



The Evidentiary Value of Digital Evidence in Deepfake Pornography Cases: A Legal Analysis of Decision No. 12/Pid.Sus/2026/PN Smg

^a Gizky Nazwa Waluyo*, ^a Hasna Afifah

^a Walisongo State Islamic University, Semarang, Indonesia

Submitted: 19-08-2026

Revised: 31-08-2026

Accepted: 26-09-2026

Published: 01-10-2026

Abstract

In 2026, the Semarang District Court adjudicated a case illustrating how artificial intelligence can be misused for criminal purposes. The defendant was found guilty of producing and disseminating more than 300 items of AI-manipulated pornographic content commonly referred to as deepfakes. This technology manipulates a person's image or video to create highly realistic yet entirely fabricated content, potentially causing victims prolonged psychological trauma and persistent social stigma. The legal complexity intensifies when such cases reach the courtroom because digital evidence is inherently susceptible to manipulation, duplication, and deletion. This article analyzes the judicial reasoning employed in assessing digital evidence and examines its evidentiary value in Decision No. 12/Pid.Sus/2026/PN Smg. The study adopts a normative juridical method using statutory, case, and conceptual approaches, with the court decision serving as the primary source of legal material and without relying on interviews or direct observation. The findings indicate that the judges adequately correlated digital evidence with witness testimony, physical evidence, and the defendant's confession through an evidentiary construction encompassing juridical, philosophical, and sociological considerations. When assessed against Debra L. Shinder's four criteria for the admissibility of electronic evidence, the digital evidence in this case satisfied the requirements of relevance and materiality, while its reliability and credibility were reinforced through consistency with other forms of evidence. However, technical authentication could not be fully assessed because the decision did not elaborate on metadata examination, hash values, digital forensic procedures, or chain-of-custody mechanisms, and no digital forensic expert was presented at trial. These findings underscore the need for regulatory harmonization and more specific legal provisions criminalizing deepfake pornography as a distinct criminal offense.

Keywords: Artificial Intelligence; Deepfake Pornography; Digital Evidence; Judicial Reasoning.

A. Introduction

The development of artificial intelligence (AI) has generated two contrasting sets of consequences. On the one hand, this technology has improved operational efficiency across various sectors, ranging from business automation to the delivery of public services. On the other hand, the same technology has also been exploited to facilitate forms of criminal conduct that were previously difficult to imagine, including deepfake pornography. Deepfake pornography refers to the manipulation of a person's photograph or video using artificial intelligence to produce content that appears authentic even though it is entirely fabricated (Noerman & Ibrahim, 2024). This technique typically involves superimposing a victim's face onto another person's body, creating content that may be extremely difficult to distinguish from genuine material.

The harmful effects of this form of crime extend beyond the content itself and affect

* ✉ Corresponding author: gizky.nazwawaluyo@gmail.com



multiple dimensions of the victim's life. Psychologically, victims may experience significant distress, while socially, the resulting stigma and reputational harm may be difficult to remedy because content disseminated in digital environments is often nearly impossible to remove completely (Hiariej, 2012). Utara and Widyawati, argue that non-consensual deepfake pornography constitutes a form of technology-facilitated gender-based violence whose consequences may be comparable in severity to those of conventional sexual violence (Utara and Widyawati, 2025). The situation is particularly concerning because virtually anyone may become a victim, as photographs and videos uploaded to social media, whether through temporary story features or regular posts, can be downloaded and manipulated without the knowledge or consent of the individual concerned (Novyanti & Astuti, 2021).

This phenomenon is concretely illustrated in Decision No. 12/Pid.Sus/2026/PN Smg, which constitutes the object of analysis in this study. The defendant, an 18-year-old university student and alumnus of SMAN 11 Semarang, obtained photographs of several former classmates from social media without their consent, altered them using artificial intelligence to create pornographic content, and subsequently uploaded the material through a publicly accessible X (formerly Twitter) account under the username @nasywamelvii. More than 300 pornographic posts were disseminated through the account, while an additional 1,100 files were stored in the defendant's private Google Drive. The victims were not limited to former students but also included teaching staff of SMAN 11 Semarang. In addition to causing trauma and humiliation to the victims, the incident also adversely affected the reputation of the school concerned.

This issue cannot be regarded merely as a local concern. In its 2022 report, Europol identified deepfakes as a serious threat to law enforcement worldwide, including in the context of image-based sexual exploitation (Europol, 2022). A systematic review conducted by Sandoval et al., further emphasized that deepfakes have the potential to undermine the integrity of evidence and judicial proceedings across jurisdictions, thereby requiring continuous development of detection methods and legal frameworks (Sandoval et al., 2024). In Indonesia, the Ministry of Communication and Digital Affairs recorded more than 233,000 items of pornographic content that were handled between October 2024 and March 2025, some of which involved artificial intelligence-based manipulation (Kemkomdigi, 2025). Deepfake pornography, therefore, is no longer merely an academic concern but has become an urgent challenge for the legal system.

The most complex aspect of this phenomenon lies in the evidentiary process. Article 183 of the Indonesian Code of Criminal Procedure (KUHAP) requires at least two legally admissible items of evidence, accompanied by the judge's conviction, as the basis for imposing a criminal sentence. This provision therefore combines formal evidentiary requirements with judicial conviction as a decisive element in criminal adjudication (Harahap, 2012). The difficulty, however, is that this evidentiary framework was formulated in a legal context still largely dominated by conventional forms of evidence, whereas digital evidence possesses characteristics that allow data to be manipulated, duplicated, transferred, or deleted within a very short period. In the Semarang District Court case, for example, the defendant's X account was no longer active when investigators conducted their examination. As a result, the relevant digital evidence could only be obtained through screenshots captured by one of the victims and by cyber-patrol officers.

From a normative perspective, Article 5(1) of the Electronic Information and Transactions Law (ITE Law) recognizes electronic information and electronic documents as an extension of legally admissible evidence. This legal status was subsequently reinforced by

Constitutional Court Decision No. 20/PUU-XIV/2016, which affirmed the position of electronic evidence within the Indonesian criminal evidentiary system (Janna & Utami, 2025). Nevertheless, the existing regulatory framework remains general in nature and does not yet fully address the evidentiary complexities arising in deepfake cases, particularly because the content presented as evidence is itself deliberately manipulated to appear authentic. According to Debra L. Shinder (Susatyo, 2023), electronic evidence must satisfy at least four requirements in order to be admissible and possess evidentiary value: it must be reliable, meaning that its dependability can be established; credible, meaning that its credibility and authenticity can be verified; relevant, meaning that it has a logical connection to the fact sought to be proven; and material, meaning that it is significant to the substantive issues of the case. The acquisition of electronic evidence must also comply with applicable law, because evidence obtained unlawfully may give rise to legal challenges concerning its use in the evidentiary process (Susatyo, 2023).

The 2024 amendment to the Electronic Information and Transactions Law (ITE Law) through Law No. 1 of 2024 has strengthened the legal recognition of electronic evidence. However, this reinforcement remains largely confined to its general admissibility and has yet to address the technical evidentiary challenges specifically associated with deepfakes, such as forensic standards for detecting AI-based manipulation and standardized procedures for verifying the authenticity of synthetic content (Noerman & Ibrahim, 2024). Sompotan, emphasizes that the artificial intelligence technologies underlying deepfakes are now capable of generating audiovisual content that is increasingly difficult to distinguish from authentic material, thereby necessitating a reassessment of the existing legal framework (Sompotan, 2026; Darmawan et al., 2025). Further argue that although Indonesia has regulations governing pornography and electronic transactions, no provision explicitly and specifically criminalizes deepfake pornography as a distinct criminal offense. This regulatory condition demonstrates that the legal challenges posed by deepfakes extend beyond determining which criminal provisions may be applied; they also concern how the integrity and evidentiary weight of digital evidence can be established before a court.

In judicial practice, these challenges surrounding digital evidence have become increasingly apparent. WhatsApp conversations, closed-circuit television (CCTV) recordings, file metadata, and other electronic records are commonly used as evidence, yet their use continues to encounter difficulties relating to authentication, chain of custody, data-seizure procedures, and the limited availability of digital forensic experts (Janna & Utami, 2025). Tanoto et al., found that although electronic evidence offers advantages in terms of efficiency and accuracy, its principal challenges remain the validity of evidence, limited technical understanding among law-enforcement officials, and divergent international standards (Tanoto et al., 2024). These difficulties become even more pronounced in deepfake cases because the content under examination is inherently manipulative and is deliberately created to resemble authentic material. Consequently, consistency between digital evidence and other forms of evidence does not necessarily establish the technical authenticity and integrity of the digital evidence itself.

A comparison with a similar case further illustrates this evidentiary problem. In Decision No. 125/Pid.Sus/2019/PN Bjn, the defendant used the FriendBlender application to superimpose the victim's face onto pornographic images and subsequently disseminated the manipulated material as a means of intimidation. The court imposed a criminal sentence under Article 29 of the ITE Law concerning threats without placing the production of manipulated pornographic images at the center of its legal reasoning (Mongkau et al., 2025).

Sompotan, characterizes the regulatory situation surrounding deepfake pornography as a *rechtsvacuum*, given the absence of a criminal provision that explicitly recognizes deepfake pornography as a distinct offense. This case is relevant as a point of comparison because it demonstrates that digitally manipulated content had already entered judicial proceedings before Decision No. 12/Pid.Sus/2026/PN Smg, although the charges and the structure of judicial reasoning differed between the two cases (Sompotan, 2026).

Previous studies demonstrate that scholarship on electronic evidence and deepfakes has developed along several distinct lines of inquiry. Qamar, examined the evidentiary weight of electronic evidence in criminal proceedings and provided an important foundation for understanding the position of electronic evidence within the criminal evidentiary system. However, the study did not specifically address the distinctive characteristics of content generated through artificial intelligence-based manipulation (Qamar, 2019). Tanoto et al., likewise analyzed the legal status and evidentiary weight of electronic evidence in criminal proceedings and emphasized the need for stronger regulation to provide digital evidence with a clearer legal position (Tanoto et al., 2024). Both studies are important in establishing the general framework of electronic evidence, yet their objects of analysis remain broad and do not examine digital evidence in a deepfake pornography case through a specific judicial decision.

Subsequent scholarship on deepfakes has largely focused on criminalization and regulatory adequacy. Noerman and Ibrahim, through normative legal research, examined the criminalization of deepfakes as a form of state protection and found that technological developments in this field have not yet been fully accommodated by Indonesian positive law (Noerman & Ibrahim, 2024; Darmawan et al., 2025). Focused on law enforcement against the misuse of deepfake technology in child pornography in the era of artificial intelligence and highlighted the limitations of the existing regulatory framework in addressing this form of crime. The central concern of both studies lies in substantive criminal law and regulatory design rather than in how judges construct and assess the evidentiary weight of digital evidence in a concrete case.

From a broader perspective, Sandoval et al., through a systematic review, identified the threats posed by deepfakes to criminal justice systems, including the potential erosion of evidentiary integrity and the difficulties faced by law-enforcement authorities in distinguishing authentic content from synthetic material (Sandoval et al., 2024). This study provides an important basis for understanding the epistemic risks that deepfakes pose to evidentiary processes. However, its scope is cross-jurisdictional and does not examine the application of Indonesian criminal evidentiary standards. Meanwhile, Utara and Widyawati situated non-consensual deepfake pornography within the context of criminal law enforcement and victim protection, but did not focus specifically on the quality, authentication, and evidentiary weight of digital evidence presented at trial (Utara and Widyawati, 2025). These differences in focus indicate that scholarship on deepfake pornography and scholarship on electronic evidence have, to a considerable extent, developed as relatively separate strands of legal discourse.

The study by Mongkau et al., is more closely related to the present research because it analyzes Decision No. 125/Pid.Sus/2019/PN Bjn, which involved the manipulation of a victim's face in pornographic content. The study highlights legal issues arising from the use of digital manipulation technology and critically examines the legal basis relied upon by the judges in that case. Nevertheless, its analysis remains primarily oriented toward law enforcement and the appropriateness of the criminal provisions applied, rather than toward

a systematic assessment of each item of digital evidence according to the criteria of reliability, credibility, relevance, and materiality. The study also does not specifically distinguish between the consistency of digital evidence with other forms of evidence and the technical authentication required to establish the integrity of the digital evidence itself (Mongkau et al., 2025).

The mapping of previous studies reveals a more specific research gap. Research on electronic evidence has generally explained its legal status and evidentiary weight, whereas studies on deepfake pornography have primarily focused on criminalization, regulatory gaps, offender liability, and victim protection. Studies based on specific judicial decisions have likewise not systematically examined how digital evidence in deepfake cases acquires evidentiary weight when assessed simultaneously against the minimum evidentiary requirements under Article 183 of the Indonesian Code of Criminal Procedure (KUHAP) and the criteria of reliability, credibility, relevance, and materiality. This gap is particularly significant because, in deepfake cases, witness testimony, physical evidence, or a defendant's confession may strengthen the factual connection of a particular item of digital evidence, yet such corroboration does not necessarily establish its technical integrity where metadata, hash values, forensic procedures, and chain-of-custody documentation are absent or inadequately recorded.

Against this background, the novelty of this study lies in its assessment of the evidentiary weight of digital evidence in a deepfake pornography case through the integration of the minimum evidentiary requirements under Article 183 KUHAP with the criteria of reliability, credibility, relevance, and materiality in Decision No. 12/Pid.Sus/2026/PN Smg, complemented by a comparative reading of the judicial reasoning in Decision No. 125/Pid.Sus/2019/PN Bjn. This novelty is not intended to formulate a new theory of evidence, but rather to systematically apply two analytical layers to digital evidence: evidentiary sufficiency under criminal procedural law and the substantive quality of electronic evidence. Through this construction, the study distinguishes corroborative support derived from consistency among different forms of evidence from the technical authentication required to assess the integrity of digital evidence more rigorously.

The principal contribution of this study is doctrinal, as it offers an analytical framework for assessing the evidentiary weight of deepfake digital evidence by linking Article 183 KUHAP with the validity criteria applicable to electronic evidence. At a practical level, the study identifies the importance of forensic authentication, metadata, hash values, chain-of-custody documentation, and the involvement of digital forensic experts in strengthening evidentiary assessment, particularly where a defendant denies any connection with the disputed content or the devices allegedly used. At the regulatory level, the findings may provide an argumentative basis for strengthening and harmonizing the provisions of KUHAP, the ITE Law, the Pornography Law, and other regulations governing the use and protection of digital data. Accordingly, the contribution of this study extends beyond recommendations concerning the criminalization of deepfake pornography and is directed more specifically toward the development of standards for assessing the evidentiary weight of digital evidence in criminal proceedings.

Based on the foregoing analysis, this study addresses two research questions. First, how did the judges assess digital evidence in Decision No. 12/Pid.Sus/2026/PN Smg? Second, to what extent does the digital evidence presented in that decision possess evidentiary weight when evaluated under the Indonesian criminal evidentiary system and the validity criteria

applicable to electronic evidence? In line with these research questions, this study aims, first, to analyze the judicial reasoning employed in assessing digital evidence in Decision No. 12/Pid.Sus/2026/PN Smg and, second, to analyze the evidentiary weight of the digital evidence in that decision based on Article 183 KUHAP and the criteria of reliability, credibility, relevance, and materiality. This formulation also ensures consistency among the research questions, research objectives, and the two principal sections of the discussion.

B. Research Methodology

This study employs a normative juridical legal research design that places legal norms, doctrines, and judicial decisions at the center of the analysis. A normative approach is adopted because the study seeks to examine the legal construction of evidentiary rules applicable to digital evidence in deepfake pornography cases and to assess their application in Semarang District Court Decision No. 12/Pid.Sus/2026/PN Smg. The study does not undertake an empirical examination of the investigation or trial process; rather, it analyzes the legally relevant facts and evidentiary process as presented in the text of the judgment. Its limitations arise from the absence of interviews with judges, public prosecutors, investigators, digital forensic experts, the defendant, or the victims, as well as from the lack of direct observation of the court proceedings. Accordingly, any assessment concerning the presence or absence of technical authentication, forensic examination, metadata analysis, hash-value verification, and chain-of-custody procedures is confined to information explicitly recorded in the judgment and the legal materials analyzed.

The legal materials used in this study consist of primary and secondary legal materials. Primary legal materials include the Indonesian Code of Criminal Procedure (KUHP), particularly Articles 183 and 184 concerning the evidentiary system and legally recognized forms of evidence; the Electronic Information and Transactions Law (ITE Law) and its amendments, including Law No. 1 of 2024, particularly provisions concerning electronic information and documents and content violating morality; Law No. 44 of 2008 on Pornography; Law No. 1 of 2023 on the Criminal Code together with Law No. 1 of 2026 on Criminal Law Adjustment; and Semarang District Court Decision No. 12/Pid.Sus/2026/PN Smg as the principal object of analysis. This decision was selected because it directly concerns the creation and dissemination of pornographic content through AI-based facial manipulation and contains several forms of digital evidence that are relevant to evidentiary analysis. Secondary legal materials include the doctrines of Andi Hamzah on criminal procedure, M. Yahya Harahap on the application of KUHP and the evidentiary system, Eddy O.S. Hiariej on evidentiary theory and law, and scholarly journal articles concerning electronic evidence, digital forensics, deepfakes, and law enforcement relating to deepfake pornography.

Legal materials were collected through library research involving the identification, inventorying, classification, and examination of statutes and regulations, judicial decisions, books, and scholarly journal articles relevant to the research problem. The search process was conducted through conventional libraries, digital libraries, and online academic journal databases, consistent with the characteristics of normative legal research, which relies primarily on documentary legal materials and secondary data (Soekanto, 2014). The collected materials were subsequently grouped into three principal categories: norms governing the criminal evidentiary system; norms and legal doctrines concerning electronic evidence; and materials specifically addressing the characteristics and evidentiary challenges of deepfake pornography. Recent literature, including publications from 2025 and 2026, was also

incorporated to capture current academic and normative developments concerning the use of artificial intelligence and digital evidence.

This study employs three principal approaches. First, the statute approach is used to identify and examine the legal norms governing the criminal evidentiary system, electronic evidence, pornography, and the use of information technology, particularly the relationship between Articles 183 and 184 of the Indonesian Code of Criminal Procedure (KUHP) and the relevant provisions of the ITE Law, the Pornography Law, and the criminal provisions applied in the case. Second, the case approach is employed to analyze Decision No. 12/Pid.Sus/2026/PN Smg by examining the legally relevant facts, admissible evidence, physical exhibits, structure of the indictment, judicial reasoning, application of the elements of the offense, and the legal basis for sentencing. The analysis covers the four alternative charges brought by the public prosecutor, namely Article 407(1) of the Criminal Code, Article 29 *juncto* Article 4(1)(d) of the Pornography Law, Article 51(1) *juncto* Article 35 of the ITE Law, and Article 45(1) *juncto* Article 27(1) of the ITE Law, including the judges' reasons for selecting the first alternative charge. Third, the conceptual approach is used to examine the concepts of material truth, the negative statutory evidentiary system, and the validity and evidentiary weight of electronic evidence as the conceptual framework for evaluating the digital evidence presented in the case.

Decision No. 125/Pid.Sus/2019/PN Bjn is used as a comparative judicial reference within the case approach and is not treated as a basis for characterizing this study as employing a separate comparative approach. The comparison serves only as an analytical enrichment technique for identifying similarities and differences in patterns of judicial reasoning concerning digital image manipulation, particularly the relationship between the nature of the conduct, digital evidence, the structure of the indictment, and the legal provisions applied. The comparison is therefore limited to relevant aspects of judicial reasoning and is not intended to constitute a comprehensive comparative study of two different legal systems or normative regimes. This position is adopted because Decision No. 12/Pid.Sus/2026/PN Smg remains the principal object of analysis, while Decision No. 125/Pid.Sus/2019/PN Bjn functions solely to enrich the analysis of the development of judicial reasoning in cases involving digitally manipulated pornographic content.

The legal materials are analyzed using a prescriptive-juridical method through legal interpretation and legal argumentation, while descriptions of facts and evidence are employed only as an initial stage for constructing the object of legal assessment. The analysis is conducted in six stages. First, the study inventories and systematizes the legal norms governing criminal evidence and electronic evidence. Second, it identifies the legally relevant facts, admissible evidence, physical exhibits, and judicial considerations contained in Decision No. 12/Pid.Sus/2026/PN Smg. Third, it constructs the relationship between each item of digital evidence and witness testimony, documentary evidence, physical exhibits, and the defendant's statement. Fourth, it assesses evidentiary sufficiency under Article 183 KUHP by determining whether at least two legally admissible forms of evidence are available to support judicial conviction, while taking into account the classification of evidence under Article 184 KUHP and the legal status of electronic evidence under the ITE Law. Fifth, it evaluates the substantive quality of digital evidence using Debra L. Shinder's criteria of reliability, credibility, relevance, and materiality (Susatyo, 2023). Sixth, it formulates legal arguments and prescriptions concerning the evidentiary weight of digital evidence, the procedural or technical weaknesses identified in the judgment, and the need to strengthen evidentiary standards for deepfake cases in the future.

The operationalization of Shinder's four parameters is applied to the digital evidence that constitutes the focus of this study, namely screenshots of AI-manipulated pornographic content, screenshots of the profile and posts associated with the X account @nasywamelvii, the victims' original photographs prior to manipulation, the Gmail account associated with the defendant, two mobile phones belonging to the defendant, and one mobile phone belonging to a victim-witness. The reliability parameter is used to assess the dependability of the source and the consistency of the evidence by examining, among other factors, the source from which the evidence was obtained, the time of documentation where recorded, the existence of comparative or corroborating evidence, and its connection with the accounts or devices under examination. The credibility parameter is used to assess support for the authenticity and integrity of the evidence by considering its provenance, acknowledgment or confirmation by relevant parties, documentation concerning the securing of the evidence, and the presence or absence of technical examination involving metadata, hash values, digital forensic procedures, and chain-of-custody documentation. The relevance parameter is used to determine the direct relationship between each item of evidence and the legally relevant facts and elements of the offense that must be proven, whereas the materiality parameter is used to assess the significance of the evidence to the substance of the case and its contribution to the overall evidentiary construction. Consistency between digital evidence and witness testimony or the defendant's confession is treated as a form of corroborative support and is not automatically equated with technical authentication of data integrity.

The results obtained from the assessment of each parameter are subsequently analyzed in conjunction with the applicable rules of criminal procedure, evidentiary doctrine, and scholarly literature on electronic evidence in order to determine the evidentiary weight of the digital evidence presented in the case. The study does not merely determine whether a particular item of evidence is formally admissible, but also evaluates the extent to which that evidence is capable of supporting the fact sought to be established. The analysis therefore distinguishes among evidentiary sufficiency under Article 183 KUHAP, the interrelationship among different forms of evidence, and issues concerning the authentication and technical integrity of electronic evidence. On the basis of these findings, the study formulates legal prescriptions concerning the need to strengthen authentication procedures, chain-of-custody documentation, the use of digital forensic examination, and the development of evidentiary standards that are better suited to the distinctive characteristics of deepfake pornography.

C. Results

C.1 Identification of Judicial Reasoning on Digital Evidence

The analysis of Decision No. 12/Pid.Sus/2026/PN Smg shows that the evidentiary construction in the deepfake pornography case was built through a combination of digital evidence, witness testimony, documentary evidence, physical exhibits, and the defendant's statement. The case originated from a cyber patrol conducted by Sub-Directorate III of the Special Criminal Investigation Directorate of the Central Java Regional Police in October 2025, which identified the dissemination of AI-generated pornographic content using the faces of several female students and teaching staff of SMAN 11 Semarang. Subsequent investigation led to the X account @nasywamelvii, which was linked to the defendant. Because the account was no longer active when the examination was conducted, part of the previously circulated content was independently documented in the form of screenshots by a victim-witness and cyber-patrol officers ([Semarang District Court, 2026](#)). This circumstance placed digital evidence in a central position in reconstructing the existence of

the content, the account used, and the defendant's connection to the digital activities forming the subject of the case.

The evidence presented at trial included 16 screenshots and digital documents consisting of AI-manipulated pornographic content, account profiles, account posts, and the victims' original photographs used for comparison. This body of evidence was supplemented by a Gmail account linked to the defendant's device, two mobile phones belonging to the defendant—an iPhone 13 Pro and an iPhone 11 Pro—and one iPhone 13 belonging to the victim-witness NP. The public prosecutor also presented nine witnesses and documentary evidence as part of the overall evidentiary construction. The screenshots produced by witness NP were recorded on 6 October 2025 at 22:07 Western Indonesian Time (WIB) and 7 October 2025 at 11:41 WIB, while cyber-patrol officers conducted separate screen captures ([Semarang District Court, 2026](#)). This evidentiary composition demonstrates that the digital evidence was not presented in isolation, but rather in conjunction with other forms of evidence and physical exhibits connected to the alleged criminal conduct.

The findings further indicate that the defendant's connection to the accounts used in the case was established through several interrelated digital facts. The account @Koko0o022 used an image of the defendant's pet cat, while a photograph of the defendant was also found in posts associated with the indecent content. The account data were then connected to devices under the defendant's control, witness testimony, and the defendant's own admission concerning account ownership and the content-creation process ([Semarang District Court, 2026](#)). This evidentiary pattern reflects the cumulative use of multiple sources of evidence to connect a digital identity with the person alleged to have committed the offense. Such an evidentiary approach is particularly relevant in deepfake cases, where identity and visual representation can be convincingly manipulated, making the relationship among digital artifacts, users, and devices an important element in identifying the perpetrator ([Hanifa et al., 2025](#); [Kurniarullah et al., 2024](#)).

The analysis of the legal construction of the judgment shows that the public prosecutor submitted four alternative charges: Article 407(1) of the Criminal Code, Article 29 *juncto* Article 4(1)(d) of the Pornography Law, Article 51(1) *juncto* Article 35 of the ITE Law, and Article 45(1) *juncto* Article 27(1) of the ITE Law. The judges selected the first alternative charge under Article 407(1) of the Criminal Code, which concerns the acts of creating, producing, and disseminating pornographic content ([Semarang District Court, 2026](#)). The element of dissemination was assessed on the basis of the public nature of the defendant's account, which allowed other users to access the content without first following the account. Within the legal construction of the judgment, artificial intelligence was treated as a means of generating pornographic content by using the victims' faces. This positioning indicates that the judgment primarily focused on the production and distribution of pornographic content rather than on the use of artificial intelligence as an independent criminal offense.

The judges also considered the consequences of the defendant's conduct for the victims. The unauthorized use of the victims' faces in manipulated pornographic content was viewed as affecting their self-image and dignity, even though the sexual acts depicted in the content had never been performed by the victims. Testimony from representatives of the school was also relied upon to demonstrate the broader social impact on the reputation of SMAN 11 Semarang ([Semarang District Court, 2026](#)). The nature of this harm is consistent with Pitaloka's, finding that non-consensual deepfake pornography may cause damage to victims' dignity and reputation ([Pitaloka, 2025](#)), while Tavadjio, associates facial and voice

manipulation with the misuse of personal identity (Tavadjio, 2025). The judges ultimately sentenced the defendant to one year of imprisonment, exceeding the public prosecutor's seven-month sentencing demand, while still recognizing the defendant's age, confession, remorse, and reconciliation with some of the victims as mitigating circumstances (Semarang District Court, 2026).

The examination of the judgment further reveals limitations in the documentation of the technical authentication of digital evidence. The decision does not describe any examination of metadata, hash values, forensic imaging, or other technical procedures for verifying the integrity of each digital object submitted as evidence. Nor does it provide a detailed account of the chain of custody from the acquisition, storage, transfer, and examination of the evidence through to its presentation at trial. No digital forensic expert testimony was identified among the evidence presented before the court (Semarang District Court, 2026). The absence of such documentation constitutes an important factual finding because electronic evidence is inherently susceptible to alteration and therefore requires particular caution in the evidentiary process (Hiariej, 2012). The evidentiary construction reflected in the judgment consequently demonstrates stronger factual interconnections among different forms of evidence than documented technical authentication grounded in digital forensic procedures.

C.2 Results of the Assessment of the Evidentiary Weight of Digital Evidence

The assessment under Article 183 of the Indonesian Code of Criminal Procedure (KUHAP) indicates that the minimum evidentiary threshold in this case was satisfied. The provision requires at least two legally admissible forms of evidence, accompanied by the judge's conviction regarding both the occurrence of the criminal offense and the defendant's culpability. In this case, the public prosecutor presented nine witnesses, documentary evidence, electronic information and documents, mobile devices, and the defendant's statement (Semarang District Court, 2026). The defense also submitted a psychological assessment report, forgiveness letters from three victims, and a written apology. Taken together, these items of evidence did not reveal any fundamental contradiction in the factual narrative relied upon by the judges in forming their conviction. This evidentiary structure is consistent with the negative statutory evidentiary system, which requires both legally admissible evidence and judicial conviction derived from such evidence (Harahap, 2012).

The assessment of the reliability parameter shows that the digital evidence received support from more than one source. Screenshots were independently obtained by victim-witness NP and cyber-patrol officers, while electronic devices under the defendant's control provided additional connections to the digital accounts under examination. The time at which several screenshots were captured was also specifically recorded in the case description (Semarang District Court, 2026). The existence of multiple sources producing mutually consistent information provides factual support for the reliability of the evidence. This characteristic is consistent with the importance of establishing connections among manipulated content, the alleged perpetrator, and the technological means used in proving deepfake-related misuse (Kurniarullah et al., 2024). Nevertheless, the technical reliability of the evidence cannot be fully established solely from the judgment because it does not provide details concerning metadata, hash values, forensic imaging, or data-preservation procedures.

The assessment of the credibility parameter similarly reveals evidentiary support for the connection between the defendant and the digital evidence presented at trial. The defendant acknowledged ownership of the relevant accounts and physical exhibits and explained the

process used to create the disputed content. These statements were consistent with the devices, account data, screenshots, and witness testimony recorded in the judgment (Semarang District Court, 2026). Such consistency among different forms of evidence provides corroborative support for the credibility of the factual connection between the defendant and the digital activities under examination. Tanoto et al., emphasize that the authenticity and evidentiary strength of electronic evidence should ideally be reinforced through mechanisms capable of ensuring data integrity (Tanoto et al., 2024). In this case, however, the technical integrity of each digital artifact cannot be fully established because the judgment does not comprehensively describe the technical authentication procedures or chain-of-custody documentation.

The assessment of the relevance parameter demonstrates a direct relationship between each item of digital evidence and the facts that had to be established. Screenshots of the pornographic content were connected to the acts of creating and producing the material, whereas screenshots of the account profile and posts were related to the act of dissemination. The victims' original photographs served as comparative material to demonstrate the use of their visual identities in the manipulated content, while the Gmail account and the defendant's devices functioned to link the digital identity associated with the relevant accounts to the defendant (Semarang District Court, 2026). These connections indicate that the evidence presented was relevant to the elements of the criminal offense forming the basis of the charges. The manipulative nature of deepfakes indeed requires a concrete nexus between digital artifacts, the alleged criminal conduct, and the individual associated with that conduct (Hanifa et al., 2025).

The materiality parameter indicates that the digital evidence was significant to the central issues of the case. The existence of AI-manipulated pornographic content, the victims' identities used in that content, the accounts employed for dissemination, the devices linked to the defendant, and the defendant's connection to the content-creation process all constituted core facts that had to be established (Semarang District Court, 2026). The digital evidence did not merely demonstrate that particular content had existed in the digital environment; it also contributed to linking the defendant to the production and dissemination of that content. The unauthorized use of the victims' identities was likewise directly related to the defining characteristics of deepfake pornography, as discussed by Pitaloka and Tavadjio. The position of this evidence therefore demonstrates that its materiality concerned the substance of the case rather than merely peripheral or supplementary facts (Pitaloka, 2025; Tavadjio, 2025).

The assessment of all four parameters reveals different levels of evidentiary support. The relevance and materiality criteria received strong support because the relationship among the digital evidence, the elements of the offense, and the central issues of the case could be directly identified. The reliability and credibility criteria, by contrast, received corroborative support from the consistency among screenshots, account data, devices, witness testimony, and the defendant's statement (Semarang District Court, 2026). Tanoto et al., indicate that the evidentiary strength of electronic evidence is closely related to its integration with other forms of evidence (Tanoto et al., 2024), while Hiariej emphasizes the need for caution in assessing electronic evidence because digital data are susceptible to alteration (Hiariej, 2012). Full verification of the technical reliability and credibility of the evidence, however, cannot be conducted on the basis of the judgment alone because metadata examination, hash-value verification, forensic imaging, and chain-of-custody documentation are not described in sufficient detail. These findings provide the basis for further distinguishing evidentiary

sufficiency under Article 183 KUHAP, corroborative support among different forms of evidence, and the technical authentication of digital evidence.

D. Discussion

D.1 Judicial Reasoning in Assessing Digital Evidence in Decision No. 12/Pid.Sus/2026/PN Smg

The case in Decision No. 12/Pid.Sus/2026/PN Smg originated from a cyber patrol conducted by Sub-Directorate III of the Special Criminal Investigation Directorate of the Central Java Regional Police in October 2025, which identified the dissemination of AI-generated pornographic content using the faces of several female students and teaching staff of SMAN 11 Semarang. The investigation led to the X account @nasywamelvii, which was linked to the defendant; however, the account was no longer active when investigators conducted their examination. Consequently, part of the previously circulated content was preserved through screenshots captured by both victim-witnesses and cyber-patrol officers. This evidentiary situation reflects a distinctive challenge in deepfake cases, as law-enforcement authorities must establish not only the existence of manipulated content but also its connection to the relevant account, devices, user identity, content-creation process, and acts of dissemination. Kurniarullah et al., demonstrate that deepfake misuse is closely associated with the manipulation of images and identity, requiring an evidentially accountable nexus between digital content and the individual alleged to have created or used it (Kurniarullah et al., 2024).

The evidentiary record described in the judgment was not limited to screenshots. The public prosecutor submitted 16 screenshots and digital documents comprising, among other materials, AI-manipulated pornographic content, account profiles, account posts, and the victims' original photographs used for comparison. These items were linked to a Gmail account associated with the defendant's mobile phone, two mobile phones belonging to the defendant—an iPhone 13 Pro and an iPhone 11 Pro—one iPhone 13 belonging to victim-witness NP, documentary evidence, and the testimony of nine witnesses. The screenshots captured by witness NP were recorded on 6 October 2025 at 22:07 WIB and 7 October 2025 at 11:41 WIB, while cyber-patrol officers separately conducted screen captures. This evidentiary configuration is significant because the digital evidence was not treated in isolation but was situated within a broader evidentiary network comprising both digital and non-digital sources.

The manner in which the judges assessed the evidence reflects a correlational model of evidentiary reasoning. The identification of the defendant as the account operator did not rely solely on a single screenshot or device but was constructed through the interrelationship of several facts, including the use of the defendant's pet cat photograph on the @Koko0o022 account, the appearance of the defendant's photograph in posts associated with indecent content, links between the digital accounts and devices under the defendant's control, witness testimony, and the defendant's admission concerning account ownership and the content-creation process. Hanifa, explain that the nature of deepfake technology enables digital identities to be obscured and visual representations to be manipulated convincingly. The use of multiple interrelated forms of evidence is therefore a relevant approach for reducing dependence on a single item of digital evidence that may be technically susceptible to reproduction or manipulation (Hanifa et al., 2025).

From a juridical perspective, the judges incorporated electronic information and documents into the evidentiary framework by linking Article 184 of the Indonesian Code of Criminal Procedure (KUHAP) with Article 5 of the ITE Law. The legally relevant facts were constructed progressively and subsequently used to assess the elements of the charged offenses. The judges selected the first alternative charge under Article 407(1) of the Criminal Code concerning the acts of creating, producing, and disseminating pornography. This choice indicates that the central focus of the judicial assessment lay in the production and distribution of pornographic content, while artificial intelligence was treated as the technological means through which such content was created. Haefani and Mulyanti argue that the development of deepfake technology poses challenges for criminal law because the distinctive nature of such conduct has not yet been fully accommodated within existing offense constructions (Haefani and Mulyanti, 2025), while Saturnus, identifies continuing issues of criminal liability when deepfake misuse is addressed within the framework of the ITE Law (Saturnus, 2026).

The judges' assessment of the element of "dissemination" was primarily linked to the public nature of the account, which enabled users to access the content without first following the account. This reasoning indicates that the judges evaluated the defendant's conduct according to the actual function of digital media as a means of distribution rather than solely on the basis of the number of individually identifiable recipients. The account profile, the form of the posts, and the accessibility of the account therefore acquired juridical relevance because they were directly connected to the conduct alleged in the indictment. In this context, digital evidence did not merely establish that particular files had once existed; it also demonstrated how the content had been positioned and made accessible within the digital public sphere.

The judicial reasoning also extended beyond the formal fulfillment of the elements of the offense. The unauthorized use of the victims' faces in pornographic content was regarded as implicating their right to their own image and their dignity. Although the depicted acts had never been performed by the victims and were entirely fabricated, the visual representations nevertheless appropriated the victims' identities to create sexualized depictions to which they had never consented. Pitaloka, demonstrates that non-consensual deepfake pornography may harm victims' dignity and reputation (Pitaloka, 2025), while Tavadjio, links facial and voice manipulation to broader concerns regarding the protection of personal identity (Tavadjio, 2025). In this case, the synthetic nature of the content did not negate its legal consequences because the harm arose precisely from the artificial association created between the victims' faces and fabricated sexual representations.

This approach is consistent with the perspective of judicial law-finding in progressive legal thought, which does not position judges merely as mechanical appliers of statutory text but also as interpreters of legal values in light of concrete circumstances (Rifai, 2010). A sociological dimension is likewise evident in the judges' consideration of the effects of the offense on the victims and on the reputation of SMAN 11 Semarang, as reflected in testimony from school representatives. Such considerations are relevant within the framework of Article 54 of the Criminal Code, which directs judges to take into account, among other matters, the offender's culpability, motives, the consequences of the offense, the circumstances of the victim, and the values of justice prevailing in society. The judges ultimately imposed a one-year term of imprisonment, exceeding the public prosecutor's seven-month sentencing demand, while still treating the defendant's age of 18 years, confession, remorse, and reconciliation with some of the victims as mitigating circumstances.

Decision No. 125/Pid.Sus/2019/PN Bjn provides a useful comparative context for examining how cases involving digitally manipulated images have been legally constructed before the courts. In the Bojonegoro case, the use of the *FriendBlender* application to superimpose the victim's face onto pornographic images was primarily framed within the context of intimidation, and the court applied Article 29 of the ITE Law (Mongkau et al., 2025). By contrast, the Semarang case involved a broader charging structure comprising four alternative legal provisions and placed the production and dissemination of pornographic content at the center of the alleged conduct. This difference reflects a divergence in the orientation of judicial reasoning. However, it is insufficient to conclude that a consistent jurisprudential development has emerged, given the limited number of comparable decisions and the differing factual configurations and charging bases of the two cases.

Regulatory limitations nevertheless remain visible in the legal construction of these cases. Situates deepfake pornography within broader concerns regarding the effectiveness of legal protection in Indonesia (Faturrachman, 2025), Paramesti et al., conceptualize it as a form of technology-facilitated gender-based violence requiring a more specific legal response (Paramesti et al., 2026), and Seveney et al., emphasize the urgency of regulating AI-based deepfake misuse in pornographic content (Seveney et al., 2025). This fragmented regulatory framework helps explain why the public prosecutor relied on several alternative legal provisions in charging the defendant. The substantive question of which criminal provision is most appropriate must, however, be distinguished from the procedural question of whether the digital evidence supporting the charge possesses sufficient evidentiary weight.

The court sentenced the defendant to one year of imprisonment, exceeding the public prosecutor's seven-month sentencing demand. Mitigating circumstances, including the defendant's age of 18 years, confession, remorse, and reconciliation with some of the victims, were nevertheless taken into account. The judges considered, however, that the reconciliation process had not fully resolved the matter because the victims continued to entrust the legal process to the court.

Compared with Decision No. 125/Pid.Sus/2019/PN Bjn, the judicial approach in the Semarang case appears more comprehensive in terms of the range of legal provisions considered. In the Bojonegoro case, the court applied Article 29 of the ITE Law concerning intimidation without placing the pornographic nature of the manipulated content at the center of its legal reasoning (Mongkau et al., 2025). In the Semarang case, by contrast, the public prosecutor formulated four alternative charges and the judges selected the provision considered most consistent with the proven conduct. Even so, this comparison remains too limited to establish a uniform pattern of judicial decision-making, as only a small number of decisions are being considered.

A particularly important issue is that the judicial reasoning did not address the technical authentication of the digital evidence in any substantial detail. The judgment does not describe metadata examination, data-integrity verification codes, or digital forensic procedures applied to the seized devices. Chain-of-custody procedures were likewise not discussed adequately, even though some screenshots had been obtained by a victim-witness before investigators became involved. Nor was digital forensic expert testimony presented at trial, despite the fact that electronic evidence, because of its susceptibility to alteration, requires heightened evidentiary caution (Hiariej, 2012). The absence of such expert testimony may have resulted from the prosecution's decision not to present a forensic expert, while the defendant's admission of the conduct without substantive objection may have been regarded by the judges as sufficient, when considered together with the other evidence, to form judicial

conviction. Under the negative statutory evidentiary system, judicial conviction derived from the consistency of legally admissible evidence remains a decisive element (Harahap, 2012). Nevertheless, from the perspective of strengthening future standards for digital evidence, the absence of technical verification remains an evidentiary vulnerability that should be anticipated, particularly in cases involving uncooperative defendants or explicit denials of involvement.

The case originated from a cyber patrol conducted by Sub-Directorate III of the Special Criminal Investigation Directorate of the Central Java Regional Police in October 2025, which identified the dissemination of AI-generated pornographic content using the faces of several female students and teachers from SMAN 11 Semarang. The investigation subsequently led to the X account @nasywamelvii, which was operated by the defendant; however, the account was no longer active when investigators conducted their examination. As a result, part of the content was obtained through screenshots that were later introduced as evidence at trial. Kurniarullah et al., explain that deepfake misuse may develop into criminal conduct involving the manipulation of images and personal identity. This circumstance placed digital evidence in a significant position in linking the defendant to the account, the content, and the conduct alleged in the indictment. The evidentiary process in this case therefore concerned not only the existence of the content itself but also the defendant's connection to its creation and dissemination (Kurniarullah et al., 2024).

The evidence presented at trial consisted of 16 screenshots and digital documents, a Gmail account linked to the defendant's mobile phone, documentary evidence, physical exhibits comprising two mobile phones belonging to the defendant and one mobile phone belonging to a victim-witness, and the testimony of nine witnesses. The screenshots captured by witness NP on 6 October 2025 at 22:07 WIB and 7 October 2025 at 11:41 WIB were particularly significant because they documented the existence of the content before the account became inaccessible. Cyber-patrol officers also conducted separate screen captures, thereby providing an additional source of digital evidence that could be compared with the screenshots obtained by the witness. The consistency between the digital evidence and other forms of evidence strengthened the evidentiary construction relied upon by the judges. Tanoto et al., emphasize that the evidentiary weight of electronic evidence in criminal proceedings is closely related to its interconnection with other forms of evidence (Tanoto et al., 2024). In this case, the judges did not assess the screenshots in isolation but considered them in conjunction with physical exhibits, witness testimony, and the defendant's statement.

The identification of the defendant as the operator of the relevant accounts was based on several interrelated evidentiary indicators. The @Koko0o022 account, which displayed a photograph of the defendant's pet cat, together with photographs of the defendant appearing in posts associated with indecent content, served as digital indicators linking the defendant to the activities conducted through those accounts. Witness testimony and the defendant's admission subsequently reinforced the connection between the defendant and the accounts used. The admission did not constitute the sole evidentiary basis but instead provided corroborative support for other evidence that was already mutually consistent. Hanifa, explain that proving deepfake-related offenses is particularly challenging because digital identities may be concealed and manipulated content can be created convincingly (Hanifa et al., 2025). This circumstance underscores the importance of relying on multiple forms of evidence cumulatively to establish the connection between the defendant's identity and the relevant digital activities. The judicial reasoning in this case reflects an effort to establish such a connection through the convergence of different forms of evidence.

From a juridical perspective, the judges based their assessment of the evidence on Article 184 of the Indonesian Code of Criminal Procedure (KUHP) *juncto* Article 5 of the ITE Law. The legally relevant facts were constructed progressively and linked to the elements of the offenses charged. The first alternative charge selected by the judges was Article 407(1) of the new Criminal Code concerning the acts of creating, producing, and disseminating pornography. This choice indicates that the judges treated the production and dissemination of pornographic content as the core of the defendant's conduct, while artificial intelligence was regarded as the technological means used to facilitate that conduct. Haefani and Mulyanti argue that the development of deepfake technology has created a need for criminal law reform because the distinctive characteristics of such conduct have not yet been fully accommodated by existing criminal provisions (Haefani and Mulyanti, 2025). Saturnus, likewise identifies continuing issues of criminal liability when deepfake misuse is addressed through the ITE Law. In this case, the element of "dissemination" was considered fulfilled because the defendant's account was publicly accessible (Saturnus, 2026).

The judicial reasoning was not limited to determining whether the formal elements of the offense had been satisfied but also took into account the consequences of the defendant's conduct for the victims. The unauthorized use of the victims' faces in manipulated pornographic content placed them in sexualized representations that they had neither performed nor consented to. Pitaloka, explains that non-consensual deepfake pornography may cause harm to victims' dignity and reputation (Pitaloka, 2025). Tavadjio, similarly links facial and voice manipulation to broader concerns regarding the protection of personal identity (Tavadjio, 2025). The judges' consideration of the victims' right to their own image and dignity demonstrates that the use of technology did not diminish the legal significance of the harm suffered by the victims. The impact on the reputation of SMAN 11 Semarang was also considered on the basis of testimony from school representatives. These considerations indicate that the judges addressed both the individual and social dimensions of the defendant's conduct.

The case also illustrates the limitations of the existing legal framework in addressing deepfake pornography. Muhammad Faturrachman explains that the handling of deepfake pornography in Indonesia is closely related to issues of rights protection and the effectiveness of law enforcement (Faturrachman, 2025). Paramesti et al., characterize deepfakes as a form of technology-facilitated gender-based violence that requires a more specific legal response (Paramesti et al., 2026). Seveney et al., likewise emphasize the urgency of regulating the misuse of AI-based deepfakes in pornographic content (Seveney et al., 2025). This regulatory context may help explain the use of multiple alternative charges in the present case. A comparison with Decision No. 125/Pid.Sus/2019/PN Bjn indicates that the Semarang case involved a broader charging structure encompassing several criminal provisions. However, this comparison remains insufficient to establish a consistent jurisprudential pattern because the number of decisions examined is still limited.

The judicial reasoning nevertheless reveals limitations in relation to the technical authentication of digital evidence. The judgment does not adequately describe metadata examination, data-authenticity verification codes, digital forensic procedures, or chain-of-custody documentation. The absence of digital forensic expert testimony also meant that the technical aspects of the content-manipulation process were not examined in substantial depth. Nurwahid et al., explain that the capacity of deepfake technology to manipulate images, audio, and video requires more adaptive identification methods within law-enforcement processes (Nurwahid et al., 2026).

These limitations do not necessarily negate the evidentiary weight of the digital evidence in the present case because the digital materials remained consistent with witness testimony, physical exhibits, and the defendant's admission. The evidentiary strength of the case was therefore derived primarily from the interrelationship and corroboration among different forms of evidence rather than from documented forensic authentication of the digital materials themselves. Nevertheless, technical authentication standards should be strengthened in future deepfake cases, particularly where defendants deny the alleged conduct, challenge their connection to the relevant accounts or devices, or dispute the authenticity and integrity of the digital evidence.

D.2 Evidentiary Weight of Digital Evidence in Decision No. 12/Pid.Sus/2026/PN Smg

The assessment of the evidentiary weight of digital evidence in this study is grounded in criminal procedural evidentiary theory and employs two principal parameters: the minimum evidentiary requirement under Article 183 of the Indonesian Code of Criminal Procedure (KUHAP) and Debra L. Shinder's criteria for the validity of electronic evidence.

Article 183 KUHAP adopts a negative statutory evidentiary system, under which judges must rely on forms of evidence recognized by law while also forming their own conviction on the basis of such evidence (Harahap, 2012). From a quantitative perspective, the minimum evidentiary threshold was clearly satisfied in this case. The public prosecutor presented the sworn testimony of nine witnesses, documentary evidence, electronic evidence in the form of screenshots and a Gmail account, and the defendant's statement admitting the conduct in question. The defense also submitted documentary materials consisting of a psychological assessment report, forgiveness letters from three victims, and a written apology. These items of evidence were mutually consistent and did not reveal any fundamental contradiction. Tanoto et al., emphasize that the evidentiary strength of electronic evidence depends substantially on its integration with other forms of evidence rather than on its operation in isolation, and such integration was present in this case (Tanoto et al., 2024).

Nevertheless, evidentiary weight cannot be assessed solely in quantitative terms; the quality of digital evidence must also be examined through more substantive criteria. In terms of reliability, the digital evidence received relatively strong support because the screenshots were obtained from two independent sources: victim-witness NP, who documented the content using a device and at clearly recorded times, and cyber-patrol officers, who conducted separate screen captures. The defendant's seized mobile phone also established a direct correlation between the physical device and the relevant digital account because the Gmail account linked to the device was the same account used to create the X account @nasywamelvii. In terms of credibility, the authenticity of the evidence was further supported by the defendant's acknowledgment of the exhibits presented at trial and by the defendant's explanation of the technical process used to create the content. Although the authenticity of electronic evidence should ideally be established through standardized forensic examination Tanoto et al., the defendant's admission strengthened the factual connection between the defendant and the digital evidence presented. Such an admission, however, does not replace the need for technical authentication where the authenticity or integrity of the evidence is disputed (Tanoto et al., 2024).

In terms of relevance, each item of digital evidence was directly connected to the elements of the charges. Screenshots of the pornographic content were related to the acts of

“creating and producing,” screenshots of the publicly accessible account profile were relevant to the element of “dissemination,” the victims’ original photographs served as comparative material demonstrating the manipulation process, and the linked Gmail account connected the defendant to the account used in the alleged conduct. In terms of materiality, the digital evidence addressed the core issues of the case and contributed directly to the overall evidentiary construction without generating substantial contradiction. The digital evidence therefore substantially satisfied the criteria of relevance and materiality, while its reliability and credibility were reinforced through consistency with witness testimony, physical exhibits, and the defendant’s statement. However, technical authenticity could not be assessed comprehensively because the judgment does not describe metadata examination, data-authenticity verification codes, chain-of-custody documentation, or digital forensic examination.

Although the digital evidence in this case was strengthened through its consistency with other forms of evidence, weaknesses remain from the perspective of evidentiary theory, particularly regarding technical authentication. No digital forensic expert testimony was presented at trial, meaning that technical verification that the content had been generated through AI-based manipulation relied primarily on the defendant’s admission and witness testimony (Hiariej, 2012). The absence of detailed chain-of-custody documentation also means that the acquisition, control, transfer, storage, and examination of the digital evidence from the time it was first obtained until its presentation at trial cannot be fully reconstructed, particularly because the principal screenshots were initially captured by a victim-witness before investigators became involved. In the present case, these weaknesses were partly mitigated by the defendant’s cooperative attitude and the absence of objections to the exhibits presented. However, in future deepfake cases where defendants deny the alleged conduct or challenge the authenticity of the evidence, the absence of standardized forensic procedures may constitute a significant evidentiary vulnerability. The evidentiary foundation would be considerably stronger if supported by independent forensic verification and systematically documented evidence-preservation procedures.

There is also a significant issue concerning the legal basis applied in the case. Article 407(1) of the new Criminal Code, which formed the basis of the first alternative charge, constitutes a general provision on pornography rather than a specific provision addressing deepfakes. The absence of specific regulation has compelled law-enforcement authorities to combine provisions from several different statutes, a situation that Sompotan and (Kartadinata, 2026) identify as contributing to legal uncertainty. Likewise emphasize that such regulatory limitations complicate the prosecution and proof of deepfake-related offenses before the courts (Darmawan et al., 2025). Greater harmonization among KUHAP, the ITE Law, the Pornography Law, and the Personal Data Protection Law is therefore necessary to avoid fragmented standards for the assessment of digital evidence (Janna & Utami, 2025).

The evidentiary weight of the digital evidence in this case may first be assessed under the negative statutory evidentiary system established by Article 183 KUHAP. Harahap explains that judges may not rely solely on the formal existence of legally recognized evidence but must also form a conviction regarding the defendant’s guilt on the basis of such evidence. Quantitatively, the minimum evidentiary requirement was satisfied through the testimony of nine witnesses, documentary evidence, electronic evidence, physical exhibits, and the defendant’s statement. These forms of evidence were mutually consistent and did not reveal any contradiction capable of materially undermining the evidentiary construction. Tanoto et

al., identify the integration of electronic evidence with other forms of evidence as an important factor in determining evidentiary weight. These circumstances indicate that the digital evidence in the *a quo* case satisfied the minimum evidentiary foundation required to support judicial conviction (Tanoto et al., 2024).

The assessment of digital evidence, however, cannot stop at the number of evidentiary items presented and must also address their quality and distinctive characteristics. Debra L. Shinder's criteria of reliability, credibility, relevance, and materiality provide a framework for evaluating evidentiary strength at a more substantive level. The reliability dimension is reflected in the existence of two independent sources of screenshots, namely victim-witness NP and cyber-patrol officers, who documented the content at different times and under different circumstances. The presence of the defendant's mobile phones and the Gmail account linked to those devices further strengthened the factual connection between the digital evidence and the defendant. Kurniarullah et al., explain that the distinctive characteristics of deepfakes require the evidentiary process to establish a clear nexus among manipulated content, the alleged perpetrator, and the technological means employed. In this case, the digital evidence demonstrates a sufficiently strong factual connection to the sequence of events alleged in the indictment (Kurniarullah et al., 2024).

The credibility dimension is reflected in the consistency between the digital evidence and the defendant's statement acknowledging the physical exhibits and explaining the content-creation process. This admission had corroborative value because it was given in conjunction with electronic evidence and physical exhibits already presented at trial. Nevertheless, the authenticity of the evidence remains open to question from a technical perspective because the judgment does not describe any in-depth forensic examination. Tanoto et al., emphasize that the authenticity of electronic evidence should ideally be reinforced through procedures capable of verifying data integrity (Tanoto et al., 2024). The circumstances of this case therefore indicate that the credibility of the evidence was established primarily through consistency among different forms of evidence and the defendant's cooperative acknowledgment rather than through documented technical authentication. Its evidentiary value nevertheless remained significant insofar as the overall body of evidence was sufficient to form the judges' conviction regarding the defendant's involvement.

The relevance dimension can be identified through the direct relationship between each item of digital evidence and the elements of the charged offense. Screenshots of the pornographic content were connected to the acts of creating and producing the material, whereas screenshots of the publicly accessible account profile were related to the act of dissemination. The victims' original photographs were used as comparative material against the manipulated content and therefore served to demonstrate the use of the victims' visual identities. The Gmail account linked to the defendant's device further connected the relevant digital identity to the defendant as the account user. This relevance is particularly significant because deepfake technology can generate visual representations that do not correspond to actual events. Hanifa, argue that the manipulative nature of deepfakes creates evidentiary challenges that require law-enforcement authorities to establish a concrete connection between digital evidence and the alleged criminal conduct. The digital evidence in this case therefore demonstrates strong relevance to the facts that had to be established (Hanifa et al., 2025).

The materiality dimension was likewise satisfied because the digital evidence related directly to the central issues of the case and contributed to proving the elements of the charges. Its material significance is reflected in the function of each item of evidence in establishing the existence of the content, the identities of the victims, the accounts used, and the defendant's connection to the alleged conduct. Pitaloka, explains that the misuse of non-consensual deepfake pornography not only produces manipulated content but also raises legal concerns because victims' identities are used without consent (Pitaloka, 2025). Tavadjio, similarly characterizes facial and voice falsification as a form of identity misuse capable of producing legal consequences for victims (Tavadjio, 2025). The digital evidence in this case therefore possesses material value because it did not merely establish the existence of particular content but also supported proof of the criminal conduct and its consequences for the victims. Considered together, the four parameters substantively indicate that the digital evidence possessed sufficient evidentiary weight in the case under examination.

This evidentiary strength nevertheless remains subject to limitations concerning technical authentication and chain of custody. The judgment does not describe metadata examination, data-authenticity verification codes, forensic examination of the devices, or procedures for securing and preserving the evidence from the time it was first obtained until its presentation at trial. The absence of digital forensic expert testimony also meant that the process of technically establishing that the content had in fact been generated through artificial intelligence manipulation was not explained in sufficient depth. Nurwahid et al., demonstrate that the capacity of deepfake technology to manipulate images, audio, and video requires identification mechanisms capable of distinguishing authentic material from synthetically generated content. In the present case, these weaknesses were partly mitigated by the defendant's admission and the consistency of the other evidence. The evidentiary position could, however, be materially different where a defendant denies the alleged conduct or challenges the authenticity of the digital evidence (Nurwahid et al., 2026).

These authentication concerns are also related to the absence of a specific legal framework governing the evidentiary treatment of deepfakes. Haefani and Mulyanti argue that the development of deepfake pornography requires criminal law reform because the existing provisions do not fully accommodate the distinctive characteristics of the conduct involved (Haefani and Mulyanti, 2025). Seveney et al., likewise emphasize the urgency of specific regulation addressing the misuse of deepfakes in pornographic content (Seveney et al., 2025), while Faturrachman links the issue to the need to strengthen legal protection for victims (Faturrachman, 2025). Paramesti et al., situate the problem within the broader framework of technology-facilitated gender-based violence requiring a more specific legal response (Paramesti et al., 2026). Saturnus, further demonstrates that reliance on the ITE Law in deepfake-related cases may create difficulties in determining the appropriate form of criminal liability (Saturnus, 2026). The current legal framework, which remains dispersed across KUHAP, the ITE Law, the Pornography Law, and the Personal Data Protection Law, therefore points to the need for more integrated evidentiary standards. Such strengthening is necessary so that the evidentiary weight of digital evidence in deepfake cases is not based solely on consistency among different forms of evidence, but is also supported by technically verifiable authentication and legally accountable evidence-preservation procedures.

1. Fulfilment of the Minimum Evidentiary Requirement under Article 183 KUHAP

The assessment of the evidentiary weight of digital evidence must first be situated within the negative statutory evidentiary system. Article 183 of the Indonesian Code of Criminal Procedure (KUHAP) provides that a judge may impose a criminal sentence only when at

least two legally admissible forms of evidence give rise to the conviction that a criminal offense has actually occurred and that the defendant is responsible for committing it. Harahap explains that this system combines an objective element, namely evidence prescribed by law, with a subjective element in the form of judicial conviction that must be derived from such evidence. The mere quantity of evidence is therefore insufficient where the evidence lacks a logical connection to the offense and the defendant.

In the *a quo* case, the minimum evidentiary requirement was not quantitatively dependent on digital evidence alone. The public prosecutor presented the sworn testimony of nine witnesses, documentary evidence, electronic information and documents in the form of screenshots and account data, physical exhibits consisting of mobile devices, and the defendant's statement. The defense also submitted a psychological assessment report, forgiveness letters from three victims, and a written apology. Taken together, these materials constituted multiple sources of evidence and revealed no fundamental contradiction in the factual narrative set out in the judgment. The principal issue in this case was therefore not the insufficiency of the number of evidentiary items, but the quality of the relationship between the digital evidence and the facts sought to be established.

Tanoto et al., emphasize that the evidentiary strength of electronic evidence in criminal proceedings depends on its integration with other forms of evidence (Tanoto et al., 2024). This principle is reflected in the present case, where screenshots were not used as the sole basis for identifying the defendant. Witness testimony, devices under the defendant's control, account data, comparative photographs, and the defendant's admission collectively reinforced the conclusion regarding control of the relevant accounts and involvement in the creation and dissemination of the content. The defendant's admission therefore functioned as corroborative evidence supporting the broader evidentiary record rather than as a substitute for the prosecution's obligation to establish the case.

This evidentiary construction is important because minimum evidentiary sufficiency must be distinguished from the technical integrity of digital evidence. Article 183 KUHAP may be satisfied through the existence of multiple legally admissible forms of evidence and judicial conviction arising from their interrelationship, but satisfaction of that threshold does not in itself establish that every digital object has undergone complete forensic authentication. The minimum evidentiary requirement addresses whether the overall body of evidence is sufficient to support a criminal conviction, whereas the assessment of reliability and authenticity concerns the qualitative strength of each digital item forming part of that evidentiary construction.

In this case, the judges had a relatively strong basis for linking the defendant to the alleged conduct because the digital evidence was supported by other independent forms of evidence. That conclusion, however, should not be extended into a finding that all technical aspects of the digital evidence were conclusively established. It is precisely at this point that the criteria of reliability, credibility, relevance, and materiality become necessary to distinguish the corroborative strength of the evidence from technical assurance regarding its integrity.

2. Assessment of Digital Evidence Based on the Parameters of Reliability, Credibility, Relevance, and Materiality

The assessment of the quality of digital evidence in this study employs Debra L. Shinder's four parameters (Susatyo, 2023): reliability, credibility, relevance, and materiality. These parameters are not treated as a single set of requirements that is automatically satisfied

merely because the defendant admitted the conduct. Each addresses a distinct evidentiary dimension. reliability concerns the dependability of the source and the manner in which the evidence was handled; credibility concerns support for its authenticity and integrity; relevance assesses the relationship between the evidence and the facts to be established; and materiality evaluates its significance to the central issues of the case.

With respect to reliability, several circumstances provide support for the dependability of the evidence. The screenshots were not obtained from a single source but were independently documented by victim-witness NP and cyber-patrol officers. The times at which the witness captured the screenshots were also specifically recorded in the factual account of the case. In addition, physical devices and digital accounts were used to establish a connection between the defendant and the online activities under examination. Kurniarullah et al., emphasize the importance of establishing a nexus among manipulated content, the alleged perpetrator, and the technological means used in proving deepfake-related misuse. Taken together, these circumstances provide corroborative support for the reliability of the evidence, particularly because multiple sources produced information that pointed in a consistent evidentiary direction (Kurniarullah et al., 2024).

Such corroborative support, however, is not equivalent to full proof of technical reliability. The judgment does not explain whether the screenshots were examined through metadata analysis, whether forensic imaging was conducted on the devices, whether digital copies were verified using hash values, or how the evidence was stored and transferred from the time it was first obtained. It is therefore more accurate to conclude that the reliability of the evidence received strong factual support from consistency among different forms of evidence, while its technical integrity cannot be fully verified solely on the basis of the judgment.

A similar pattern applies to the credibility parameter. The defendant's acknowledgment of account ownership, the physical exhibits, and the process used to create the content strengthened the credibility of the connection between the defendant and the digital evidence presented. Witness testimony and the existence of the devices also provided external support for that account. Tanoto et al., emphasize that the authenticity of electronic evidence should ideally be supported by mechanisms capable of ensuring its integrity (Tanoto et al., 2024). The defendant's admission therefore performed an important corroborative function, but it cannot be treated as a substitute for technical authentication where the authenticity or integrity of the evidence is contested.

In deepfake cases, the concept of authenticity must also be used with greater precision because it involves two distinct layers. The first concerns the authenticity of the digital evidence as an evidentiary object: whether the screenshots, accounts, files, and data presented genuinely represent the digital conditions existing at the relevant time and whether they remained materially unaltered during the handling process. The second concerns the authenticity of the visual representation itself: whether the image depicts an actual event or is instead a manipulated construction. In deepfake pornography, the second layer is intentionally inauthentic because the content is fabricated. This, however, does not prevent the digital object itself from functioning as evidence. What must be established is that the evidence presented constitutes a trustworthy representation of the manipulated content that was created or disseminated and that it can be connected to the defendant. Nurwahid et al., demonstrate that the capacity of deepfake technology to manipulate images, audio, and video makes technical identification mechanisms increasingly important in law-enforcement processes (Nurwahid et al., 2026).

The relevance parameter presents a stronger evidentiary position. Screenshots of the pornographic content were directly related to the acts of creating or producing the material at issue. Screenshots of the public account profile and posts were connected to the element of dissemination. The victims' original photographs provided a comparative basis for demonstrating the use of their visual identities in the manipulated content, while the Gmail account and the defendant's devices served to link the relevant digital identity to the defendant. Hanifa, emphasize that the manipulative nature of deepfakes requires law-enforcement authorities to establish a concrete connection between digital artifacts and the alleged criminal event. The direct relationship between these evidentiary objects and the elements of the offense indicates that the relevance criterion was relatively well supported (Hanifa et al., 2025).

The materiality parameter likewise received adequate support. The digital evidence was not peripheral to the case but concerned the core facts that had to be established, including the existence of manipulated pornographic content, the identities used in that content, the accounts employed for distribution, and the defendant's connection to the creation and dissemination process. Pitaloka, explains that the misuse of non-consensual deepfake pornography raises legal concerns because victims' identities are used without consent (Pitaloka, 2025), while Tavadjio characterizes facial and voice manipulation as forms of identity misuse capable of producing legal consequences for victims (Tavadjio, 2025). The evidence therefore bore direct significance to the central issues of the case, indicating that the materiality criterion was also relatively well supported.

The assessment of all four parameters leads to a more qualified conclusion than the study's initial formulation. relevance and materiality were relatively well established because the connection between the digital evidence, the elements of the offense, and the core issues of the case could be demonstrated concretely. reliability and credibility, by contrast, received substantial corroborative support from the consistency among screenshots, devices, account data, witness testimony, and the defendant's admission, while their technical integrity could not be fully verified on the basis of the judgment alone. This distinction avoids conflating evidentiary corroboration derived from consistency among different forms of evidence with digital authentication established through forensic examination.

3. Weaknesses in Technical Authentication, Chain of Custody, and Their Legal Implications

The principal limitation in the evidentiary construction of Decision No. 12/Pid.Sus/2026/PN Smg lies in the limited discussion of technical authentication. The judgment does not describe metadata examination, hash-value verification, forensic imaging, file-integrity verification methods, or detailed procedures governing the preservation and transfer of digital evidence. Nor does it indicate the presence of a digital forensic expert who explained the process of identifying synthetic content or assessing the integrity of the relevant digital artifacts. Hiariej cautions that the susceptibility of electronic evidence to alteration requires a higher degree of evidentiary caution than forms of evidence whose physical characteristics are more readily observable (Hiariej, 2012).

The absence of a detailed chain-of-custody account is particularly significant because some screenshots were captured by a victim-witness before the evidence came under the formal control of investigators. In the context of digital evidence, chain of custody should not merely identify who possessed the evidence. It should also enable the reconstruction of when and from what source the evidence was obtained, how it was copied, who exercised

control over it, how it was stored, whether it was transferred or analyzed, and how the integrity of the originally acquired data was preserved in relation to the evidence ultimately presented at trial. Without such documentation, those assessing the evidence lack a complete technical basis for auditing whether the digital artifact presented before the court remained materially identical to the artifact initially obtained.

An incomplete chain-of-custody account in the judgment cannot, however, automatically be equated with the invalidity of all digital evidence. In the present case, the evidence was admitted and incorporated into the evidentiary construction, the defendant was not recorded as challenging its authenticity, and its contents were supported by witness testimony, physical devices, account data, and the defendant's admission. Under these circumstances, weaknesses in chain-of-custody documentation more directly affect the weight of evidence, particularly the degree of confidence that may be placed in the technical reliability and credibility of the evidence, rather than automatically eliminating its admissibility.

The distinction between admissibility and weight of evidence is therefore essential to maintaining analytical consistency. admissibility concerns whether a particular item of evidence may legally be used in the evidentiary process, whereas weight of evidence concerns the degree of persuasive force or evidentiary strength that the evidence carries in forming judicial conviction. The absence of metadata analysis or hash-value verification does not, by itself, establish that the evidence was unlawfully obtained. Based solely on the text of the judgment, there is insufficient basis to conclude that the screenshots or other digital evidence should have been excluded entirely. Rather, the inability to demonstrate technically documented preservation and integrity reduces the basis for assigning maximum evidentiary weight to such evidence when considered in isolation.

The issue may shift from weight of evidence to admissibility where defects in the acquisition or handling process indicate that the evidence was obtained unlawfully, did not originate from the claimed source, or suffered such a fundamental break in integrity that the object presented at trial can no longer be reliably connected to the object initially obtained. This distinction is consistent with the importance of the lawful acquisition of electronic evidence, an issue also addressed in Constitutional Court Decision No. 20/PUU-XIV/2016. Chain of custody therefore serves two functions: it operates as a mechanism for preserving evidentiary weight and reliability, while in certain circumstances serious defects may also raise admissibility concerns where they affect the legality of acquisition or the fundamental authenticity of the digital object.

In the *a quo* case, the technical weaknesses were partly offset by corroborative support. Screenshots from two different sources, the defendant's devices, the linkage among relevant accounts, the testimony of nine witnesses, and the defendant's admission meant that the digital evidence did not stand in isolation. Harahap emphasizes that, under the negative statutory evidentiary system, judicial conviction must be derived from legally admissible forms of evidence that mutually reinforce one another. This consistency helps explain how the judges were able to form a conviction regarding the defendant's conduct despite the limited description of forensic authentication in the judgment.

Nevertheless, corroborative support cannot be treated as a permanent substitute for technical authentication. In cases where a defendant denies ownership of an account, disputes control of a device, alleges that screenshots have been manipulated, or rejects the allegation that the content was created using the seized devices, simple consistency among

testimonial and documentary sources may no longer be sufficient. In such circumstances, metadata, hash values, forensic images of devices, access logs, account histories, and chain-of-custody documentation become considerably more important in distinguishing authentic evidence from artifacts that may have been altered. The absence of digital forensic expert testimony in the present case likewise does not automatically invalidate the evidentiary process, but it limits the judgment's ability to provide independent technical justification concerning the creation, provenance, and integrity of the disputed content.

The distinctive characteristics of deepfakes further reinforce the need for this distinction. In conventional criminal cases, authentication generally focuses on whether the evidence genuinely originates from the source claimed. In deepfake cases, however, law-enforcement authorities must additionally establish that the digital object presented is authentic as an evidentiary artifact even though the visual content contained within it is synthetic. Nurwahid et al., demonstrate that the capacity of artificial intelligence to manipulate images, audio, and video requires more adaptive identification methods (Nurwahid et al., 2026). Digital forensic examination is therefore necessary not merely to determine whether a photograph is “real” or “fake,” but also to establish that the artifact under examination is the same artifact originally discovered, has not undergone material alteration during handling, and maintains a technically verifiable connection to the account or device associated with the alleged perpetrator.

Weaknesses in authentication also cannot be separated from the fragmentation of the existing regulatory framework. Article 407(1) of the Criminal Code, applied in the first alternative charge, is a general provision concerning pornography rather than a provision specifically designed to address deepfakes. Sompotan and (Kartadinata, 2026) identify regulatory gaps or uncertainty in responding to the distinctive characteristics of deepfake-related offenses. Likewise emphasize that regulatory limitations may complicate law-enforcement efforts in addressing deepfake misuse, while Janna and Utami underline the need to harmonize the regulation of electronic evidence within the criminal justice system (Darmawan et al., 2025; Janna and Utami, 2025).

These issues demonstrate that legal reform cannot be limited to the creation of a specific offense criminalizing deepfake pornography. Haefani and Mulyanti emphasize the urgency of criminal law reform in responding to deepfakes (Haefani and Mulyanti, 2025); Seveney et al., advocate more specific regulation of deepfake misuse in pornographic content (Seveney et al., 2025); Faturrachman associates the issue with the need to strengthen victim protection (Faturrachman, 2025); and Paramesti et al., conceptualize it as part of technology-facilitated gender-based violence requiring a specific legal response (Paramesti et al., 2026). Saturnus, further identifies difficulties in determining criminal liability when deepfake misuse is addressed within the framework of the ITE Law (Saturnus, 2026). Taken together, these concerns indicate that reform of substantive criminal law should proceed alongside the development of more rigorous standards for digital evidence.

Decision No. 12/Pid.Sus/2026/PN Smg demonstrates a relatively strong evidentiary construction in terms of the interrelationship among different forms of evidence and the satisfaction of the minimum evidentiary requirement under Article 183 KUHAP. However, the judgment does not provide sufficient documentation to establish that the technical integrity of each item of digital evidence was fully verified. The relevance and materiality of the evidence were relatively well established, whereas its reliability and credibility received substantial corroborative support without being equivalent to forensic authentication. In the

specific configuration of this case, weaknesses in chain-of-custody documentation primarily affected the weight of evidence. In other cases, however, where such weaknesses concern the legality of acquisition, provenance, or fundamental integrity of the evidence, the issue may develop into one of admissibility. Strengthening digital forensic procedures, chain-of-custody documentation, hash-value verification, metadata examination, and the involvement of competent experts is therefore necessary to ensure that the evidentiary assessment of deepfake cases does not depend excessively on defendants' admissions or testimonial consistency.

E. Conclusion

The judicial reasoning in Decision No. 12/Pid.Sus/2026/PN Smg adequately connected digital evidence with witness testimony, physical exhibits, and the defendant's statement to construct a coherent evidentiary narrative. The digital evidence was not assessed in isolation but was incorporated into an evidentiary framework encompassing juridical, philosophical, and sociological considerations. Compared with Decision No. 125/Pid.Sus/2019/PN Bjn, the Semarang case involved a broader legal construction in terms of the range of criminal provisions considered and the attention given to the pornographic nature of the manipulated content. Nevertheless, the judgment did not sufficiently address technical authentication or chain-of-custody procedures, and no digital forensic expert testimony was presented at trial.

When assessed through the applicable evidentiary framework, the digital evidence in this case satisfied the minimum evidentiary requirement under Article 183 KUHAP. Its relevance and materiality were relatively well established, while its reliability and credibility received substantial corroborative support from the consistency among digital evidence, witness testimony, physical exhibits, and the defendant's statement. The resulting evidentiary construction therefore provided a relatively coherent factual basis for judicial conviction. However, from a technical evidentiary perspective, the case would have presented a stronger evidentiary foundation had it been supported by independent forensic verification and systematically documented evidence-preservation procedures. The absence of specific regulation governing deepfake pornography further required law-enforcement authorities to rely on and combine provisions from several different statutes, thereby contributing to legal uncertainty.

On the basis of these findings, greater harmonization among KUHAP, the ITE Law, the Pornography Law, and the Personal Data Protection Law is necessary to develop more coherent and consistent standards for digital evidence. More specific regulation addressing deepfake pornography as a distinct criminal offense should also be considered in order to provide greater legal certainty. For law-enforcement authorities, strengthening digital forensic capacity is essential to ensure that electronic evidence is acquired, preserved, examined, and presented before the courts through standardized and legally accountable procedures.

References

- Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan hukum terhadap penyalahgunaan deepfake pada pornografi anak di era artificial intelligence di Indonesia. *Jurnal Penelitian Serambi Hukum*, 18(01), 42-54. <https://doi.org/10.59582/sh.v18i01.1257>.

- Europol. Facing Reality? Law Enforcement and the Challenge of Deepfakes. European Union Agency for Law Enforcement Cooperation, 2022. <https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes>.
- Faturrachman, Sy, M. (2025). Deepfake pornografi: Studi konstitusi dan penegakannya di Indonesia. *Jurnal Legislatif*, 113-128. <https://doi.org/10.20956/jl.v8i2.44186>.
- Haefani, Hayya Zafna, and Asti Sri Mulyanti. "Urgensi Reformasi Hukum Pidana Indonesia dalam Menjerat Pelaku Deepfake Pornografi Berbasis Artificial Intelligence." *Aladalah: Jurnal Politik, Sosial, Hukum dan Humaniora* 3.3, 2025: 12-26. <https://doi.org/10.59246/aladalah.v3i3.1554>.
- Hanifa, Roihan Hanaan, et al. "Kekosongan Hukum dalam Menjerat Tindak Pidana Berbasis Deepfake: Ancaman Baru dalam Pembuktian." *Syah Kuala Law Journal* 9.3, 2025. <https://doi.org/10.24815/sklj.v9i3.51766>.
- Harahap, M. Yahya. *Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*. Edisi Kedua. Jakarta: Sinar Grafika, 2012.
- Hiariej, Eddy O.S. *Teori dan Hukum Pembuktian*. Jakarta: Erlangga, 2012.
- Janna, Reftahu dan Ria Anggraeni Utami. "Relevansi Alat Bukti Dalam Sistem Peradilan Pidana Indonesia: Analisis Normatif Dan Praktis." *Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan*, Vol. 2, No. 1, 2025, hlm. 438-440. <https://jurnal.globalscients.com/index.php/jkhp/article/view/837>.
- Kartadinata. "Rekonstruksi delik pidana dalam kejahatan deepfake: Tantangan pembuktian dan perlindungan korban." *Muara Hukum: Jurnal Ilmiah Ilmu Hukum dan Administrasi Publik*, Vol. 6, No. 1, 2026, hlm. 32-48. <https://doi.org/10.64365/muarakum.v2i1.203>.
- Kemkomdigi. "Kemkomdigi Telah Tangani 1,3 Juta Konten Pornografi dan Judi Online." ANTARA News, 10 Maret 2025. <https://www.antaraneews.com/berita/4699853/kemkomdigi-telah-tangani-13-juta-konten-pornografi-dan-judi-online>.
- Kurniarullah, Muhammad Rizki, et al. "Tinjauan kriminologi terhadap penyalahgunaan artificial intelligence: Deepfake pornografi dan pencurian data pribadi." *Jurnal Ilmiah Wabana Pendidikan* 10.10, 2024: 534-547. <https://doi.org/10.5281/zenodo.11448814>.
- Mongkau, Natanael Hiskia, Herlyanty Y. A. Bawole, dan Altje A. Musa. "Penegakkan Hukum Terhadap Penyalahgunaan Kecerdasan Buatan Dengan Cara Memanipulasi Wajah Seseorang Ke Dalam Gambar Atau Video Porno." *Lex Administratum: Jurnal Fakultas Hukum Unsrat*, Vol. 13, No. 2, 2025. <https://ejournal.unsrat.ac.id/v3/index.php/administratum/article/view/61073>.
- Noerman, Chiquita Thefirstly dan Aji Lukman Ibrahim. "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara." *Jurnal USM Law Review*, Vol. 7, No. 2, 2024, hlm. 603-621. <https://doi.org/10.26623/julr.v7i2.8995>.
- Novyanti, Risa dan Astuti. "Perlindungan Hukum bagi Korban Penyebaran Konten Deepfake Pornografi." *Jurnal Hukum dan HAM*, Vol. 12, No. 3, 2021, hlm. 1-15.

- Nurwahid, Tri, Sri Amlinawati Muin, and Rizki Ramadhani. "Deepfake sebagai Kejahatan: Manipulasi AI Audio, Video, dan Gambar dalam Hukum Pidana Indonesia." *Legal Dialogica* 1.2, 2026. <https://doi.org/10.29303/parhesia.v2i2>.
- Paramesti, Zahra Anindya, et al. "Kekosongan Hukum Dalam Penanganan Kekerasan Gender Berbasis Digital Melalui Teknologi Deepfake Di Indonesia." *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4.4, 2026: 7977-8008. <https://doi.org/10.61104/alz.v4i4.8643>.
- Pitaloka, Cerens Amanda Gea. "Penyalahgunaan Teknologi Deepfake untuk Konten Pornografi Non-Konsesual di Indonesia." *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora* 2.2, 2025: 74-81. <https://doi.org/10.62383/humif.v2i2.1475>.
- Qamar, Nurul. "Kekuatan Pembuktian Alat Bukti Elektronik dalam Perkara Pidana." *Jurnal Hukum*, Vol. 26, No. 2, 2019, hlm. 200-215.
- Rifai, Ahmad. *Penemuan Hukum oleh Hakim dalam Perspektif Hukum Progresif*. Jakarta: Sinar Grafika, 2010.
- Sandoval, M. P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: a systematic review. *Crime Science*, 13(1), 41. <https://doi.org/10.1186/s40163-024-00239-1>.
- Saturnus, Albert Andre. "Pertanggungjawaban Pidana Penyalahgunaan Deepfake Berbasis Artificial Intelligence Dalam Perspektif Undang-Undang ITE Baru." *Causa: Jurnal Hukum dan Kewarganegaraan* 16.8 (2026). <https://doi.org/10.2238/cwmb9040>.
- Seveney, Madalaine Christella, Demas Brian Wicaksono, and Irwan Kurniawan Soetijono. "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi." *Disiplin: Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda* 31.2, 2025: 97-106. <https://doi.org/10.46839/disiplin.v31i2.1167>.
- Semarang District Court. Judgment No. 12/Pid.Sus/2026/PN Smg
- Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: UI Press, 2014.
- Sompotan. "Kekosongan Hukum (Rechtsvacuum) dalam Penjeratan Tindak Pidana Pembuatan dan Penyebaran Deepfake Pornografi Menggunakan Kecerdasan Buatan di Indonesia." *Jurnal Lex Crimen*, Vol. 15, No. 1, 2026, hlm. 1-12. <https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/67834>.
- Susatyo, Febriyan Alam. "Kriteria Alat Bukti Elektronik yang Sah dalam Urgensi Pembaharuan KUHAP." *Jurnal Hukum dan Dinamika Masyarakat*, Vol. 21, No. 1, 2023, hlm. 51-65. <http://dx.doi.org/10.56444/hdm.v21i1>.
- Tanoto, E., Tandy, J., & Banke, R. (2024). Kekuatan alat bukti elektronik dalam proses pembuktian di peradilan pidana. *Jurnal Ilmu Hukum*, 2(1), 90-96. <https://doi.org/10.62017/syariah.v2i1.2352>.
- Tavadjio, Syifa Nurlita. "Implikasi Legal dari Deepfake: Ganti Rugi Perdata atas Pemalsuan Wajah dan Suara." *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 3.4, 2025: 4566-4577. <https://doi.org/10.61104/alz.v3i4.1995>.
- Utara, Elang Rinjani dan Anis Widyawati. "Analisis Penegakan Hukum Pidana Deepfake Pornografi Non-Konsensual Dalam Penyebaran Konten Manipulatif di Indonesia." *Al-Jinayah: Jurnal Hukum Pidana Islam*, Vol. 11, No. 1, 2025, hlm. 125-153. DOI: <https://doi.org/10.15642/aj.2025.11.1.125-153>.