Digital Forensic Data In Technology-Based Crime Investigations: A Juridical-Empirical Review Of Obstacles And Solutions

Zain Arfin Utama[1]*, Dwi Kusumawati[2], Sutinnarto[3]
[1,2,3]*Institute Karya Mulia Bangsa*

Corresponding Author
Email: zainjournals@gmail.com

ABSTRACT

Digital forensic evidence has become a critical tool in cybercrime investigations, yet its implementation in Indonesia faces normative and technical gaps. This study analyzes the urgency, evidentiary paradigms, and challenges of digital forensic data using a juridical-empirical approach and case studies (MV Run Zeng Case, 2024). Findings indicate that while Law No. 19/2016 on ITE and the Criminal Procedure Code (KUHAP) recognize digital evidence, weak chain of custody, lack of certified experts, and overlapping regulations threaten evidentiary integrity. Proposed solutions include standardizing DEFR procedures, inter-agency collaboration, and capacity-building through certified training. These findings contribute to developing adaptive digital forensics policies for Industry 5.0, balancing substantive justice and privacy protection. This research underscores that the successful implementation of digital forensic evidence depends not only on strong regulations, but also on a collective commitment to adopting global best practices. In this way, Indonesia can position itself as a pioneer in enforcing cyber law in the digital era, while maintaining a balance between public security and protecting individual rights.

Keywords: *Digital Forensics, Cybercrime, Criminal Evidence, ITE Law, Chain of Custody.*

INTRODUCTION

The development of information technology has transformed the crime landscape, with cybercrime increasing by 93% in 2020–2024 (Ministry of Communication and Information, 2024). Crimes such as defamation (65%), digital fraud (25%), and system hacking (10%) dominate cases in Indonesia (ITU Global Cybersecurity Index, 2024). In response, digital forensic data has become an essential evidentiary tool, but its implementation is hampered by:

1. Overlapping regulations: Law No. 19/2016 on the Electronic Information and Transactions (ITE) recognizes digital evidence, but the Criminal Procedure Code (KUHAP) does not yet regulate detailed procedures for its collection.

2. Limited infrastructure: Only 5 of 34 provinces have digital forensic laboratories (*BPS, 2025*).
3. Human resource gap: Only 12% of investigators hold Certified Forensic Examiner (CFE) certification (*Laporan Kemenkopolhukam, 2024*).
4. Privacy vs. Privacy Conflict Investigation: Personal Data Protection Law (PDP) No. 27/2022 restricts investigators' access to personal data, while the need for evidence demands high levels of accessibility.

Amidst these complex challenges, the dynamics of cybercrime in Indonesia are increasingly showing systematic and organized patterns. According to the Indonesia Cyber Threat Landscape 2025 report published by the National Cyber and Crypto Agency (BSSN), the modus operandi of cybercriminals is no longer solely local but also involves transnational networks that exploit legal and technological loopholes across jurisdictions. For example, phishing and ransomware cases targeting the financial and public service sectors often involve servers located overseas, complicating investigations and prosecutions.

Furthermore, technological developments such as the Internet of Things (IoT) and cloud computing have expanded the attack surface, with every connected device becoming a potential entry point for criminals. Data from the Indonesia Cybersecurity Forum (2025) indicates that 40% of cyberattacks in 2024 targeted IoT devices, such as CCTV cameras and building automation systems, which often lack adequate security protocols. This not only complicates the process of collecting digital evidence but also requires investigators to have a deep technical understanding of various platforms and security protocols.

In this context, the role of digital forensic evidence is not merely as a means of proof, but also as an instrument for building public trust in the judicial system. However, without a clear framework and adequate resources, the potential of digital evidence to uncover crimes and protect victims will remain hampered. Therefore, efforts to strengthen digital forensic infrastructure must be accompanied by public awareness campaigns and holistic policy reforms so that Indonesia can respond to cyber threats more effectively and adaptively.

Rapid technological developments have also given rise to new, more sophisticated and difficult-to-detect forms of cybercrime. For example, the use of deepfakes and synthetic identity fraud is increasingly prevalent in cases of defamation and online fraud. According to the Interpol Global Crime Trend (2025) report, Indonesia is among the 10 countries with the highest growth in deepfake cases in Southeast Asia, where this technology is used to

manipulate individuals' voices and faces in content intended to slander or blackmail. This not only causes material losses but also damages the reputation and public trust in institutions, both in the private and government sectors.

Furthermore, cybercrime is now increasingly integrated with conventional crimes, such as money laundering and terrorism. The Financial Action Task Force (FATF) noted in its 2025 report that Indonesia is one of the countries most vulnerable to money laundering through cryptocurrency. The anonymous and cross-border nature of crypto transactions is often exploited by criminals to conceal the origins of illicit funds. This challenge is further complicated by the lack of comprehensive regulations regarding the monitoring and tracking of crypto transactions, making it difficult for investigators to uncover organized crime networks.

At the international level, Indonesia also faces pressure to comply with global standards in handling cybercrime. The Budapest Convention on Cybercrime, ratified by more than 60 countries, requires cross-border cooperation in the investigation and exchange of digital evidence. However, limited infrastructure and regulations that are not yet fully aligned with international standards often hinder this cooperation. For example, differences in digital evidence collection procedures between countries can result in evidence collected in Indonesia being inadmissible by courts in other countries, or vice versa.

In this context, the importance of building a robust and integrated digital forensics ecosystem becomes increasingly urgent. This ecosystem should involve not only law enforcement agencies but also the private sector, academia, and civil society. Collaboration with technology companies, for example, can assist in the development of more sophisticated digital forensic tools and methods, while collaboration with universities can encourage research and the development of qualified human resources. Furthermore, active public participation in reporting and preventing cybercrime through digital awareness programs will also strengthen prevention and law enforcement efforts.

Thus, the challenges Indonesia faces in implementing digital forensic evidence are not only technical or legal, but also social and cultural. A comprehensive and sustainable approach involving regulatory reform, infrastructure strengthening, human resource capacity building, and public participation will be key to addressing existing gaps and ensuring that the justice system can adapt to the evolving dynamics of cybercrime.

METHODS

This research uses a juridical-empirical approach with: Document analysis: ITE Law No. 19/2016, Criminal Procedure Code, Minister of Communication and Information Regulation No. 5/2020, and court decisions (Supreme Court Decision No. 156K/Pid/2023). Case study: MV Run Zeng Case (2024): Use of screenshots and videos as evidence without chain of custody. Defamation Case (2023): Rejection of WhatsApp chat evidence because it was not verified by forensic experts (Bandung District Court Decision No. 45/Pid.B/2023). Secondary data: International journals (Digital Investigation, Journal of Cybersecurity), ITU reports, and Indonesia Cybersecurity Report 2025.

RESULT AND DISCUSSION

A. Digital-Based Criminal Evidence Paradigm

1. Legal Framework

ITE Law Article 5 paragraph (1): Recognizes electronic documents as evidence, but does not regulate procedures for obtaining evidence (e.g.: imaging, hash verification). Criminal Procedure Code Article 184: Five forms of evidence (witnesses, letters, instructions, confessions, expert statements) do not explicitly include digital evidence, although judicial practice has used it (Supreme Court Decision No. 156K/Pid/2023). Minister of Communication and Information Regulation No. 5/2020: Regulates the termination of access to illegal content, but does not regulate the acquisition of forensic evidence.

Table. 1 Comparison of Digital Evidence Regulations

Regulation	Superiority	Weakness
UU ITE No. 19/2016	Recognizing digital evidence as valid	Does not regulate technical procedures
KUHAP	Providing a common evidentiary framework	Not yet adaptive to digital evidence
Permenkominfo 5/2020	Regulating illegal content	Does not regulate chain of custody

To be accepted as valid evidence, electronic information and/or electronic documents must meet the following formal and material requirements:

a. Formal requirements: Authenticity, integrity, and reliability of the electronic

system used.

b. Material requirements: Relevance and evidentiary value directly related to the case being tried.

2. Digital Based Proof Procedures

The Role of Digital Forensics in Evidence: Digital forensics plays a crucial role in analyzing, collecting, and presenting digital evidence in court. This process involves:

a. Collecting digital evidence from electronic devices (computers, cell phones, CCTV cameras, etc.).
b. Analyzing the evidence by a digital forensics expert to ensure the integrity and authenticity of the data.
c. Presenting evidence in the form of expert testimony or authenticated electronic documents.

Forensic Expert Testimony is a digital forensic expert's testimony that has high evidentiary value in court, as the expert can explain the process of collecting, analyzing, and authenticating digital evidence. According to the Criminal Procedure Code, expert testimony is a valid form of evidence and can strengthen the case. (*UNS Faculty of Medicine, "The Importance of Forensic Experts in the Indonesian Criminal Justice System"*)

3. Chain of Custody (CoC) in Handling Digital Evidence

Chain of Custody (CoC) is a chronological documentation procedure that ensures the integrity and authenticity of digital evidence from the time it is discovered at a crime scene until it is presented at trial. The CoC includes:

a. Recording every interaction with digital evidence (who handled it, when, and what actions were taken).
b. Using technologies such as hashing to ensure data is not manipulated.
c. Secure storage to prevent damage or loss of evidence. *(Islamic University of Indonesia, "Study on Chain of Custody of Digital Evidence")*

4. CoC regulations and standards in Indonesia

Although there are no specific regulations comprehensively governing the CoC, several guidelines have been implemented, such as:

a. Police Regulation (Perkap) No. 10/2010 concerning Procedures for Handling Evidence.

b. ISO/IEC 27037 Guidelines for the Identification, Collection, and Preservation of Digital Evidence.

c. Digital Forensic Examination Reports, including information about personnel, evidence specifications, and actions taken. (Hukumonline, "Blockchain-Based Chain of Custody in Handling Digital Evidence,)

5. The Urgency of Digital Forensics in Cybercrime

Indonesia has faced a significant surge in cybercrime cases in recent years. According to data from the Indonesian National Police Criminal Investigation Agency (Bareskrim Polri), in 2025, there were 32,073 reports of cybercrime, with the number of victims reaching 29,067 people (Bareskrim Polri, 2025). Defamation (65% of total cases), Digital fraud (25%), System hacking (10%) (*Kemenkominfo, "Cybercrime Statistics in Indonesia," 2024.)*.

Digital forensics plays a crucial role in collecting, analyzing, and presenting digital evidence that can be used in court. Without digital forensics, the evidentiary process would be difficult because:

a. Digital evidence is volatile (easily changed, lost, or manipulated).

b. Cybercrimes often involve perpetrators using sophisticated technology to conceal their identities and digital footprints. (*Alu Oleo University*).

Challenges in Implementing Digital Forensics: Despite the importance of digital forensics, its implementation in Indonesia still faces several challenges, including:

a. Infrastructure limitations: Only 5 of 34 provinces have digital forensics laboratories. (*BPS, "Digital Forensic Infrastructure Data in Indonesia," 2025*.)

b. Human Resources Gap: Only 12% of investigators have a Certified Forensic Examiner (CFE) certificate (*Coordinating Ministry for Political, Legal, and Security Affairs, "Digital Forensic Human Resources Availability Report," 2024.*)

c. Incomplete regulations: The ITE Law and the Criminal Procedure Code do not

fully regulate standard procedures for collecting and analyzing digital evidence. (*Islamic University of Indonesia, "Legality of Electronic Evidence in the Criminal Justice System*")

To address these challenges, efforts are needed to strengthen digital forensics, including:

a. Improving infrastructure: Building more digital forensics laboratories throughout Indonesia.
b. Training and certification: Increasing the number of certified digital forensics investigators and experts.
c. Regulatory reform: Developing more detailed regulations regarding procedures for collecting, analyzing, and presenting digital evidence. (*Teknokrat Indonesia University, "The Role of Digital Forensics as Digital Evidence of Criminal Acts"*).

One example of the urgency of digital forensics is in handling deepfake cases, where AI technology is used to manipulate an individual's voice and face. In January 2025, the Indonesian National Police's Criminal Investigation Agency (Bareskrim Polri) arrested a suspect in Lampung who used deepfake videos to offer fake social assistance, causing losses of tens of millions of rupiah. Digital forensics is used to:

a. Analyze metadata from deepfake videos.
b. Trace the origin of the video's distribution.
c. Proving the authenticity and ensuring that the video is not manipulated (Verihubs, "Deepfake di Indonesia: Prabowo dan Jokowi jadi Korbannya," 2025)

6. Barriers to Implementing Digital Forensic Data

Table. 2 Barriers to Implementing Digital Forensic Data

Dimension	Problems	References
Normative	The ITE Law and the Criminal Procedure Code (KUHAP) are not synchronized in	Marzuki (2021), *Ius Quia Iustum Law Journal*

	regulating digital evidence.	
Technical	Forensic laboratories are only available in five provinces.	BPS Cybercrime Statistics (2025)
HR	Only 12% of investigators have CFE certification.	Coordinating Ministry for Political, Legal, and Security Affairs Report (2024)
Legal and Ethics	Conflict between the PDP (privacy) Law and investigative needs.	Utama (2024), *SYNERGY Journal*

B. Criminal Law Reform About Arrangement of Digital Forensik

1. Revisions and Additions to Regulations in the ITE Law and the Criminal Procedure Code

The ITE Law (Law Number 19 of 2016) needs to be updated to regulate in detail:

a. Procedures for collecting, storing, and analyzing digital evidence in accordance with international standards (e.g., ISO/IEC 27037).
b. Investigators' authority to access and secure digital evidence, including in cases involving new technologies such as cloud computing and blockchain.
c. Legal sanctions for perpetrators who manipulate or destroy digital evidence during the investigation process. (Mahasiswaindonesia.id, 2025)

Article 43 of the ITE Law needs to be updated to provide investigators with clearer authority to:

a. Access and secure digital evidence from electronic devices, including data stored in the cloud or on overseas servers.
b. Conduct wiretapping or digital monitoring under strict conditions to avoid privacy violations.
c. Use digital forensic technologies such as hashing and imaging to ensure the integrity of evidence.

The Criminal Procedure Code (KUHAP) needs to be revised to:

a. nclude digital evidence as a separate category in Article 184, not simply as an extension of conventional evidence.
b. Regulate procedures for testing the credibility of digital forensic experts in court, including competency requirements and methodologies that must be met. (*Islamic University of Indonesia, 2025*)

Emphasizing that technological developments demand an updated legal framework to address the potential risks of data misuse, privacy violations, and inequitable digital access, Indonesia, as a developing country, needs to strengthen regulations based on a sociological approach so that legal policies can respond to rapid changes without neglecting the protection of citizens' rights. Therefore, adapting to technological challenges is key to maintaining the relevance of law in the modern social context.

Law as a social reality is also relevant in understanding how it can create or reinforce social inequality. When legal structures do not reflect existing social realities, the law can become a tool to maintain injustice or inequality in society. For example, in many legal systems, there is a tendency to ignore the rights of marginalized or minority groups, whether in economic, ethnic, religious, or gender contexts. In this regard, critical legal theory can help us understand how the law often functions to maintain unjust social structures and ignores the needs of more vulnerable groups.

2. Ratification of International Conventions

Indonesia needs to ratify the Budapest Convention on Cybercrime to:

a. Strengthen international cooperation in addressing transnational cybercrime.
b. Align national regulations with global standards for handling digital evidence and investigating cybercrime.
c. Facilitating the exchange of digital evidence with other countries, which is especially important given the transnational nature of cybercrime. (Universitas Airlangga, 2022).

The steps for ratifying the Budapest Convention involve several key stages:

a. Government Consideration and Approval: The Indonesian government must examine the benefits and implications of ratification, including its compliance with national laws (UU ITE, KUHAP). The Ministry of Foreign Affairs (Kemlu) and the Ministry of Communication and Information Technology (Kominfo) are responsible for preparing the ratification text and ensuring alignment with existing regulations. (*Hukumonline, "Legal Basis for Cybercrime Internationally and Nationally," 2025*)

b. Approval by the House of Representatives (DPR): Ratification of an international convention requires the approval of the DPR through a Ratification Law (UU Ratification). The DPR will discuss the legal, political, and economic implications of ratification, including its impact on state sovereignty. (Airlangga University, "UNAIR Cyber Law Expert: Indonesia Must Ratify the Budapest Convention," 2022).

c. Signing and Submission of Ratification: After approval by the DPR, the President signs the instrument of ratification and submits it to the Secretary General of the Council of Europe. The Convention enters into force for Indonesia 30 days after the deposit of the instrument of ratification. (Wikipedia, "Budapest Convention on Cybercrime," 2025).

Benefits of Ratification for Indonesia

The gap between ethical communication principles and legal implementation. Although the law requires consent and the right to information, in practice, platforms' information delivery tends not to prioritize communication ethics. This leads to a situation where the law is formally fulfilled, but the ethical substance is not implemented. (Sutinnarto,2025)

a. International Cooperation in Law Enforcement

Exchange of digital evidence: The Budapest Convention allows Indonesia to request and provide digital evidence from/to other countries, which is crucial in cases of transnational cybercrime (e.g., phishing, ransomware, or money laundering through cryptocurrencies). Extradition of cybercrime perpetrators: Facilitates the arrest and extradition of perpetrators

operating from abroad. (Council of Europe, "Benefits of the Budapest Convention," 2025)

b. Regulatory Harmonization and Law Enforcement Capacity Building

Legal Harmonization: The Budapest Convention serves as a global benchmark for handling cybercrime. By ratifying it, Indonesia can align its ITE Law and Criminal Procedure Code with international standards, enabling digital evidence collected in Indonesia to be admitted in courts of other countries. (Airlangga University, "UNAIR Cyber Law Expert: Indonesia Must Ratify the Budapest Convention," 2022)

Training and Technical Assistance: Countries participating in the Budapest Convention frequently provide technical assistance and training to each other in handling cybercrime, including digital forensics and cross-border investigations. Access to Global Networks: Indonesia can join global cyber law enforcement networks, such as the 24/7 Network, for rapid information exchange on cyber threats.

CONCLUSION

The process of testing the credibility of digital forensic experts in Indonesian courts involves qualification assessment, methodology testing, cross-examination, and judicial review. Credible experts must be able to demonstrate competence, objectivity, and the integrity of the digital evidence presented. Without these, expert testimony can be rejected or deemed insufficiently probative. Digital forensics plays a crucial role in addressing cybercrime in Indonesia. Without strengthening infrastructure, human resources, and regulations, the process of proving evidence in cybercrime cases will continue to face obstacles. Therefore, collaboration between the government, academia, and the private sector is needed to build a robust digital forensics ecosystem that is adaptive to technological developments.

Legal Reform as the Main Key To ensure that digital forensics runs as it should, legal Reform are a step that cannot be postponed. Without clear and adaptive regulations, the process of proving cybercrime will continue to face obstacles, such as: Digital evidence that is not recognized in court due to non-standard collection procedures, Difficulties in international cooperation because national regulations are not aligned with global

standards,

Limited human resources and infrastructure that hinder the effective handling of cybercrime cases. Therefore, updating the ITE Law, the Criminal Procedure Code, and ratification of international conventions must be a top priority for the government. In addition, strengthening infrastructure, human resource training, and collaboration between institutions are also needed to build a strong and adaptive digital forensics ecosystem.

REFERENCES

International Journals

Friedman, M. (2020). *Digital Evidence and the U.S. Criminal Justice System*. *Digital Investigation*, 34, S43-S52

Interpol. (2024). *Global Crime Trend Report: Cybercrime and Digital Forensics*. Lyon: Interpol.

NIST. (2023). *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86.

Nasional Journals

Achmad, T. Y. (2024). *Peran Digital Forensik Dalam Penegakan Hukum*. *Lex Progressium*, 2(1), 45-60.

Pandam Bayu Seto Aji, & Zain Arfin Utama. (2025). Hukum Sebagai Kenyataan: Teori Sebagai Objek Studi dan Bahan Penelitian. *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, *3*(4), 3681–3694. https://doi.org/10.61104/alz.v3i4.1579

Sutinnarto, S., & Zain Arfin Utama. (2025). Etika Komunikasi dan Aspek Hukum dalam Penggunaan Data Konsumen Oleh Platform Digital. *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, *3*(4), 3695–3702. https://doi.org/10.61104/alz.v3i4.1918

Tatumpe, A. (2019). *Analisis Yuridis Digital Forensik*. *Scientia De Lex*, 7(1), 89-104

Utama, Z. A., & Asokawati, D. (2024). PEMBAHARUAN SISTEM HUKUM TERHADAP PENYELENGGARAN SISTEM ELEKTRONIK DALAM PENCEGAHAN KEJAHATAN. *Synergy : Jurnal Ilmiah Multidisiplin*, *2*(01), 62–74. Retrieved from http://e-journal.naureendigition.com/index.php/sjim/article/view/1543

Statistical Data

ITU. (2024). *Global Cybersecurity Index 2024*. Geneva: ITU.

Kemenkominfo. (2024). *Indonesia Cybersecurity Report 2025*. Jakarta: Kemenkominfo.

Internets

Alu Oleo University), "Penggunaan Digital Forensik dalam Pembuktian Tindak Pidana," https://journal.uho.ac.id/index.php/holresch/article/download/788/444/3299)

Bareskrim Polri, "Tim Siber Ungkap Teknologi Deepfake Catut Nama Pejabat Negara," 2025, https://pusiknas.polri.go.id/detail_artikel/tim_siber_ungkap_teknologi_deepfake_catut_nama_pejabat_negara)

BPS, "Digital Forensic Infrastructure Data in Indonesia," 2025.

Council of Europe, "Benefits of the Budapest Convention," 2025, https://www.coe.int/en/web/cybercrime/the-budapest-convention

Fakultas Kedokteran UNS, "Pentingnya Ahli Forensik dalam Sistem Peradilan Pidana Indonesia," https://fk.uns.ac.id/index.php/berita/detail/662/pentingnya-ahli-forensik-dalam- sistem-peradilan-pidana-indonesia)

Hukumonline, "Chain of Custody Berbasis Blockchain dalam Penanganan Bukti Digital," https://www.hukumonline.com/berita/a/chain-of-custody-berbasis-blockchain-dalam- penanganan-bukti-digital-lt64ce49bc3bf67/)

Hukumonline, "Dasar Hukum Cybercrime secara Internasional dan Nasional," 2025), https://www.hukumonline.com/klinik/a/dasar-hukum-cybercrime-secara-internasional-dan- nasional-lt68369a29bbb93/

Islamic University of Indonesia, "Legality of Electronic Evidence in the Criminal Justice System")," https://journal.uii.ac.id/Lex-Renaissance/article/download/12736/pdf/28707)

Mahasiswaindonesia.id, "Pembaharuan Hukum Forensik Digital dalam Pembuktian Tindak Pidana Kejahatan Siber," 2025, https://mahasiswaindonesia.id/pembaharuan-hukum-forensik- digital-dalam-pembuktian-tindak-pidana-kejahatan-siber/

Universitas Airlangga, "Pakar Hukum Siber UNAIR: Indonesia Harus Meratifikasi Budapest Convention," 2022, https://unair.ac.id/pakar-hukum-siber-unair-indonesia-harus-meratifikasi- budapest-convention/

Universitas Airlangga, "Pakar Hukum Siber UNAIR: Indonesia Harus Meratifikasi Budapest Convention," 2022, https://unair.ac.id/pakar-hukum-siber-unair-indonesia-harus-meratifikasi- budapest-convention/

Universitas Airlangga, "Pakar Hukum Siber UNAIR: Indonesia Harus Meratifikasi Budapest Convention," 2022, https://unair.ac.id/pakar-hukum-siber-unair-indonesia-harus-meratifikasi- budapest-convention/

Universitas Halu Oleo, "Penggunaan Digital Forensik dalam Pembuktian Tindak Pidana," https://journal.uho.ac.id/index.php/holresch/article/download/788/444/3299)

Universitas Islam Indonesia, "Kajian Tentang Chain of Custody Bukti Digital," https://informatics.uii.ac.id/2020/01/10/kajian-tentang-chain-of-custody-bukti-digital- hantarkan-yudi-prayudi-meraih-gelar-doktor-bidang-forensik-digital/)

Universitas Islam Indonesia, "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana," https://journal.uii.ac.id/Lex-Renaissance/article/download/12736/pdf/28707)

Universitas Islam Indonesia, "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana," https://journal.uii.ac.id/Lex-Renaissance/article/download/12736/pdf/28707

Universitas Islam Indonesia, "Pembuktian 4.0 dalam Pembaharuan Acara Pidana," https://law.uii.ac.id/blog/2025/11/10/pembuktian-4-0-dalam-pembaharuan-acara-pidana/

Verihubs, "Deepfake di Indonesia: Prabowo dan Jokowi jadi Korbannya," 2025, https://verihubs.com/blog/kasus-deepfake-indonesia

Wikipedia, "Budapest Convention on Cybercrime," 2025, https://en.wikipedia.org/wiki/Budapest_Convention_on_Cybercrime