



## Deepfake Sexual Abuse and Digital Evidence under Indonesia's New Criminal Procedure Code

Khodijah Asshofiah<sup>1\*</sup>, Humairourrohmah binti Mastor<sup>2</sup>, Maryam<sup>3</sup>, Fitrahtul Saahira Khairunnisa<sup>4</sup>

<sup>1,3-4</sup> Universitas Islam Negeri Raden Mas Said Surakarta, Indonesia

<sup>2</sup> Universiti Islam Selangor, Malaysia

Email: [asshofiahkhodijah@gmail.com](mailto:asshofiahkhodijah@gmail.com)<sup>1</sup>

### Article Info :

Received:  
24-09-2026  
Revised:  
07-10-2026  
Accepted:  
21-10-2026

### Abstract

*This article examines the evidentiary consequences of synthetic sexual imagery in Indonesian criminal procedure after the enactment of Law No. 20 of 2025 on the Criminal Procedure Code. It uses doctrinal and case-based analysis centered on Semarang District Court Decision No. 12/Pid.Sus/2026/PN Sng and, as a pre-deepfake comparator, Bojonegoro District Court Decision No. 125/Pid.Sus/2019/PN Bjn. The study integrates Article 235 of the new KUHP, Article 5 of the Electronic Information and Transactions Law, the Sexual Violence Crime Law, the Pornography Law, and relevant constitutional jurisprudence. The findings distinguish legal admissibility from forensic reliability. Electronic files may qualify as evidence, yet synthetic media creates a separate authentication problem involving provenance, device linkage, metadata, hashing, generation history, and chain of custody. The new KUHP's express recognition of electronic evidence and its authenticity requirement provides a stronger procedural basis for scrutinizing manipulated content, but statutory recognition does not by itself establish authorship or integrity. The article proposes an evidence matrix for courts that separates content identification, source attribution, technical authenticity, lawful acquisition, and victim-centered proof.*

**Keywords:** Deepfake, Digital Evidence, Electronic Evidence, New KUHP, Sexual Violence.



©2026 Authors.. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.  
(<https://creativecommons.org/licenses/by-nc/4.0/>)

## INTRODUCTION

Generative artificial intelligence has changed the evidentiary structure of image-based sexual abuse. A manipulated sexual image can be visually persuasive without documenting an event that occurred, while the underlying act of creation may still produce serious privacy, dignity, and psychological harms. Deepfake technology therefore presents two distinct legal questions: how substantive criminal law characterizes non-consensual synthetic sexual content, and how criminal procedure proves that a particular accused created, possessed, transmitted, or distributed the relevant electronic files. Technical realism makes those questions harder to collapse into ordinary visual identification (Mirsky & Lee, 2022; Westerlund, 2019).

Indonesia acquired an unusually concrete setting for this problem in 2026. Semarang District Court case No. 12/Pid.Sus/2026/PN Sng concerned AI-generated pornographic content made from images of identifiable women, and public reporting records a conviction under Article 407(1) of Law No. 1 of 2023 on the Criminal Code. The case is important because it emerged just as the new Criminal Procedure Code, Law No. 20 of 2025, came into force and expressly listed electronic evidence in Article 235(1)(f). Article 235 also requires authentication and lawful acquisition, giving courts a textual basis for distinguishing the existence of a digital file from its evidentiary reliability (Semarang District Court, 2026; Republic of Indonesia, 2025).

The legal framework is multi-layered. Article 5 of Law No. 1 of 2024 recognizes electronic information, electronic documents, and their printouts as lawful evidence, subject to the statutory framework governing electronic systems. Law No. 12 of 2022 on Sexual Violence Crimes separately regulates electronic-based sexual violence in Article 14, including non-consensual recording, sexual transmission, and electronic stalking, while Law No. 44 of 2008 on Pornography remains relevant to prohibited pornographic production and distribution. The national Criminal Code supplies additional substantive provisions after its entry into force. These statutes overlap in object but differ in protected

interest, prohibited conduct, complaint structure, and proof (Republic of Indonesia, 2008, 2022, 2023, 2024).

Deepfake sexual abuse also exposes a conceptual limitation in older evidence practice. Traditional image evidence often carries an intuitive assumption that the image depicts an external event, so disputes focus on who captured it, whether it was altered, and whether it is connected to the accused. Synthetic media disrupts that assumption because the file may be authentic as a file yet false as a depiction. The evidentiary inquiry must therefore distinguish file integrity from representational truth, and both from attribution of the generative process to a person or device. Scholarship on digital forensics consistently treats provenance and chain of custody as central to this distinction (Casey, 2011; Mason & Seng, 2017).

Constitutional jurisprudence adds a legality constraint. Constitutional Court Decision No. 20/PUU-XIV/2016 interpreted electronic evidence provisions in relation to lawfully obtained recordings and the statutory authority for interception. The decision does not resolve deepfake authentication, but it reinforces a basic proposition now made explicit in Article 235 of the new KUHAP: evidence cannot be separated from the legality of acquisition. This is particularly relevant where investigators obtain cloud accounts, private devices, messaging records, or intercepted communications while attempting to establish the production history of synthetic material (Constitutional Court of Indonesia, 2016).

Victim-centered analysis is equally necessary. Image-based sexual abuse literature demonstrates that harm is not limited to the circulation of an original intimate image; manipulation, threatened distribution, repeated discoverability, and loss of informational control can generate comparable forms of abuse (McGlynn & Rackley, 2017; McGlynn, Rackley, & Houghton, 2017). Recent legal scholarship on intimate deepfakes similarly argues that consent, sexual autonomy, and representational integrity must be considered even when the depicted sexual event never occurred (Karagianni & Doh, 2024). The evidentiary framework should therefore avoid requiring victims to prove the falsity of an image in ways that reproduce its degrading content unnecessarily.

A useful comparator is Bojonegoro District Court Decision No. 125/Pid.Sus/2019/PN Bjn, which involved manipulated pornographic photographs used as threats before generative AI became widely accessible. The decision, and later scholarship analyzing it, shows that Indonesian courts already confronted edited sexual imagery through the ITE Law and related offences. Deepfakes differ in scale, automation, and realism, but the comparator reveals continuity in core questions of manipulation, authorship, distribution, and evidentiary linkage (Mahanani & Sulistyanta, 2022). The shift from manual editing to generative synthesis therefore intensifies rather than replaces earlier proof problems.

This article asks how the new KUHAP should structure the proof of deepfake sexual abuse and what the 2026 Semarang case reveals about the relationship between statutory admissibility and forensic reliability. The contribution is an integrated legal-evidentiary matrix that separates five inquiries: content identification, source attribution, technical authenticity, lawful acquisition, and victim-centered corroboration. The framework is designed for doctrinal use and does not assert that a particular forensic technique is always required. It identifies the evidentiary functions that must be satisfied when synthetic media becomes central to criminal adjudication.

## RESEARCH METHODS

This research uses normative legal research with statute, case, conceptual, and comparative-evidentiary approaches. Primary materials include Law No. 20 of 2025 on the Criminal Procedure Code, Law No. 1 of 2024 amending the Electronic Information and Transactions Law, Law No. 12 of 2022 on Sexual Violence Crimes, Law No. 44 of 2008 on Pornography, Law No. 1 of 2023 on the Criminal Code, Constitutional Court Decision No. 20/PUU-XIV/2016, Semarang District Court Decision No. 12/Pid.Sus/2026/PN Smg, and Bojonegoro District Court Decision No. 125/Pid.Sus/2019/PN Bjn. Public court records and reliable reporting are used only to establish case chronology where the full judgment is not uniformly accessible online.

The analysis codes the legal materials across five evidentiary functions: identification of the alleged sexual content, attribution to a person or account, authentication and integrity of the electronic file, lawful acquisition and chain of custody, and corroboration of distribution or victim impact. The coding framework is informed by digital-evidence scholarship, ISO/IEC 27037 principles, and literature on image-based sexual abuse and deepfake detection. It does not treat an automated detector score as

dispositive. Instead, technical methods are evaluated according to the legal proposition they can support and the uncertainty they leave unresolved.

## RESULTS AND DISCUSSION

### Substantive Offences and the Evidentiary Object of Synthetic Sexual Content

The first analytical task is to identify the legal object being proved. In a conventional pornography case, the prosecution may rely heavily on the content of an image or video to show that the material falls within a prohibited category. Deepfake content requires an additional step because the apparent sexual act may be synthetic while the use of a real person's likeness is itself central to the alleged harm. The court therefore needs to separate what the file depicts, how it was generated, and what conduct the accused is alleged to have performed with it (Hörnle, 2026a; Umbach et al., 2026).

Article 407(1) of the 2023 Criminal Code, as publicly reported in the Semarang case, provided the basis for conviction. The significance for evidence is that the prosecution must connect the content to the statutory elements actually charged rather than prove 'deepfake' as a free-standing offence label. Synthetic generation can be a factual mechanism through which prohibited pornographic content is produced, but the legal characterization follows the charged norm. This avoids making novelty of technology substitute for statutory analysis (Semarang District Court, 2026; Monatares et al., 2026).

**Table 1. Principal Indonesian Norms Relevant to Deepfake Sexual Content**

| Instrument                     | Provision              | Regulated object/function                                                      | Evidentiary implication                                                       |
|--------------------------------|------------------------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Law No. 1/2023 (Criminal Code) | Art. 407(1)            | Pornographic production/related prohibited conduct as charged in Semarang case | Content and accused's conduct must match statutory elements                   |
| Law No. 12/2022 (TPKS)         | Art. 14                | Electronic-based sexual violence                                               | Consent, electronic act, and sexual character become distinct proof questions |
| Law No. 44/2008                | Pornography provisions | Production/distribution/other pornography-related conduct                      | Requires proof of conduct falling within the charged provision                |
| Law No. 1/2024 (ITE amendment) | Art. 5                 | Status of electronic information/documents as lawful evidence                  | File may qualify as evidence subject to procedural and system requirements    |
| Law No. 20/2025 (KUHAP)        | Art. 235               | Electronic evidence, authenticity, lawful acquisition                          | Authentication and legality are express admissibility questions               |

Table 1 shows that no single statute answers every deepfake question. Substantive offence, evidentiary status, authentication, and consent operate through different provisions. Law No. 12 of 2022 creates a separate route through electronic-based sexual violence. Article 14 addresses specified electronic conduct undertaken without consent, including sexual recording or screenshots, transmission of sexual electronic information, and electronic stalking. The text was not drafted exclusively for generative AI, so application to synthetic content requires careful interpretation of the relevant verb, object, and consent element. A court should identify whether the prosecution relies on production, transmission, threat, deception, or another act rather than assume that all deepfake conduct falls within the same statutory paragraph.

Law No. 44 of 2008 remains relevant where production, possession, facilitation, or dissemination falls within its provisions. Its relationship with later sexual-violence legislation and the new Criminal Code must be resolved through ordinary principles of statutory interpretation, including specificity and temporal relationship. The evidentiary consequence is practical: different charges may require proof of

different acts, mental states, and dissemination pathways. A technically identical file can therefore have different evidentiary significance under different substantive provisions.

The Bojonegoro comparator illustrates this point. Decision No. 125/Pid.Sus/2019/PN Bjn involved edited pornographic images used in threatening communication, and published legal analysis records the use of Article 29 of the ITE Law in the conviction. The image manipulation was important but not the sole object of proof; the threat and communication context supplied the legal connection to the charged offence (Mahanani & Sulistyanta, 2022). Deepfake cases likewise require courts to resist treating the disturbing visual output as a substitute for proof of the specific prohibited act.

**Table 2. Case Comparison: Manipulated Sexual Imagery Before and After Generative AI**

| Feature                | PN 125/Pid.Sus/2019                           | Bojonegoro      | PN 12/Pid.Sus/2026                                                 | Semarang             | Evidentiary significance                            |
|------------------------|-----------------------------------------------|-----------------|--------------------------------------------------------------------|----------------------|-----------------------------------------------------|
| Manipulation technique | Edited pornographic photograph                |                 | AI/deepfake sexual imagery                                         |                      | Technology changes scale and forensic traces        |
| Core legal context     | Threatening communication under ITE framework | under           | Pornographic production under 2023 Criminal Code, as reported      |                      | Charge determines elements to prove                 |
| Digital linkage        | Chat/application edited image                 | and             | Large corpus of generated files and digital production environment |                      | Attribution requires account/device evidence        |
| Victim interest        | Threat, reputational harm                     | dignity,        | Non-consensual sexualization and psychological harm                | synthetic and        | Consent and victim impact require independent proof |
| Procedural environment | Old KUHAP sectoral evidence rules             | plus electronic | New KUHAP recognizes evidence                                      | expressly electronic | Authentication becomes textually explicit           |

The comparison indicates continuity in manipulation and attribution problems, but the new KUHAP supplies a more explicit procedural vocabulary for authentication. Consent also operates differently across evidentiary questions. A person may have consented to publication of an ordinary portrait but not to its sexual manipulation; conversely, a prosecution may need to prove lack of consent only where the charged statute makes it an element. Image-based sexual abuse scholarship treats contextual consent as narrower than general possession of an image (McGlynn & Toparlak, 2025). This distinction is legally useful because it prevents the existence of a publicly available source photograph from being treated as consent to synthetic sexualization.

The victim's testimony can establish identity, absence of consent, discovery of the content, and resulting consequences, but it does not by itself establish who generated the file. Device evidence, account records, local project files, prompts, payment records, cloud histories, or transmission logs may supply the attribution layer. Separating these propositions protects both complainants and defendants: victims are not burdened with proving technical authorship, while attribution is not inferred merely from the offensive character of the content.

The evidentiary object is therefore modular. Content classification, non-consent, authorship, possession, production, and dissemination are related but analytically separate propositions. A clear charge-to-evidence map is particularly important in synthetic-media cases because the same visual artefact can otherwise dominate reasoning and obscure which statutory element each item of evidence actually proves.

### **Authentication, Integrity, and Lawful Acquisition under Article 235 KUHAP**

Article 235 of Law No. 20 of 2025 materially changes the doctrinal starting point for digital proof. Paragraph (1)(f) expressly lists electronic evidence, while paragraph (3) requires evidence to be authenticable and lawfully obtained. Paragraphs (4) and (5) authorize the judge to assess authenticity and legality and exclude evidence found unauthentic or unlawfully acquired. The structure turns

authentication from an implied technical concern into an express legal question (Republic of Indonesia, 2025).

Authentication should not be confused with truth. A hash value can demonstrate that a file has not changed between two forensic acquisitions, but it cannot prove that the scene depicted in the file occurred. Metadata can reveal creation time, software, device information, or editing history, but metadata may be absent, altered, or stripped by social-media platforms. Deepfake detection tools may estimate whether content bears synthetic traces, yet their outputs can be sensitive to compression, model updates, and unseen generation techniques (Mirsky & Lee, 2022; Sandoval et al., 2024).

**Table 3. Authentication Layers for Synthetic Media Evidence**

| Layer                      | Typical evidence                                           | Legal proposition                                      | Residual uncertainty                      |
|----------------------------|------------------------------------------------------------|--------------------------------------------------------|-------------------------------------------|
| Identity                   | File name, visual content, exhibit number                  | Which item is before the court                         | Does not establish origin                 |
| Integrity                  | Hash values, forensic image, copy logs                     | Item remained unchanged after acquisition              | Does not prove depiction is real          |
| Provenance                 | Metadata, application artefacts, project files             | How/where file was created or processed                | Metadata may be incomplete or manipulable |
| Synthetic-content analysis | Expert examination, detector outputs, compression analysis | Likelihood and method of manipulation                  | Model error and novel generators          |
| Attribution                | Device control, accounts, prompts, payments, logins        | Connection between accused and generation/distribution | Shared devices or compromised accounts    |
| Lawful acquisition         | Warrant/order/consent and procedural record                | Legality of state access                               | Separate from technical reliability       |

No layer in Table 3 is sufficient for every case. Strong proof arises when the layers converge on the propositions required by the charge. The most reliable approach is cumulative. Investigators can preserve the original device or account environment, create a forensic image, calculate cryptographic hashes, record acquisition steps, preserve relevant application and browser artefacts, and identify project or prompt traces where they exist. Each step supports a different proposition. ISO/IEC 27037 and digital-forensics scholarship emphasize identification, collection, acquisition, and preservation as related stages designed to maintain traceability of digital evidence (ISO/IEC, 2012; Casey, 2011).

Source attribution requires even more than file authentication. A device containing deepfake outputs does not necessarily prove that the owner personally generated them, particularly where devices are shared or accounts are compromised. Attribution can be strengthened through account credentials, payment records for generation services, prompt histories, local cache files, user-specific communication, login records, and testimony about control of the device. The legal standard remains one of proof within the criminal process; the technical artefacts are inferential components rather than self-executing conclusions.

Lawful acquisition is a separate axis. Constitutional Court Decision No. 20/PUU-XIV/2016 demonstrates that electronic evidence obtained through interception must be connected to lawful authority. The new KUHAP generalizes the relevance of lawful acquisition by making it part of Article 235's admissibility structure. Investigators handling private cloud repositories, seized devices, or platform records must therefore be able to identify the legal basis for access in addition to the forensic steps used to preserve integrity (Constitutional Court of Indonesia, 2016; Komalasari & Mustafa, 2023).

**Table 4. Chain-of-Custody Record for Deepfake Investigations**

| Stage                | Minimum record                                    | Integrity control                          | Courtroom relevance                                  |
|----------------------|---------------------------------------------------|--------------------------------------------|------------------------------------------------------|
| Seizure/collection   | Date, place, collector, device/account identifier | Photograph and unique identifier           | Links exhibit to source                              |
| Forensic acquisition | Tool/version, method, examiner                    | Bitstream copy and hash where feasible     | Demonstrates reproducibility                         |
| Analysis             | Working copy, analytical steps, software          | Preserve master image; log transformations | Separates examination from source alteration         |
| Transfer/storage     | Custodian, date/time, destination                 | Access control and audit trail             | Explains custody continuity                          |
| Presentation         | Exhibit mapping and derivative files              | Hash/link to examined source               | Shows that courtroom display corresponds to evidence |

The record described in Table 4 is not a rigid statutory checklist. It is a practical means of satisfying the authenticity and traceability concerns made legally salient by Article 235. Chain of custody becomes especially important when the evidence is repeatedly copied for forensic examination, prosecution disclosure, and courtroom presentation. A documented chain should identify who collected the device or data, when it was acquired, what method was used, the hash or other integrity identifier, each transfer, and the relationship between the examined copy and the original source. Gaps do not automatically establish fabrication, but they weaken the capacity to demonstrate that the item examined is the item seized. This is precisely the kind of uncertainty Article 235's authentication requirement is positioned to address.

Automated deepfake detection should be treated as expert-assisted evidence rather than as a substitute for legal authentication. Detection models can help identify anomalies and guide forensic analysis, but adversarial adaptation and rapid changes in generative methods create non-trivial error risks. Peer-reviewed technical literature therefore supports ensemble and provenance-oriented approaches rather than exclusive reliance on a single classifier (Mirsky & Lee, 2022; Sandoval et al., 2024). In legal terms, a detector answers a narrow technical question and must be contextualized with expert methodology, validation, and case-specific limitations.

Article 235 can thus support a layered authentication model. The judge can ask whether the electronic item is the same item acquired, whether acquisition was lawful, whether its technical history is sufficiently documented, whether the alleged synthetic nature is supported by competent evidence, and whether the item can be attributed to the accused. This model gives independent content to authenticity without turning courts into forensic laboratories.

### **Victim-Centered Corroboration and a Judicial Evidence Matrix**

A technically rigorous case can still mishandle the victim dimension if courtroom proof unnecessarily reproduces intimate synthetic content. Image-based sexual abuse scholarship emphasizes that repeated viewing, copying, and circulation can extend the harm caused by the original act (McGlynn & Rackley, 2017; McGlynn et al., 2021). Evidentiary management should therefore pursue necessity and minimization. Courts can establish identity, non-consent, and content characteristics through controlled exhibits, expert descriptions, and limited access without treating unrestricted reproduction as the default.

Victim testimony has distinct evidentiary value. It can establish that the source portrait was taken in a non-sexual context, that no consent was given for sexual manipulation, how the synthetic material was discovered, whether threats or dissemination occurred, and what consequences followed. Those propositions should be separated from technical questions that require expert or digital evidence. This division avoids the common error of asking a victim to authenticate the generation process simply because the depicted face is theirs.

**Table 5. Victim-Centered Evidentiary Propositions**

| Proposition                    | Primary source of proof                             | Supplementary source                     | Minimization measure                     |
|--------------------------------|-----------------------------------------------------|------------------------------------------|------------------------------------------|
| Identity of depicted person    | Victim testimony / known source image               | Witness recognition                      | Use limited comparison exhibits          |
| Absence of consent             | Victim testimony and communication history          | Platform/account records                 | Avoid irrelevant sexual-history evidence |
| Discovery and dissemination    | Victim/witness testimony                            | URLs, messages, platform logs            | Restrict reproduction of explicit files  |
| Psychological or social impact | Victim testimony; professional evidence if relevant | Contemporaneous records                  | Limit repetitive recounting              |
| Authorship/generation          | Device/account forensic evidence                    | Expert testimony, prompts, project files | Do not shift technical burden to victim  |

Table 5 separates victim evidence from technical attribution. This reduces both evidentiary confusion and unnecessary exposure to the synthetic material. Corroboration may also be distributed across witnesses and electronic sources. Platform notifications, messages from third parties, complaint reports, links, screenshots, account identifiers, and preserved URLs can demonstrate dissemination. However, screenshots should be treated as representations of a digital interaction rather than as self-proving originals. Where the underlying account or device can be examined, the evidentiary record should explain how the screenshot corresponds to the source data (Mason & Seng, 2017; Samudra, Basu, & Saenz Perez, 2026).

The Semarang case illustrates why scale matters. Public reporting described approximately 1,100 pornographic photo and video files. A large corpus can support inferences about systematic production, but volume does not remove the need to establish representative samples, provenance, and attribution. A court need not conduct identical forensic analysis on every file if evidentiary rules permit representative proof, yet the selection method should be transparent so that the scale claim is not divorced from verified items.

Expert evidence can assist with manipulation method, file structure, metadata, and the limits of detection. Article 235 does not specify a single technical threshold, so judicial evaluation should focus on method, reproducibility, and fit with the proposition being proved. An expert who concludes that a file is likely synthetic does not necessarily establish who created it; an examiner who links a project file to a seized device may provide stronger attribution even without a universal deepfake-detection score. The matrix therefore separates expertise by function.

Defense testing is also important. The new KUHP's authentication requirement has practical meaning only if the defense can understand the acquisition method, examine relevant forensic reports, and contest attribution or integrity. Disclosure of sensitive victim material must be controlled, but procedural equality does not require either unrestricted circulation or complete opacity. A structured access protocol can reconcile defense rights with privacy and victim protection, consistent with the broader principle that evidentiary reliability depends on contestability.

**Table 6. Proposed Judicial Matrix for Deepfake Electronic Evidence**

| Question            | Required legal focus         | Indicative evidence           | Reasoned finding should state           |
|---------------------|------------------------------|-------------------------------|-----------------------------------------|
| 1. What is charged? | Elements of specific offence | Indictment and statutory text | Conduct and mental element to be proved |

|                                           |                                        |                                                 |                                         |
|-------------------------------------------|----------------------------------------|-------------------------------------------------|-----------------------------------------|
| 2. What electronic item is relied on?     | Relevance and identity                 | Exhibit mapping, source device/account          | Connection between item and element     |
| 3. Is it authentic and lawfully obtained? | KUHAP Art. 235                         | Hashes, acquisition log, legal authority        | Integrity and legality                  |
| 4. Is it synthetic and how?               | Technical reliability                  | Expert analysis, metadata, generator artefacts  | Method and uncertainty                  |
| 5. Who is attributable?                   | Authorship/control/distribution        | Accounts, device control, prompts, transactions | Inference connecting accused to conduct |
| 6. What victim facts remain?              | Consent, identity, harm, dissemination | Testimony and corroboration                     | Independent victim-centered findings    |

The matrix is intended to organize judicial reasoning, not to impose a single forensic technology. It preserves the distinction between legal admissibility and the weight of technical evidence. The judicial matrix developed here uses five questions in sequence: What conduct is charged? What electronic item proves each element? Is the item authentic and lawfully obtained? What evidence attributes the relevant act to the accused? What victim-related propositions remain to be established independently? The sequence prevents visual shock from becoming an evidentiary shortcut. It also gives courts a disciplined way to explain why a particular file, device, account, or testimony carries probative weight.

Synthetic sexual imagery will continue to evolve faster than statutory terminology. The new KUHAP nevertheless provides durable procedural concepts authenticity, legality, judicial evaluation, and electronic evidence that can accommodate technological change if applied with forensic specificity. The strongest doctrinal response is therefore not to create a presumption that deepfakes are inherently unreliable, but to require proof that distinguishes file integrity, representational falsity, and human attribution.

## CONCLUSION

Deepfake sexual abuse requires Indonesian criminal procedure to separate questions that conventional visual evidence often allowed courts to combine. The electronic file may be admissible, intact, and lawfully acquired while still depicting an event that never occurred; conversely, a synthetic file can accurately evidence the accused's act of generation or distribution even though its sexual scene is fictitious. Law No. 20 of 2025 supplies a stronger procedural basis for this distinction by expressly recognizing electronic evidence and requiring authentication and lawful acquisition in Article 235. When read with Article 5 of the ITE Law, the Sexual Violence Crime Law, the Pornography Law, and substantive provisions of the new Criminal Code, the central evidentiary problem becomes one of layered proof rather than categorical acceptance or rejection of synthetic media.

The Semarang and Bojonegoro cases show continuity in the need to connect manipulated sexual imagery to specific criminal conduct, while generative AI increases the scale and sophistication of the attribution problem. A defensible evidentiary record should document integrity, provenance, acquisition authority, source attribution, and the precise victim-related facts required by the charge. Hashes, metadata, detector outputs, devices, accounts, prompts, and expert testimony each answer different questions and should not be treated as interchangeable. The proposed judicial matrix provides a structured basis for explaining those distinctions. Future empirical research should examine published 2026–2028 judgments under Article 235 to determine how Indonesian courts operationalize authenticity, chain of custody, and expert proof in synthetic-media cases.

## REFERENCES

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet (3rd ed.)*. Academic Press.

- Constitutional Court of Indonesia. (2016). Decision No. 20/PUU-XIV/2016 concerning electronic information and electronic documents as evidence.
- Hörnle, J. (2026a). Deepfake intimate images and criminal law: Part I. *International Journal of Law and Information Technology*. <https://doi.org/10.1093/ijlit/eaag006>.
- Hörnle, J. (2026b). Deepfake intimate images and criminal law: Part II. *International Journal of Law and Information Technology*. <https://doi.org/10.1093/ijlit/eaag007>.
- ISO/IEC. (2012). ISO/IEC 27037:2012: Guidelines for identification, collection, acquisition and preservation of digital evidence.
- Karagianni, A., & Doh, M. (2024). Intimate deepfakes, sexual autonomy and legal regulation. *Porn Studies*. <https://doi.org/10.1080/23268743.2024.2408277>.
- Komalasari, R., & Mustafa, C. (2023). Digital evidence in Indonesian criminal procedure: Reliability, admissibility and procedural safeguards. *Jurnal Hukum dan Peradilan*, 12(3), 547–580. <https://doi.org/10.25216/jhp.12.3.2023.547-580>.
- Mahanani, A., & Sulistyanta. (2022). Tinjauan yuridis tindak pidana pengancaman dengan foto rekayasa bermuatan pornografi (Studi Putusan Nomor 125/Pid.Sus/2019/PN Bjn). *Recidive*, 11(1), 36–47. <https://doi.org/10.20961/recidive.v11i1.67433>.
- Mason, S., & Seng, D. (Eds.). (2017). *Electronic evidence (4th ed.)*. Institute of Advanced Legal Studies.
- McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies*, 37(3), 534–561. <https://doi.org/10.1093/ojls/gqw033>.
- McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond revenge porn: The continuum of image-based sexual abuse. *Feminist Legal Studies*, 25, 25–46. <https://doi.org/10.1007/s10691-017-9343-2>.
- McGlynn, C., Johnson, K., Rackley, E., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2021). ‘It’s torture for the soul’: The harms of image-based sexual abuse. *Social & Legal Studies*, 30(4), 541–562. <https://doi.org/10.1177/0964663920947791>.
- McGlynn, C., & Toparlak, R. (2025). The legal regulation of sexually explicit deepfakes: Consent, dignity and sexual autonomy. *Journal of Law and Society*. <https://doi.org/10.1111/jols.12527>.
- Mirsky, Y., & Lee, W. (2022). The creation and detection of deepfakes: A survey. *ACM Computing Surveys*, 54(1), 1–41. <https://doi.org/10.1145/3425780>.
- Monatares, C., Holijah, Andriy, P. R., Ramadhani, N., & Perdana, I. (2026). Kesenjangan regulasi hukum pidana terhadap kejahatan deepfake: Studi kasus manipulasi konten asusila dalam Putusan Pengadilan Negeri Semarang. *Journal of Law and Legal System*, 2(1), 154–166. <https://doi.org/10.61994/jlls.v2i1.1925>.
- Republic of Indonesia. (2008). Law No. 44 of 2008 concerning Pornography.
- Republic of Indonesia. (2022). Law No. 12 of 2022 concerning Sexual Violence Crimes.
- Republic of Indonesia. (2023). Law No. 1 of 2023 concerning the Criminal Code.
- Republic of Indonesia. (2024). Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.
- Republic of Indonesia. (2025). Law No. 20 of 2025 concerning the Criminal Procedure Code.
- Samudra, A. H., Basu, S., & Saenz Perez, M. (2026). Electronic evidence and the reconstruction of criminal proof in Indonesia. *Journal of Indonesian Legal Studies*, 11(1). <https://doi.org/10.15294/jils.v11i1.35378>.
- Sandoval, M. M., et al. (2024). Deepfake detection and digital forensic challenges: A systematic assessment. *Crime Science*, 13, 41. <https://doi.org/10.1186/s40163-024-00239-1>.
- Semarang District Court. (2026). Decision No. 12/Pid.Sus/2026/PN Sng.
- Bojonegoro District Court. (2019). Decision No. 125/Pid.Sus/2019/PN Bjn.
- Umbach, R., Henry, N., Beard, G., & Berryessa, C. M. (2026). Non-consensual intimate deepfakes: Harm, perception and legal responses. *Computers in Human Behavior*, 179, 108935. <https://doi.org/10.1016/j.chb.2026.108935>.
- Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 39–52. <https://doi.org/10.22215/timreview/1282>.
- Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of minors: Characteristics and dynamics. *Journal of Adolescent Health*, 62(1), 72–79. <https://doi.org/10.1016/j.jadohealth.2017.08.014>.

- Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse*, 19(2), 195–208. <https://doi.org/10.1177/1524838016650189>.
- Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, 1753–1819.
- Franks, M. A. (2017). Revising the revenge porn agenda: A commentary on Henry and Powell. *Sexualization, Media, & Society*, 3(2). <https://doi.org/10.1177/2374623817706392>.
- Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, 18, 199–210. <https://doi.org/10.1007/s10676-016-9406-0>.
- Powell, A., Scott, A. J., Flynn, A., & Henry, N. (2020). Image-based sexual abuse: An international study of victims and perpetrators. *Criminology & Criminal Justice*, 20(5), 565–584. <https://doi.org/10.1177/1748895819871542>.
- Powell, A., Henry, N., Flynn, A., & Scott, A. J. (2019). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample. *Computers in Human Behavior*, 92, 393–402. <https://doi.org/10.1016/j.chb.2018.11.009>.