practice of proving digital evidence is the difficulty of distinguishing between original data and engineered data. In the digital space, it is very easy for someone to falsify data, either through deep fake, metadata manipulation, or other techniques that are obfuscated. Therefore, the presence of expert witnesses in the field of digital forensics is very important to assess the validity of the evidence. Unfortunately, not all courts in Indonesia have access or standard procedures to present competent and independent digital forensic experts. This is a serious obstacle in ensuring a fair trial, especially in cybercrime cases where the main evidence is entirely digital-based.

In a theoretical context, digital evidence also challenges the paradigm of procedural law that is still oriented towards physical forms and paper documents. Digital evidence is immaterial, can be duplicated without limits, and is easily distributed. This raises new legal dilemmas, such as how to calculate the evidentiary weight of a single video or audio clip that could come from an anonymous source. Can the principle of non-self-incrimination (the right not to be forced to reveal oneself as a perpetrator of a crime) be maintained if someone is forced to open access to their personal email or social media account? In this case, it is important to balance the effectiveness of the evidence with the protection of the suspect's rights as regulated in Articles 28G and 28H of the 1945 Constitution concerning the protection of privacy rights and procedural justice.(Country 2001)The legal regime for digital evidence also does not yet have uniform procedures at the technical regulation level. In practice, law enforcement officers refer to the Regulation of the Chief of Police Number 6 of 2019 concerning Criminal Investigation, but this regulation does not yet regulate digital investigation techniques in detail. On the other hand, there are also guidelines from the Attorney General's Office and the Supreme Court regarding evidence in cyber cases, but they are not yet binding and are still

administrative in nature. As a result, there is inconsistency in the application of the law between one case and another, depending on the capacity and perception of each officer.

From an international perspective, Indonesia can actually learn from the experiences of countries that have previously set technical standards for digital evidence. The United States, for example, through the Federal Rules of Evidence (FRE) has explicitly regulated the recognition and verification of electronic evidence. Likewise, the European Convention on Cybercrime (Budapest Convention) sets minimum standards for procedures for the seizure, storage, and presentation of digital evidence. Although Indonesia has not ratified the Budapest Convention, the substance of the convention can be used as a reference in updating the Criminal Procedure Code or drafting new regulations that are more adaptive to digital needs.

Criminal evidence in cyber cases also has its own dynamics related to jurisdiction. In the digital world, perpetrators and victims can be in two different countries, servers that store data can be in a third country, and the process of collecting evidence can involve cross-border evidence collection. This raises new questions: what is the legality of digital evidence taken from overseas servers? Can evidence obtained through cooperation with Interpol, or through the Mutual Legal Assistance Treaty (MLAT) be directly accepted in Indonesian courts? Currently, domestic regulations do not comprehensively answer these questions, so in many cases, such evidence is still considered with a high degree of caution by judges.

To address all of the above challenges, systemic reforms are needed in three aspects. First, it is necessary to immediately ratify the new Criminal Procedure Code which explicitly regulates the types, forms, and procedures for proving digital evidence, as well as recognizing digital forensics as a mandatory procedure in cybercrime cases. Second, the technical capacity and infrastructure of the judiciary and law enforcement agencies must be improved through training, technology investment, and cooperation with academic and professional institutions. Third, it is necessary to create binding technical guidelines for proving digital evidence, in order to create uniformity in legal practices throughout the jurisdiction of Indonesia.(Yoserwan 2023)

Ultimately, the recognition of the legality of digital evidence in the Indonesian criminal justice system is an inevitability that cannot be rejected. However, normative recognition alone is not enough without being balanced with technical regulations, improving the capacity of judicial institutions, and an understanding of procedural law that is adaptive to the development of the times. In the era of the industrial revolution 4.0, justice must not be left behind by technological advances. In fact, the law must be present to bridge digital innovation and protection of citizens' rights in criminal proceedings. Digital evidence, with all its complexity and potential, must be understood not as a threat to the legal system, but as an opportunity to realize a more transparent, accurate, and materially truth-based justice system.

CONCLUSION

Based on the discussion that has been outlined, it can be concluded that the legality of digital evidence in cybercrime evidence in Indonesia has been normatively recognized through the provisions of the ITE Law, especially Article 5 and Article 44, which state that electronic information and/or electronic documents are valid legal evidence. However, this recognition has not been fully effective in judicial practice, considering that there are still limitations in aspects of technical regulations, legal procedures, and the capacity of law enforcement officers to understand and handle digital evidence professionally. Challenges such as the integrity of evidence, the validity of digital seizure procedures, and the availability of digital forensic expertise are obstacles that must be overcome immediately. Therefore, reform of criminal procedural law, strengthening institutions, and the formation of technical guidelines for digital evidence are urgent needs so that criminal justice in Indonesia is able to respond to the dynamics of cybercrime fairly and accountably.

BIBLIOGRAPHY

Dhadha, Tegar Pan, Laras Atika Rahayu, Dewi Sito Resmi, and 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 Studies 6 (1): 40–48.

Ersya, Muhammad Prima. 2017. "Legal Issues in Tackling Cyber Crime in Indonesia." Journal of Moral and Civic Education 1 (1): 50–62.

Hasibuan, Aulia R Hakim, Indra Utama Tanjung, and Kharisma Preety Queen Br Panjaitan. 2024. Criminal Law in Product Reviews on Social Media. Serasi Media Technology.

Hasibuan, Aulia Rahman Hakim, Indra Utama Tanjung, and Kharisma Preety Queen Br Panjaitan. 2024. "Legal Protection for Consumers from Defamation Crimes Due to Product Reviews on Social Media." In Law Sinergy Conference Proceeding, 1:337–44.

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

Lawalata, Jesylia Hillary, Juanrico Alfaromona Sumarezs Titahelu, and 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, and 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 in 1945." In accordance with the order of chapters, articles and verses, (Jakarta: Secretariat General of the MPR RI, 2006).

Nurdin1, Merry Kurniawati, Chika Aurel Rivaldi, Novia Rahmadani, Hilyah Az Zahra4, Andika Rayhan, and Putra Herang5. nd "THE ROLE OF TELEMATICS LAW IN SOLVING CYBERCRIME CASES."

Rofiqoh, Anita Zulfiani. nd "Unraveling 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.

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

Yam, Jim Hoy. 2022. "Reflections on Mixed Methods Research." EMPIRE 2 (2): 126–34.

Yoserwan, 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.