SNLPR: Siber Nusantara of Law and Politic Review
E-ISSN : 3089-2287
+62 822 1012 3600 https://research.e-siber.org/SNLPR siberpublisher.info@gmail.com
**DOI:** https://doi.org/10.38035/snlpr.v2i2


# Digital Evidence in the Crime of Disseminating Indecent Content on Social Media: Analysis of Expert Statements, Electronic Evidence, and Criminal Liability under the ITE Law

**Edy Krispono[1], Ade Zamrah[2], Zainal Arifin Hoesein[3]**
[1]Universitas Borobudur, Jakarta, Indonesia, 25730857@borobudur.ac.id
[2]Universitas Borobudur, Jakarta, Indonesia, 25730885@borobudur.ac.id
[3]Universitas Borobudur, Jakarta, Indonesia, zainal.arifin@umj.ac.id

Corresponding Author: 25730857@borobudur.ac.id[1]

**Abstract:** The development of information technology has changed the pattern of criminal acts, including the dissemination of immoral content through social media. These acts no longer only abandon conventional evidence but also produce various forms of electronic evidence that require special evidentiary mechanisms. The problems that arise are the position of electronic evidence in proving elements of a crime, the evidentiary strength of the testimony of digital forensic experts and Information and Electronic Transactions (ITE) experts, and how the perpetrators are held criminally liable based on the provisions of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. This study aims to analyze the evidentiary strength of electronic evidence, the relevance of expert testimony in the evidentiary process, and the construction of criminal liability for perpetrators of the dissemination of immoral content through social media. The study employed normative legal research methods with a statute approach, a conceptual approach, and a case approach. Data was analyzed qualitatively by reviewing the provisions of the Criminal Procedure Code (KUHAP), the ITE Law, Law Number 1 of 2024, and the investigative facts in a case of alleged distribution of indecent content via an Instagram account handled by the Special Criminal Investigation Directorate of the West Kalimantan Regional Police. The results of the study indicate that digital evidence in cases of crimes against morality on social media cannot only rely on the existence of screenshots but must be supported by a series of other electronic evidence, such as electronic devices, digital traces of accounts, metadata, witness statements, and expert statements explaining the relationship between the perpetrator's identity and the electronic activities carried out. Expert statements have an important function in explaining the fulfillment of the element "intentionally and without rights" as regulated in Article 27 paragraph (1) in conjunction with Article 45 paragraph (1) of the ITE Law, thereby strengthening the judge's belief in the validity of electronic evidence. The perpetrator's criminal liability is not only based on ownership of a social media account, but also on the investigator's ability to prove control of the account, use of electronic devices, a causal relationship between the perpetrator's actions and the distribution of content, and the existence of intent in distributing electronic information containing morality.

**Keyword:** Digital Evidence, Electronic Evidence, Expert Testimony, Social Media, ITE Law, Criminal Liability.

## INTRODUCTION

The development of information and communication technology has brought significant changes to people's lives. The use of the internet and social media is no longer merely a means of communication, but has evolved into a digital public space that allows individuals to produce, store, and disseminate information in a very short time. While this convenience benefits economic development, education, and democracy, it has also given rise to various new forms of crime (cybercrime) that are difficult to address using conventional criminal evidence.

Digital transformation has transformed nearly every aspect of society, including the way people communicate, interact, and exchange information. The development of the internet, social media, cloud computing, and artificial intelligence has created a digital space capable of accelerating the dissemination of information without the constraints of time and space. On the other hand, these developments have also given rise to new forms of crime (cybercrime) that differ from conventional crimes. One form of crime that has seen an increase is the dissemination of indecent content through social media, which not only causes legal harm but also impacts the psychological, social, and reputational impacts of victims.

One form of cybercrime that has increased in recent years is the distribution of indecent content via social media. This act often involves sharing private photos or videos of someone without their consent via various digital platforms such as Instagram, Facebook, WhatsApp, Telegram, and other internet-based applications. In practice, the distribution of this content is not only intended to humiliate the victim, but is also often used as a form of revenge porn, blackmail (sextortion), or psychological intimidation, resulting in material and immaterial losses for the victim.

The characteristics of these crimes differ from conventional crimes because the entire sequence of actions takes place electronically. The evidence used is no longer merely physical objects, but also electronic information, electronic documents, social media accounts, metadata, digital activity records, system logs, and even the electronic devices used by the perpetrator. Therefore, establishing evidence in cyber cases requires a different approach than establishing evidence in conventional criminal cases, as stipulated in the Criminal Procedure Code (KUHAP).

The recognition of electronic information and electronic documents as valid evidence represents a significant reform in the Indonesian legal system. Through Law No. 11 of 2008 concerning Electronic Information and Transactions, as most recently amended by Law No. 1 of 2024, lawmakers legitimized the use of electronic evidence in law enforcement. However, this normative recognition still leaves various practical challenges, particularly regarding how to prove the authenticity of electronic evidence, how to link the identity of the perpetrator to the social media account used, and how to prove the existence of intent and unauthorized dissemination of indecent content.

This problem was apparent in the case of the distribution of obscene content handled by the West Kalimantan Regional Police's Special Criminal Investigation Directorate. Based on the results of the investigation, the case involved the distribution of the victim's personal photos via an Instagram account controlled by the suspect. In the process of providing evidence, investigators not only used screenshots, but also confiscated mobile phones, presented witnesses, examined social media accounts, and requested expert testimony in the field of Information and Electronic Transactions to explain the relationship between digital activities and elements of criminal acts as regulated in Article 27 paragraph (1) in conjunction with Article 45 paragraph (1) of the ITE Law.

This case demonstrates that digital evidence cannot rely solely on screenshots as the sole evidence. Screenshots merely provide a visual representation of electronic information,

but they are insufficient to prove who uploaded it, when it occurred, what device was used, or whether the electronic data was manipulated. Therefore, an integration of electronic evidence, witness testimony, expert testimony, and other digital evidence is necessary to establish a corroboration that meets the standards of proof in criminal procedure law.

In this context, expert testimony is a crucial instrument. Experts not only explain the technical aspects of electronic systems and the characteristics of digital evidence, but also provide scientific explanations regarding the relationship between the perpetrator's digital identity and the electronic activity they engage in. This testimony serves as the basis for investigators, prosecutors, and judges to assess whether the elements of actus reus and mens rea in cybercrimes are met. In this case, the ITE expert explained that proving the element of "intentionally and without right" must be analyzed through the relationship between the perpetrator's actions and the distribution or transmission of electronic information within an electronic system.

Academically, studies on proving cybercrime in Indonesia still focus primarily on the legality of electronic evidence from a normative perspective. Meanwhile, research integrating analysis of electronic evidence, the function of expert testimony, and the construction of criminal liability in cases involving the distribution of indecent content based on the latest amendments to the Electronic Information and Transactions Law (ITE Law) remains relatively limited. This situation suggests there is room for developing more comprehensive studies on digital evidence in law enforcement practices in Indonesia.

Based on the description, this research is important to analyze in depth the position of electronic evidence, the function of expert testimony in digital evidence, and the construction of criminal liability for perpetrators of disseminating immoral content through social media based on the provisions of Indonesian positive law.

## METHOD

This research is a normative legal research that aims to examine legal norms regarding digital evidence in the criminal act of disseminating indecent content through social media. Normative legal research focuses on the analysis of laws and regulations, legal principles, doctrines, and court decisions related to the legal issue under study. [1]However, to strengthen the normative analysis, this research also uses factual data in the form of investigative documents as a case study to illustrate the implementation of legal norms in law enforcement practices regarding the criminal act of disseminating indecent content through social media.

The approaches used in this research include the statute approach, the conceptual approach, and the case approach. The statutory approach is used to examine the provisions of the Criminal Procedure Code, Law Number 1 of 2023 concerning the Criminal Code, and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. The conceptual approach is used to analyze [2]the theory of proof, the theory of criminal liability, the concept of electronic evidence, and the theory of cyber law that have developed in the legal literature. [3]The case approach is used to examine the application of legal norms in the case of alleged dissemination of immoral content through social media handled by the Directorate of Special Criminal Investigation of the West Kalimantan Regional Police as the object of research.

The legal materials used consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include the 1945 Constitution of the Republic of Indonesia, the Criminal Procedure Code, Law Number 1 of 2023 concerning the Criminal Code, Law Number 1 of 2024 concerning the Second Amendment to Law Number

[1]Peter Mahmud Marzuki, Legal Research, Revised Edition (Kencana 2021), pp. 35–57.
[2]Johnny Ibrahim, Theory and Methodology of Normative Legal Research (Bayumedia Publishing 2019), pp. 295–310.
[3]Edmon Makarim, Introduction to Telematics Law (Rajawali Pers 2021), pp. 168–184.

11 of 2008 concerning Electronic Information and Transactions, and investigative documents in the form of case summaries that are the object of research. Secondary legal materials are obtained from books, national and international scientific journals, previous research results, and expert opinions related to criminal law, criminal procedure law, cyber law, and electronic evidence. [4]Meanwhile, tertiary legal materials include legal dictionaries, legal encyclopedias, and other scientific sources that support the research analysis.

The collection of legal materials was conducted through library research and document study. The former involved inventorying and reviewing various relevant laws and regulations, scientific literature, and research findings. The latter involved reviewing investigative documents, including police reports, witness examination minutes, suspect examination minutes, electronic evidence seizure minutes, and expert testimony on Electronic Information and Transactions, which were included in the case files.

The legal material analysis was conducted qualitatively using descriptive-analytical and prescriptive methods. Descriptive analysis was used to describe the construction of digital evidence in cases involving the distribution of immoral content through social media, while prescriptive analysis was used to provide legal arguments regarding the status of electronic evidence, the function of expert testimony, and criminal liability based on the provisions of the Criminal Procedure Code and the Electronic Information and Transactions Law. [5]The results of the analysis were then systematically compiled to answer the research problem formulation and provide recommendations for the development of a digital evidence system in criminal law enforcement in Indonesia.

## RESULTS AND DISCUSSION

The case that is the object of research is the alleged crime of distributing electronic information containing indecency through Instagram social media which is handled by the Special Criminal Investigation Directorate of the West Kalimantan Regional Police. The case began with a police report from the victim regarding the alleged distribution of personal photos containing indecency by the victim's ex-partner through an Instagram social media account. Based on the results of the investigation, the suspect is suspected of intentionally distributing electronic information containing indecency through two Instagram accounts, namely mtransport56 and joky8159, so that investigators apply Article 45 paragraph (1) in conjunction with Article 27 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

The investigation revealed that the alleged act occurred after the victim ended her personal relationship with the suspect. The victim stated that the suspect had previously threatened to release private photos of her if their relationship ended. This threat was then realized by uploading sexually explicit photos to an Instagram account allegedly under the suspect's control. According to the victim and witnesses, the uploads were accessible to social media users, potentially exposing them to the wider public.

The investigation facts also show that investigators have carried out a series of legal actions in the form of arrests, detention, confiscation of electronic evidence, examination of witnesses, and examination of experts in the field of Electronic Information and Transactions in order to obtain sufficient evidence to prove the alleged criminal act.

The research results indicate that the evidence in this case was dominated by the use of electronic evidence. Investigators confiscated an Infinix Smart 8 mobile phone, which the suspect allegedly used to access social media accounts and upload obscene content. In addition to the electronic device, investigators also confiscated screenshots of the Instagram account, screenshots of uploaded photos of the victim, and other electronic documents related to the activity of the social media accounts.

[4]Soerjono Soekanto, Introduction to Legal Research (UI Press 2019), pp. 51–66.
[5]M. Yahya Harahap, Volume II (Sinar Grafika 2021), pp. 273–301.

In addition to the evidence obtained from the suspect, the victim also submitted several screenshots of Instagram accounts, stories, and feeds showing the distribution of sexually explicit photos. This evidence was used to demonstrate the existence of electronic information allegedly distributed to the public through electronic systems.

Witness testimony in this case came from the victim and witnesses with direct knowledge of the upload. The victim explained that the uploaded photo was a personal document previously known only to her and the suspect. The victim also stated that she never gave the suspect permission to disseminate the photo on social media. The victim admitted to experiencing psychological pressure, embarrassment, and disruption to her social and work activities as a result of the photo's distribution.

Other witnesses testified that they directly witnessed posts on an Instagram account believed to belong to the suspect. Several witnesses recognized the account as one previously used by the suspect, further strengthening the suspicion of a link between the perpetrator's digital identity and the social media account used to disseminate indecent content.

The research results indicate that investigators brought in an expert in the field of Electronic Information and Transactions to explain the technical aspects of electronic evidence. The expert explained that, from the perspective of the ITE Law, proving electronic crimes requires not only physical acts (actus reus) but also the element of intent (mens rea), which must be proven through the perpetrator's electronic activity.

The expert also explained that the distribution, transmission, and access to electronic information constitute legal acts within an electronic system. Therefore, proof of social media account activity must be linked to the electronic device, user identity, and a digital footprint demonstrating a connection between the perpetrator and the disseminated electronic information.

Based on the results of the investigation document study, investigators based the suspicion on the alleged fulfillment of the elements of "any person", "intentionally", "without right", "distributing and/or making accessible electronic information", and "content that violates morality". The fulfillment of these elements was built through a combination of evidence in the form of witness statements, electronic evidence, the results of the seizure of electronic devices, and expert testimony explaining the relationship between digital activities and the elements of the alleged crime.

Overall, the research results show that the evidentiary process in this case does not only rely on one type of evidence, but rather uses a combination of various electronic and non-electronic evidence to build a chain of evidence against the alleged distribution of immoral content via social media.

## Discussion

### 1. The Position of Electronic Evidence in the Evidence System for Criminal Acts of Disseminating Content Containing Moral Content

In this section, you will examine how electronic evidence is positioned within the evidentiary system of Indonesian criminal procedure, with the recognition of electronic information and electronic documents as valid evidence under the Electronic Information and Transactions Law. The discussion goes beyond normative aspects, but also outlines how legal developments have expanded the concept of evidence to include digital evidence such as screenshots, metadata, social media accounts, activity logs, electronic recordings, and digital devices.

In the case under investigation, investigators not only used screenshots of Instagram posts but also confiscated the suspect's cell phone, secured social media accounts, questioned witnesses, and presented an IT expert. This evidentiary pattern demonstrates that digital evidence is constructed through the interconnection of multiple pieces of evidence, forming a coherent chain of evidence, rather than a stand-alone case.

Furthermore, the analysis can be linked to M. Yahya Harahap's theory of proof and digital evidence theory, which emphasizes that electronic evidence must meet the requirements of authenticity, integrity, reliability, and traceability. Therefore, the existence of electronic evidence is not only measured by its physical form, but also by its ability to accurately depict the electronic activity carried out by the perpetrator.

**2. The Probative Power of Electronic Evidence and Expert Testimony in Cases of the Distribution of Content Containing Moral Content.**

Proving a cyber case is not sufficient simply to demonstrate that a post existed on social media. Law enforcement officials must prove that the post actually originated from the perpetrator, was made intentionally, and used an account under their control. Therefore, electronic evidence requires authentication through digital forensic examination and expert testimony.

In this case, investigators seized electronic devices allegedly used to upload the content, obtained screenshots of the uploads, and presented an IT expert who explained the relationship between the perpetrator's actions and the distribution of electronic information within the electronic system. This demonstrates that screenshots are not considered the sole evidence but are instead corroborated by the electronic devices, account identification, and expert testimony.From a legal perspective, this pattern aligns with the principle of proof, which requires a logical relationship between pieces of evidence. Expert testimony serves to explain technical aspects that cannot be assessed solely based on the judge's general knowledge, such as account ownership, electronic system activity, and the device's relationship to the upload in question. Therefore, the evidentiary value of electronic evidence increases when supported by the results of a digital forensic examination and objective expert testimony.

**3. Analysis of Fulfillment of the Elements of Article 27 Paragraph (1) in conjunction with Article 45 Paragraph (1) of the ITE Law**

This section discusses each element of a crime systematically. The element of "every person" is fulfilled because the suspect is a legal subject who can be held criminally responsible.

The element of "intentionally" was analyzed based on the suspect's sequence of actions before and after the photo was shared. According to investigative documents, there were alleged threats made to the victim before the upload, and then the threat was carried out through the distribution of the victim's private photos on her Instagram account. This sequence demonstrates a connection between the perpetrator's intent and the resulting consequences.

The "without rights" element is analyzed from the victim's lack of consent to the distribution of her private photos. The victim stated that the photos originated from private communication and were never authorized for publication.

Furthermore, the element of distributing or making accessible electronic information is analyzed based on the fact that the upload was made through a public social media account and therefore accessible to other users. Therefore, this action meets the characteristics of distributing electronic information as defined in the ITE Law.

**4. Criminal Responsibility of the Perpetrator from the Perspective of Criminal Law Theory**

Criminal liability cannot be simply based on the fact that a social media account was used to disseminate indecent content. Criminal liability must be established through proof of fault (schuld), which includes the capacity to take responsibility, intent or negligence, and the absence of justification or excuse.

In this case, the investigation revealed a suspected link between control of social media accounts, use of electronic devices, threats to the victim, and the distribution of indecent content. From the perspective of Moeljatno and Simons' theory of criminal responsibility, these facts form the basis for assessing whether or not the perpetrator is at fault. However, the

final determination of whether the elements of the crime are proven remains the court's prerogative, based on all evidence examined at trial.

This discussion can also link victim protection as part of the objectives of modern criminal law. The distribution of intimate content without consent not only violates morality but also the victim's right to privacy, dignity, and a sense of security in the digital space.

### 5. The Ideal Model of Digital Evidence in Criminal Acts of Disseminating Content Containing Moral Content

Based on the results of research and analysis, this study offers a digital evidence model that places electronic evidence as a unified evidentiary system. The model consists of five main components, namely: (1) electronic evidence in the form of electronic devices and information; (2) digital forensic examination to ensure the authenticity and integrity of data; (3) metadata and digital traces that link electronic activity to the perpetrator; (4) expert testimony explaining the technical aspects of the electronic system; and (5) witness testimony that corroborates the facts of the distribution of electronic information. These five components are then assessed jointly by the judge in accordance with the principles of evidence according to criminal procedural law.

This model demonstrates that digital evidence should not rely solely on a single type of evidence. Using screenshots without supporting metadata, device inspection, or expert testimony has the potential to raise doubts about the authenticity and linkage of the evidence to the perpetrator. Conversely, integrating all components of evidence will increase legal certainty, protect victims' rights, and guarantee the suspect's right to a fair trial.

## CONCLUSION AND SUGGESTIONS

### Conclusion

The development of information technology has driven a transformation in the Indonesian criminal law evidentiary system, particularly following the enactment of Law Number 20 of 2025 concerning the Criminal Procedure Code and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. In cases of dissemination of immoral content through social media, electronic evidence has an important position as part of the modern evidentiary system. However, electronic evidence cannot be assessed in isolation, but must be combined with other evidence in accordance with the negative evidentiary system according to the law (negative wettelijk bewijsstelsel). Thus, evidence is not sufficient based solely on the existence of screenshots or social media posts, but must be supported by electronic devices, metadata, digital traces, witness statements, and other interrelated evidence to be able to form a judge's conviction.

Expert testimony has a strategic function in proving electronic system-based crimes. Experts not only explain the technical aspects regarding the authenticity, integrity, and reliability of electronic evidence, but also provide scientific explanations regarding the relationship between digital activities, account user identities, and the fulfillment of criminal elements as regulated in Article 27 paragraph (1) in conjunction with Article 45 paragraph (1) of Law Number 1 of 2024. In the cases analyzed, expert testimony plays a role in strengthening the relationship between electronic evidence and the alleged act, so that the proof does not solely rely on visual digital evidence, but is also supported by scientific explanations that can be accounted for.

Criminal liability for perpetrators of dissemination of obscene content through social media is not solely based on ownership of a social media account, but must also be demonstrated through control of the account, use of electronic devices, a link between digital traces, and deliberate and unauthorized actions in distributing obscene electronic information. Based on the research findings, evidence that integrates electronic evidence, digital forensic examination results, metadata, expert testimony, and other evidence provides a more

comprehensive evidentiary construction, increases legal certainty, and provides more effective protection for the rights of victims and suspects in the criminal justice process. This integrated evidentiary model is a contribution of this research to the development of Indonesian criminal procedure law in facing the challenges of law enforcement in the digital era.

**Limitations**

This study is limited to normative legal research that examines the legal framework governing electronic evidence in cases involving the dissemination of indecent content through social media under Indonesian law. Although the analysis is strengthened by a case study based on investigative documents from the Directorate of Special Criminal Investigation of the West Kalimantan Regional Police, the research does not include empirical data obtained through interviews with investigators, prosecutors, judges, digital forensic experts, or victims. In addition, the study focuses on the application of Law Number 1 of 2024 concerning Information and Electronic Transactions and the relevant provisions of Indonesian criminal procedure, without conducting a comparative analysis of digital evidence frameworks in other jurisdictions. Because the legal framework on electronic evidence continues to evolve alongside technological developments, future research should incorporate empirical studies, comparative legal analysis, and evaluations of judicial decisions to assess the effectiveness and consistency of digital evidence practices in Indonesian criminal justice.

**Recommendation**

Based on the research results, there are several recommendations that can be considered in order to strengthen the digital evidence system in the criminal act of spreading immoral content through social media.

First, lawmakers need to refine the provisions regarding electronic evidence in Law Number 20 of 2025 concerning the Criminal Procedure Code and Law Number 1 of 2024 concerning Electronic Information and Transactions, particularly regarding electronic evidence authentication standards, digital forensic examination procedures, and mechanisms for guaranteeing the integrity and chain of custody of digital evidence. More detailed regulations will provide legal certainty and reduce differences in interpretation in law enforcement practices.

Second, the Indonesian National Police, particularly cybercrime investigators, need to improve their human resource capacity through ongoing education and training in digital forensics, metadata analysis, and electronic evidence handling techniques in accordance with scientific standards and applicable legal procedures. Furthermore, digital forensic laboratory facilities need to be strengthened so that the evidentiary process does not rely solely on screenshots but is supported by comprehensive and scientifically verifiable digital examination results.

Third, the Indonesian Prosecutor's Office (AGO) advises that during the process of examining case files and drafting indictments, a careful assessment of the relationship between electronic evidence, digital forensic examination results, and expert testimony is necessary. This approach is crucial to ensuring that the evidence presented in court meets the standards of proof established by criminal procedure law and fully proves each element of the crime.

Fourth, judges are expected to continue developing their capacity to understand the characteristics of electronic evidence, including its authenticity, integrity, reliability, and its relationship to other evidence. This understanding is necessary to ensure that the assessment of digital evidence remains oriented toward the pursuit of material truth, the protection of victims' rights, and the guarantee of the rights of the accused in a fair trial.

Fifth, academics need further research on digital evidence by examining the implementation of Law Number 20 of 2025 concerning the Criminal Procedure Code in various types of cybercrimes, such as the distribution of non-consensual intimate images, online fraud, digital extortion, and artificial intelligence-based crimes. Comparative research with other countries' legal systems is also crucial to generate policy recommendations that adapt to technological developments.

Overall, this study recommends the implementation of an integrated digital evidence model, one that connects electronic evidence, digital forensic findings, metadata, expert testimony, witness testimony, and other evidence into a single, unified evidentiary system. This model is expected to improve the quality of evidence, strengthen legal certainty, provide balanced protection for both victims and defendants, and support effective law enforcement against the crime of disseminating indecent content through social media in Indonesia.

**Author Contribution**

Edy Krispono conceived and designed the research, collected and analyzed legal materials and case documents, interpreted the research findings, and prepared the original manuscript. Ade Zamrah contributed to the legal analysis, literature review, methodological refinement, and critical revision of the manuscript. ZA Hoesein supervised the research, provided conceptual guidance in criminal law and legal theory, reviewed the manuscript for important intellectual content, and approved the final version for publication. All authors have read and approved the final manuscript and agree to be accountable for all aspects of the work.

**Acknowlegment**

The authors express their sincere gratitude to the Faculty of Law, Universitas Borobudur, for its academic support throughout this research. The authors also appreciate the Directorate of Special Criminal Investigation of the West Kalimantan Regional Police for providing access to investigative documents used solely for academic analysis in accordance with applicable legal and ethical standards. The constructive comments and suggestions from colleagues and anonymous reviewers are also gratefully acknowledged. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

## REFERENCES

Adami Chazawi. (2022). *Pelajaran hukum pidana*. RajaGrafindo Persada.

Ardhani Subarzah, N., Wijaya, F., & Ambarita, F. P. (2023). The probative strength of electronic evidence in money laundering crimes in Decision Number 844/Pid.Sus/2019/PN.Ptk. *Krisna Law Journal, 5*(1).

Arief, B. N. (2022). *Hukum pidana*. Citra Aditya Bakti.

Asimah, D. (2021). To overcome the constraints of evidence in the application of electronic evidence. *Peratun Law Journal, 3*(2), 97–110.

Directorate of Special Criminal Investigation, West Kalimantan Regional Police. (2025). *Summary of investigation into the alleged criminal act of disseminating indecent content through social media* (Unpublished research document).

Firmansyah, A. W. (2022). Digital evidence in the Indonesian criminal evidence system. *Amanna Gappa, 30*(2).

Harahap, M. Y. (2021). *Pembahasan permasalahan dan penerapan KUHAP: Pemeriksaan sidang pengadilan, banding, kasasi, dan peninjauan kembali*. Sinar Grafika.

Ibrahim, J. (2019). *Teori dan metodologi penelitian hukum normatif*. Bayumedia Publishing.

Iskandar, T., Mauluddin, R., & Utoyo, M. (2023). The probative strength of electronic evidence based on the Electronic Information and Transactions Law. *Lex Stricta: Journal of Legal Studies, 2*(1).

Law Number 1 of 2023 concerning the Criminal Code.

Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 20 of 2025 concerning the Criminal Procedure Code.

Law Number 48 of 2009 concerning Judicial Power.

Makarim, E. (2021). *Hukum telematika*. Rajawali Pers.

Mantik, V. L. M. T., Watulingas, R. R., & Muaja, H. S. (2022). A legal review of the position of digital evidence in cyber-crimes. *Lex Privatum, 10*(2).

Marzuki, P. M. (2021). *Penelitian hukum*. Kencana.

Mertokusumo, S. (2021). *Mengenal hukum: Suatu pengantar*. Liberty.

Moeljatno. (2021). *Asas-asas hukum pidana*. Rineka Cipta.

Saleh, R. (2021). *Perbuatan pidana dan pertanggungjawaban pidana*. Aksara Baru.

Soekanto, S. (2020). *Pengantar penelitian hukum*. UI Press.

Soroinda, D. L. (2022). The probative power of electronic evidence in criminal procedure. *Journal of Law & Development, 52*(2).

The 1945 Constitution of the Republic of Indonesia.

Tobing, Y. F., & Rahmat, D. (2025). A legal review of the authentication of electronic evidence in court. *LEX PROGRESSIUM: Journal of Legal Studies and Legal Development, 2*(1).

Yusandy, T. (2022). The position and probative power of electronic evidence in civil procedure law in Indonesia. *Jurnal Serambi Akademica, 10*(1).