JIHAD: Jurnal Ilmu Hukum dan Administrasi
Vol. 8 No. 2 Mei 2026
p-ISSN : 2745-9489, e-ISSNl 2746-3842
DOI: *10.36312/jihad.v8i2.10613/https://ejournal.mandalanursa.org/index.php/JIHAD/issue/archive*

Legal Challenges to Proving Deepfake Video Evidence in the Criminal Justice Process in Indonesia

Daniel Johnson Goenawan[1], Muhammad Naufal Rionatadiradja[2], Reyzel Yandika Lim[3], Denovan Salim[4], Marchya Gwenerve Mongkaw[5], Pietro Grassio E.Y[6]
Fakultas Hukum, Universitas Pelita Harapan, Indonesia

Article Info
Article history:
Received: 30 April 2026
Publish: 9 May 2026

Keywords:
Deepfake;
Artificial Intelligence;
Electronic Evidence;
Cybercrime;
Criminal Procedure.

Abstract
Deepfake technology, powered by generative artificial intelligence, poses significant challenges to the integrity of electronic evidence in Indonesia's criminal justice system. This study examines the legal position of deepfake videos as evidence under the Electronic Information and Transactions Law (UU ITE) and the Criminal Procedure Code (KUHAP). Using a normative juridical method with a statutory approach, the research analyzes formal and material requirements for electronic evidence, technical and juridical obstacles in authentication, and real-world cases such as the Baim Wong voice cloning fraud. The findings indicate that current regulations lack specific standards for authenticating synthetic media, creating a legal vacuum and risks of misjudgment in post-truth court proceedings. This paper recommends regulatory updates, standardization of digital forensics, and capacity building for law enforcement to strengthen evidentiary reliability.

Corresponding Author:
Daniel Johnson Goenawan
Fakultas Hukum, Universitas [Nama Universitas Anda], Indonesia
Email Coresspondent: danielgoenawan017@gmail.com

1. INTRODUCTION

The digital transformation has transformed the legal landscape of evidence. Video, once considered "golden evidence" for its ability to capture reality, can now be completely manipulated using Deepfake technology. In Indonesia, although the ITE Law recognizes electronic information as valid evidence, there are no clear legal definitions regarding how the law addresses synthetic media capable of identically resembling a person's face and voice. This creates the risk of disqualification of evidence or even wrongful criminalization.

The development of digital technology over the past decade has brought significant changes to various aspects of human life, including communication, information, and law enforcement. One of the most recent developments in information technology is the use of artificial intelligence (AI), particularly generative AI technology, which can automatically create new content. This development has given rise to the phenomenon of deepfakes, a technology that allows for the realistic manipulation of faces, voices, and videos to resemble real-life situations, even though the content is digitally engineered.

Initially, this technology was developed for entertainment and the creative industry. However, as it evolved, deepfakes began to be misused for various crimes, such as non-consensual pornography, voice-cloning fraud, and the spread of disinformation that could influence public opinion and even political stability. This situation demonstrates that a neutral technology can become an instrument of crime when used without oversight and clear legal boundaries.

In the context of Indonesian law, regulations regarding information technology-based crimes still rely on provisions in the Electronic Information and Transactions Law

and the Criminal Code. However, neither legal instrument explicitly addresses deepfakes, a form of cybercrime with unique characteristics, particularly the manipulation of digital reality, which is extremely difficult to detect with the naked eye.

This lack of specific regulations creates problems in law enforcement practices, both in terms of qualifying criminal acts, providing evidence, and determining criminal liability for perpetrators. Law enforcement officials often have to "enforce" existing norms to prosecute perpetrators, even when the characteristics of their actions do not fully align with the existing criminal code.

Furthermore, the development of deepfake technology also poses serious challenges to the evidentiary system in criminal law. The authenticity of digital evidence is becoming increasingly difficult to verify, opening up debate about the validity and reliability of electronic evidence in court. This demonstrates the gap between technological developments and the legal system's ability to respond.

Based on this description, it can be understood that the deepfake phenomenon is not merely a technological issue, but also a complex legal one. Therefore, an in-depth study is needed on how Indonesian positive law responds to the misuse of this technology, as well as the extent to which the concept of criminal liability can be effectively applied to address AI-based crimes.

2. RESEARCH METHOD

This research uses a normative juridical method with a statute approach. The analysis is conducted on the synchronization between the ITE Law, Criminal Procedure Code, and the Personal Data Protection Law (PDP Law) related to the phenomenon of AI-based cybercrime. Secondary data in the form of laws and regulations, court decisions (including case number 1295/Pid.Sus/2023/PN Mdn), and legal literature were analyzed qualitatively using descriptive-analytical techniques.

3. DISCUSSION

The Legal Status of Deepfake Videos as Evidence in the Indonesian Criminal Prosecution System

1. Normative Basis for Electronic Evidence

In the Indonesian criminal procedure system, valid evidence is regulated in a limited manner in Article 184 paragraph (1) of the Criminal Procedure Code, which includes witness statements, expert statements, letters, instructions, and statements from the accused. Along with technological developments, the ITE Law has expanded the scope of this evidence by recognizing electronic information and electronic documents as valid evidence. Article 5, paragraph (1) of the ITE Law explicitly states that electronic information and/or electronic documents constitute valid legal evidence.

However, the most fundamental legal issue with the deepfake phenomenon is the degradation of trust in digital evidence. Although the ITE Law recognizes electronic information and electronic documents as valid evidence, the presence of deepfakes raises questions about whether a video is a recording of reality or simply a digital fabrication.

This situation creates two problems simultaneously: on the one hand, judges can reject genuine video evidence because it is suspected to be a deepfake; on the other hand, fake video evidence resulting from AI manipulation could potentially be accepted as truth if it goes undetected. Both pose serious threats to legal certainty.

2. Formal and Material Requirements for Electronic Evidence

For electronic information to have evidentiary force, it must meet two main requirements: formal and material. Formally, electronic evidence must be legally

obtained in accordance with applicable procedural law. Materially, its authenticity, completeness, and integrity must be guaranteed.

Deepfake videos inherently violate these material requirements because deepfake content is often very convincing and widely distributed on various platforms without intact metadata, so verifying the authenticity of the video or sound requires digital forensic expertise that not all law enforcement officers have.

The lack of complete and intact metadata is a critical point. Metadata in video files—such as timestamp information, device used, and modification history—are primary indicators of a recording's authenticity. AI manipulation through deepfake technology can produce recordings that are visually identical to the original, but have missing or manipulated metadata. Therefore, deepfake videos are fundamentally flawed and cannot meet the requirements for authenticity as valid evidence.

Technical and Legal Obstacles in Proving the Authenticity of Videos in Court

1. Technical Barriers: Limitations of Digital Forensics

The Indonesian justice system requires new standards in digital forensics. Judges and prosecutors can no longer rely solely on sight or hearing to assess the authenticity of a video. Certified AI experts and AI detector software are essential to ensure legal certainty. Without updates to procedural law regarding digital content validation, there is a risk of a justice crisis where genuine evidence is rejected as deepfakes or false evidence is accepted as truth.

Current deepfake detection methods include several approaches: visual artifact analysis, lighting and shadow inconsistency detection, and AI-based biometric analysis, such as eye blink patterns and facial micro-expressions. However, all of these methods are highly technical and require equipment and human resources that are not widely available in Indonesian law enforcement institutions.

2. Legal Obstacles: Regulatory Vacuum

From a regulatory perspective, the Indonesian legal system currently lacks explicit regulations regarding deepfakes, creating a legal vacuum that makes it difficult to establish evidence and weakens victim protection.

The Director General of Digital Space Supervision at Komdigi, Brigadier General Alexander, explained that the ITE Law remains the legal basis used to handle deepfake crime cases, due to the incomplete discussion of regulations specifically governing the ethics and use of artificial intelligence (AI).

This situation forces law enforcement officials to use analogies or broaden their interpretation of existing norms. Substantively, the ITE Law prohibits the dissemination of information that violates morality (Article 27 paragraph 1) or defamation (Article 27 paragraph 3), but deepfakes often operate in a "gray area" not fully captured by these definitions.

In addition to the ITE Law, several other legal instruments that can be used include: Law Number 27 of 2022 concerning Personal Data Protection which provides an important foundation in protecting identity elements such as face, voice, and biometrics as personal data that may not be used without the owner's consent, as well as Article 27A and Article 29 of the ITE Law to ensnare perpetrators of spreading deepfake content containing insults, threats, or defamation.

From a general criminal perspective, digital identity manipulation that harms an individual can be subject to sanctions under Article 378 of the Criminal Code concerning fraud if there is material loss. If used to damage a reputation or commit extortion, the perpetrator can be charged under articles on forgery, defamation, and unpleasant acts.

However, all of this depends on the ability of law enforcement officials to understand and analyze complex and rapidly changing digital evidence.

Case Study Analysis: Baim Wong's Voice Cloning and Synthetic Media Fraud

The case involving public figure Baim Wong has become one of the most important legal precedents in Indonesia in understanding how technology...*deepfake* used to manipulate public trust and commit massive economic crimes. This case provides a vivid illustration of the transition of fraud modus operandi from simple text or static photos to highly convincing synthetic audio-visual media.

1. Modus Operandi and Technology Characteristics

In case number **1295/Pid.Sus/2023/PN Mdn**, the perpetrator used artificial intelligence technology to misuse Baim Wong's identity in the context of the program *giveaway*. The techniques used include:

- **Voice Cloning**: The perpetrator used Baim Wong's original voiceover from an old video of the 2021 "Indonesia Giveaway" program, then manipulated it using AI to produce new sentences that fit the fraudulent narrative.
- **Video Call Manipulation**: The perpetrator made a video call (*video call*) to the victim by displaying a visual of Baim Wong's face that was manipulated, creating the impression as if the artist was interacting directly with the victim in *real-time*.
- **Ancaman Epistemic**: This manipulation aims to lead public opinion to believe events that never actually happened, thereby destroying the victim's ability to distinguish between real and fake information.

2. Impact and Losses to Victims

This misuse of technology has proven highly effective in trapping victims with limited digital literacy. One victim, a woman with the initials E (49 years old), suffered material losses estimated at Rp149,000,000 after registering through a social media link and receiving the manipulative call. The losses were not only financial but also damaged the reputations of public figures whose names were impersonated, as the public could question the integrity of the genuine programs they ran.

3. Legal Entanglement and Considerations of the Panel of Judges

The Medan District Court panel of judges declared the defendant legally and convincingly proven guilty of committing the crime of "intentionally and without authority spreading false and misleading news that resulted in consumer losses in Electronic Transactions." The main legal basis used is:

- **Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) of the ITE Law**: This article is the main instrument because it focuses on the impact of fake news, which causes consumer losses.
- **Article 378 of the Criminal Code (Fraud)**: Although the ITE Law has become a *special law*, the element of fraud with trickery through false identity is the criminal background of this action.
- **Relevance of the 2024 ITE Law**: From the perspective of the latest revision (Law No. 1 of 2024), this kind of action can also be prosecuted with **Article 27A,** regarding attacks on honor if the content is detrimental to good name, or **Article 35,** regarding the manipulation of electronic information to make it appear as if it were authentic data.

Baim Wong's case highlights that, while comprehensive AI-specific regulations are not yet available, an extensive interpretation of the fraud and fake news articles

in the ITE Law can still provide legal protection for victims, provided that forensic evidence can demonstrate the existence of digital manipulation in the media used.

4. CONCLUSION AND SUGGESTIONS

The presence of technology, *deepfakes,* has fundamentally changed the way criminal procedure law views digital evidence. While previously considered an objective representation of reality, video must now be treated as highly dynamic information susceptible to manipulation. The challenges of evidentiary law in Indonesia lie not only in the regulatory vacuum but also in the gaps in technological infrastructure and the capacity of law enforcement to validate digital content.

Based on a comprehensive analysis of the normative basis, technical obstacles, and phenomenology of the case, strategic steps are needed to strengthen the Indonesian criminal evidence system in dealing with this phenomenon of *post-truth*:

First, there is a need to accelerate the revision or creation of specific laws governing artificial intelligence and synthetic media. These regulations must include clear definitions of *deepfakes* and require platform providers and AI developers to implement the technology, *watermarking,* and labeling of all machine-generated content. This will help meet the material requirements for authenticity of evidence from the early stages of an investigation.

Second, standardization of digital forensic procedures should be mandatory for all law enforcement agencies through the full adoption of the ISO/IEC 27037 standard and the ACPO principles. Any video evidence presented in court must be accompanied by a forensic audit report explaining the integrity of the evidence *metadata* and consistency of values from the source to the courtroom. The use of forensic copies (*working copies*) in the inspection process must be the norm to maintain the authenticity of primary data.

Third, strengthening the capacity of judicial institutions through ongoing education and training for judges, prosecutors, and investigators on generative technology. Judges should be encouraged to be independent in assessing digital evidence without relying passively on expert testimony. Understanding visual artifacts and biometric anomaly patterns in-*depth* will assist judges in developing more objective confidence.

Fourth, improvements to digital forensic laboratory infrastructure at the regional level must be implemented immediately. The availability of certified AI detection software at every regional police station will expedite the evidence verification process and minimize the risk of evidence damage due to long-distance transportation or incompetent handling.

Fifth, multi-stakeholder collaboration between government, academics, and technology companies is needed to build a resilient digital ecosystem. The development of detectors, *deepfakes, and l*ocal AI-based systems tailored to the sociolinguistic and visual characteristics of Indonesian society will be a crucial pillar of national cyber defense. With a holistic, adaptive, and collaborative approach, Indonesia's criminal justice system can remain a guardian of material justice, even when faced with the increasingly complex challenges of digital reality manipulation.

5. BIBLIOGRAPHY

Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan hukum terhadap penyalahgunaan deepfake pada pornografi anak di era artificial intelligence di Indonesia. Jurnal Serambi Hukum, 18(1).

Insan, P. (2018). Legalitas alat bukti elektronik dalam sistem peradilan pidana. Lex Renaissance, 3(1), 109–124.

Kiliç, B., & Kahraman, M. E. (2023). Current usage areas of deepfake applications with artificial intelligence technology. İletişim ve Toplum Araştırmaları Dergisi.

Kumar, M., Rai, P. K., & Kumar, P. (2024). A novel approach for detecting deepfake face using machine learning algorithms. In 2024 2nd International Conference on Disruptive Technologies (ICDT), 1588–1592.

Liambas, C., & Manios, A. (2023). Pornography image detection in digital forensics. In 2023 8th International Conference on Frontiers of Signal Processing (ICFSP), 88–92.

Mrvić-Petrović, N. (2024). Criminal law approach to regulating non-consensual pornographic deepfake. Bezbednost.

Panda, J. K., & Panigrahy, R. (2023). Unmasking deception in the age of artificial intelligence: A comprehensive analysis of Indian celebrity's deepfakes news. ShodhKosh: Journal of Visual and Performing Arts, 4(2).

Purwono, A., et al. (2024). Implications and considerations of the new electronic information and transaction law. ANAYASA: Journal of Legal Studies.

Rahmadie, D. T. R. (2016). Regulasi penyimpangan artificial intelligence pada tindak pidana malware berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016. Jurnal Hukum Pidana dan Penanggulangan Kejahatan, 9(2), 128–136.

Shahzad, H., et al. (2022). A review of image processing techniques for deepfakes. Sensors, 22.

Supriya, et al. (2024). Investigating the evolving landscape of deepfake technology: Generative AI's role in its generation and detection. International Research Journal on Advanced Engineering Hub.

Wibowo, A. M. T. A. P. G., Maharani, D. P., & lainnya. (2024). Analisis yuridis penggunaan artificial intelligence yang menjalankan fungsi legal audit dalam regulatory compliance system di Indonesia. Brawijaya Law Student Journal.

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

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.