

DOI: <https://doi.org/10.38035/gijlss.v4i4><https://creativecommons.org/licenses/by/4.0/>

Received: 30 August 2026 | Revised: 05 October 2026 | Accepted: 15 October 2026

The Execution of Deletion of Electronic Evidence Following Criminal Verdicts under Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions

Gracia Wulandari Manurung^{1*}, Prija Djatmika², Faizin Sulistio³

¹Universitas Brawijaya, Malang, Indonesia, graciawulandari@student.ub.ac.id

²Universitas Brawijaya, Malang, Indonesia, prija.djatkika@ub.ac.id

³Universitas Brawijaya, Malang, Indonesia, faizin@ub.ac.id

*Corresponding Author: graciawulandarim@gmail.com¹

Abstract: Intimate and other unlawful sexual content seldom stays on the device that police seize from an offender, so the fate of electronic evidence after a criminal verdict matters to victims long after sentencing. Indonesian law does not lack removal tools. Law Number 12 of 2022 on Sexual Violence Crimes authorizes the central government to delete or terminate access to electronic content containing sexual violence (Article 46), allows a prosecutor to ask the chief of a district court to order the communications ministry to delete such content (Article 47), and recognizes the victim's right to its removal (Articles 68(g) and 70(2)(l)), with procedures now laid down in Government Regulation Number 30 of 2025. Article 40 of the Electronic Information and Transactions Law, as amended by Law Number 1 of 2024, provides for access termination, and Articles 43 to 45 of Law Number 27 of 2022 impose deletion, destruction, and notification duties on data controllers. Using statute, case, and conceptual approaches, this normative study asks how these instruments connect with the disposition and execution of electronic evidence under Law Number 8 of 1981 and Law Number 20 of 2025. It examines Decision Number 47/Pid.Sus/2025/PN Bhn, as amended on appeal by Decision Number 251/PID.SUS/2025/PT BGL, and Decision Number 74/Pid.Sus/2026/PN Bdg, classifying their procedural regime under Article 361 of Law Number 20 of 2025 on the basis of verified case chronologies. Both courts ordered seized devices and accounts to be destroyed or erased, yet neither judgment addressed copies held by platforms or recipients, named the executing authority, set a verification standard, or linked the order to the removal channels available under the Sexual Violence Crimes Law and the Electronic Information and Transactions Law. The problem lies in regulatory fragmentation and weak integration between evidence disposition and content removal, not in a normative vacuum. The study proposes an operational framework that separates preservation, secure destruction, platform takedown, access termination, and de-indexing, and that marks where positive law ends and reform begins.

Keywords: Electronic Evidence, Evidence Disposition, Content Removal, Non-Consensual Intimate Imagery, Sexual Violence Crimes Law.

INTRODUCTION

Smartphones and messaging platforms have changed the way sexual harm is inflicted in Indonesia. A private video call can be screen-recorded without consent and forwarded within minutes to a campus WhatsApp group, while a pornographic clip reposted on a public X account stays retrievable long after the first upload. Comparative scholarship calls this conduct image-based sexual abuse and treats removal of the material as part of the remedy rather than as an administrative afterthought (Huber, 2025; Rigotti et al., 2024; O'Connell, 2020). Indonesian criminal law reaches the conduct through more than one statute. Article 27 paragraph (1) of Law Number 11 of 2008 on Electronic Information and Transactions, as last amended by Law Number 1 of 2024 (the ITE Law), prohibits distributing, transmitting, or making accessible electronic information whose content violates decency for public knowledge, and Article 27B paragraph (2) penalizes coercion through threats of defamation or of disclosing a secret. Law Number 12 of 2022 on Sexual Violence Crimes (the TPKS Law) adds a victim-centred layer: Article 14 penalizes, as electronic-based sexual violence, the recording or screen capture of sexual content without the consent of the person depicted and the transmission of sexual content against the recipient's will, while Article 4 paragraph (2) letter d extends the TPKS regime to acts violating decency against the victim's will.

Electronic evidence has gained a firmer footing over the same period. Article 184 of Law Number 8 of 1981 on Criminal Procedure (the 1981 KUHP) did not list electronic material among the means of proof, so its admissibility rested on Article 5 of the ITE Law and on sectoral statutes. Article 24 paragraph (1) of the TPKS Law later recognized electronic information and documents, together with objects used in or produced by the offence, as valid evidence in sexual violence cases. Law Number 20 of 2025 on the Code of Criminal Procedure (the 2025 KUHP), in force since 2 January 2026 (Article 369), now lists object evidence (*barang bukti*) and electronic evidence (*bukti elektronik*) separately in Article 235 paragraph (1) letters e and f and requires every means of proof to be authenticated and lawfully obtained (Article 235 paragraph (3)). Scholarship on this development has concentrated on validity, authentication, and the persistence of an analogue evidentiary mindset (Samudra et al., 2026; Vanessa & Firmansyah, 2025).

Indonesia also possesses explicit removal mechanisms, and an accurate analysis has to begin with them. Article 46 paragraph (1) of the TPKS Law authorizes the central government to delete and/or terminate access to electronic information and documents containing sexual violence, and Article 47 allows a prosecutor, in the public interest, to ask the chief of a district court to order the ministry responsible for communications and informatics to delete such content. Victims hold a corresponding right to the removal of sexual content under Article 68 letter g, as part of the right to handling, and under Article 70 paragraph (2) letter l, as part of recovery before and during the judicial process. Article 46 paragraph (2) delegated the procedure to a government regulation. That regulation now exists: Chapter IV (Articles 78 to 84) of Government Regulation Number 30 of 2025, enacted on 18 June 2025, sets out who may request removal, the decision of the Attorney General's Office, the ministry's execution, and notification to the victim. Separately, Article 40 paragraphs (2a) to (2c) of the ITE Law oblige the government to prevent the dissemination of prohibited content and authorize it to terminate access or order electronic system operators to do so, with the elucidation of paragraph (2b) defining access termination to include blocking, account closure, and content deletion. Government Regulation Number 71 of 2019 adds a right to erasure and a right to delisting from

search engines (Articles 15 to 17) and allows law enforcement agencies to request, and courts to order, access termination (Article 97).

Data protection law adds a further and often misdescribed layer. Article 19 of Law Number 27 of 2022 on Personal Data Protection (the PDP Law) only identifies who may act as a personal data controller or processor, namely every person, public bodies, and international organizations. The legal bases for processing appear in Article 20, where explicit consent is one of six bases. Deletion and destruction duties sit in Articles 43 and 44, and Article 45 requires the controller to notify the data subject of deletion or destruction. Two qualifications shape how these duties apply to criminal evidence: Article 15 paragraph (1) letter b exempts certain data subject rights where law enforcement requires it, and Article 44 paragraph (1) letter c ties the destruction duty to data that no longer relate to the settlement of a legal process (Syailendra et al., 2024; Triyanti et al., 2025).

Criminal procedure governs a different object again. A conviction must state the disposition of evidence, as required by Article 197 paragraph (1) letter i of the 1981 KUHAP and now by Article 250 paragraph (1) letter i of the 2025 KUHAP. Seized objects are returned unless the court orders them confiscated for the state or destroyed (Article 46 paragraph (2) of the 1981 KUHAP and Article 135 of the 2025 KUHAP). The public prosecutor executes the final judgment (Article 270 of the 1981 KUHAP and Article 342 paragraph (1) of the 2025 KUHAP), and objects confiscated for the state go to the state auction office (Article 273 paragraph (3) of the 1981 KUHAP and Article 345 paragraph (3) of the 2025 KUHAP). Which code governs a given case during the changeover depends on Article 361 of the 2025 KUHAP, which allocates the old or new code according to the procedural stage a case had reached on 2 January 2026.

The legal question is therefore not whether Indonesia has any mechanism to remove sexual content. It has several. The question is whether the mechanisms that remove content from platforms, restrict access, protect victims, and govern personal data are connected with the disposition of evidence in a criminal judgment and with the execution of that judgment once it becomes final. A court order to destroy a seized telephone does not, by itself, reach a copy stored on a platform server or on the telephone of a group member, and the authorities that could reach those copies act on different triggers and under different statutes.

Existing studies approach parts of this problem. Purnomo et al. (2026) found that no technical mechanism governs the destruction of digital evidence in the form of electronic accounts, but their analysis is conceptual and does not examine judgments or the TPKS removal channel. Yuwono and Ikhsan (2026) note the content removal mechanisms of the TPKS Law in a comparison with Laos, while Nesi and Umar (2025) analyse the element of acting without right in the ITE decency offence. International literature discusses platform duties, intermediary liability, and the limits of takedown (Hörnle, 2026; Sahak et al., 2026; O'Connell, 2020) and the legal treatment of cloud-stored evidence and its disposal (Karagiannis & Vergidis, 2021). None of these studies traces, at the level of specific judgments, how evidence dispositions interact with the TPKS and ITE removal channels during the transition between the 1981 and 2025 codes, or separates the different objects that the single word deletion tends to cover.

This article contributes in two ways, without claiming to be the first treatment of the subject. It offers an auditable reading of two decisions whose procedural regime is determined under Article 361 from documented chronologies rather than from the year of judgment, and it proposes an operational framework that maps each object and stage of removal to existing provisions while stating plainly where positive law is silent. Three research questions follow. How did the courts dispose of electronic evidence in the two cases, and under which procedural regime? How do those dispositions relate to the removal, access termination, data protection, and victim protection mechanisms described above, and where do gaps of integration and

implementation appear? What operational framework could connect these mechanisms without compromising the preservation of evidence?

METHODS

This is normative legal research. It examines legislation, judicial decisions, and doctrine and does not collect field, survey, or interview data, so it makes no claim about how often deletion orders are executed in practice. Procedural facts were taken from official public records, namely the judgments themselves and the case-tracking system of the court concerned, and are used only to classify the cases and to describe what the records show.

The statute approach covers the 1981 KUHAP and the 2025 KUHAP (in particular Articles 1, 130, 132, 135, 140, 156, 235, 250, 323, 342, 345, 353, 361, 362, and 369, together with the provisions cited by the courts), the ITE Law as amended by Law Number 19 of 2016 and Law Number 1 of 2024 (Articles 26, 27, 27B, 40, and 45), Government Regulation Number 71 of 2019 (Articles 15 to 17 and 95 to 97), the TPKS Law (Articles 4, 14, 24, 46, 47, 66, 68, 70, and 91), Government Regulation Number 30 of 2025 (Articles 78 to 84), the PDP Law (Articles 2, 8, 15, 19, 20, and 43 to 45), and Law Number 31 of 2014 on the Protection of Witnesses and Victims. Article 407 of Law Number 1 of 2023 on the Penal Code is considered only because one court cited it. Statutory texts were read in the official copies published by the Legal Documentation and Information Network of the Audit Board (JDIH BPK).

The case approach uses purposive selection. A decision qualified if it (a) convicted the defendant at first instance under Article 27 paragraph (1) in conjunction with Article 45 paragraph (1) of the ITE Law as amended by Law Number 1 of 2024, (b) contained an operative order on at least one physical device and at least one intangible item such as an account or a file, (c) was published in full in the Directory of Decisions of the Supreme Court, and (d) had a chronology that placed it on a different side of 2 January 2026 from the other selected case, one concluded before that date and one still pending on it. Decision Number 47/Pid.Sus/2025/PN Bhn and Decision Number 74/Pid.Sus/2026/PN Bdg meet these criteria. Because the case-tracking record of the Bintuhan District Court showed that the prosecutor had appealed, the appellate Decision Number 251/PID.SUS/2025/PT BGL was added. The two cases are illustrative and do not represent Indonesian judicial practice as a whole.

Full texts were downloaded from the Directory of Decisions and case-tracking data were read in the Case Tracking Information System (SIPP) of the Bintuhan District Court, all accessed on 5 October 2026. The SIPP of the Bandung District Court could not be read on that date because the site returned an automated verification page, and the Directory listed no appellate decision related to the Bandung case. Each judgment was read in full and coded on a sheet that records the item, its exact location in the judgment or record, and the coding result. Three codes were used. Specified means that the considerations or the operative part state the item expressly. Not specified means that the item belongs to the content a judgment would ordinarily carry, but a full reading and a keyword search (eksekusi, jaksa, Kementerian, penghapusan, dihapus, pemutusan akses, Penyelenggara Sistem Elektronik, berita acara pemusnahan, platform, forensik) found no statement of it. Not available means that the information lies outside the judgment and could not be obtained from the official records accessed. Table 3 reports the derivation of each entry.

The procedural regime was determined case by case. For each case, the dates of the alleged act, investigation, prosecution, registration, first examination, decision, appeal, and finality were recorded with their sources, the stage reached on 2 January 2026 was identified, and each limb of Article 361 (letters a to d) was applied to that stage. The year of the judgment was not used as a criterion. The provisions actually cited by each court were recorded separately so that the classification under Article 361 could be compared with the court's own practice.

The conceptual approach draws on the theories of legal certainty, justice, and legal protection, and on the notion of chain of custody for digital evidence (Karagiannis & Vergidis, 2021). The materials were analysed qualitatively through grammatical and systematic interpretation. Grammatical interpretation fixed the meaning of terms such as *dirampas untuk dimusnahkan*, *dihapus*, *pemutusan akses*, and *penghapusan konten*, and systematic interpretation placed each provision within the relationship between criminal procedure, the TPKS Law, the ITE Law, and the PDP Law.

RESULTS AND DISCUSSION

Procedural Status and Selection of the Two Decisions

The Bintuhan case concerned a defendant who used a public X (formerly Twitter) account, opened in February 2024, to repost 14 videos showing sexual intercourse between foreign nationals. The first repost was dated 18 May 2024 and the last 9 May 2025, the Cyber Sub-directorate of the Bengkulu Regional Police detected the account during a cyber patrol on 30 April 2025, and the defendant was arrested on 19 May 2025. The prosecutor's indictment is dated 25 July 2025, the case was registered the same day, and the first hearing took place on 31 July 2025. The district court convicted on 3 September 2025. The prosecutor appealed on 9 September 2025, and the Bengkulu High Court decided the appeal on 15 October 2025 in Decision Number 251/PID.SUS/2025/PT BGL.

The Bandung case arose from a relationship that began on social media in mid-2025. During a sexual video call, the defendant recorded the screen although the victim had refused, and after the relationship ended he threatened to circulate the material and then sent photographs and videos to members of a campus WhatsApp group of about 180 members, to other individuals, and to the victim's parent. The judgment records an investigation warrant and the defendant's arrest on 28 November 2025, detention by the prosecutor from 26 January 2026, registration on 5 February 2026, and pronouncement on 22 April 2026. Table 1 sets out both chronologies with their sources.

Table 1. Procedural Timeline and Application of Article 361 of Law Number 20 of 2025

Item	Bintuhan case (first instance and appeal)	Bandung case
Case number and court	47/Pid.Sus/2025/PN Bhn (Bintuhan District Court). Appeal 251/PID.SUS/2025/PT BGL (Bengkulu High Court)	74/Pid.Sus/2026/PN Bdg (Bandung District Court)
Date of alleged act	Reposting from 18 May 2024 to 9 May 2025 (indictment, judgment p. 3, findings, p. 13)	Indictment: 4 October 2025 "or at least in 2025" (p. 4). Findings place the dissemination after the relationship ended around November 2025 (pp. 28 to 29)
Start of investigation	Cyber patrol detection 30 April 2025, arrest 19 May 2025, detention by the investigator from 20 May 2025 (pp. 1, 3 to 4). Date of the investigation warrant: not specified	Investigation warrant Sp.Sidik/139/XI/RES.2.5/2025/Ditressiber dated 28 November 2025, arrest and detention 28 November 2025 (pp. 1, 15)
Start of prosecution	Not specified as such. Detention by the prosecutor from 8 July 2025, indictment No. PDM-08/L.7.16/Eku.2/07/2025 dated 25 July 2025 (pp. 1, 3)	Not specified as such. Detention by the prosecutor from 26 January 2026 (p. 1). Date of the indictment: not specified
Registration	25 July 2025 (judgment p. 1, SIPP)	5 February 2026 (judgment p. 1, Directory metadata)
First examination	31 July 2025, reading of the indictment (SIPP, hearing schedule)	Not available. Hearing date fixed by order of 5 February 2026 without the date being stated (pp. 1 to 2). SIPP not accessible
Decision	Deliberation 29 August 2025, pronounced 3 September 2025 (p. 20). Appeal decided 15 October 2025	Deliberation 21 April 2026, pronounced 22 April 2026 (p. 34)

Item	Bintuhan case (first instance and appeal)	Bandung case
Appeal or other remedy	Prosecutor's appeal filed 9 September 2025 (SIPP, appeal tab). No cassation recorded in SIPP	Not available. No related decision listed in the Directory. SIPP not accessible
Finality	Appellate decision notified to the defendant on 20 October 2025 and to the prosecutor on 21 October 2025 (SIPP). Finality inferred from the absence of a recorded cassation, not from a certificate	Not available
Article 361 assessment	Investigation, prosecution, trial, and appeal were all completed before 2 January 2026. No limb of Article 361 is triggered for these stages	On 2 January 2026 the investigation was pending, so letter a requires it to be completed under the 1981 KUHAP. Letter b does not apply because investigation had begun. Letters c and d do not apply literally because the case reached the court on 5 February 2026
Procedural code cited in the record	Law Number 8 of 1981 in the closing citation of legal bases (p. 19). The appellate court cited Article 222 paragraph (1) KUHAP	Indictment: Law Number 20 of 2025, Article 165(2), for venue (p. 4). Judgment: Articles 108(2) and 250(1)(k) of Law Number 20 of 2025 (pp. 31 to 32), alongside "Pasal 193 ayat (1) KUHAP" (p. 30) and reliance on <i>petunjuk</i> (pp. 25, 31)
Classification in this study	1981 KUHAP throughout	Mixed: investigation under the 1981 KUHAP, adjudication and evidence disposition under the 2025 KUHAP

Source: Decision Number 47/Pid.Sus/2025/PN Bhn, Decision Number 251/PID.SUS/2025/PT BGL, Decision Number 74/Pid.Sus/2026/PN Bdg (Directory of Decisions of the Supreme Court), and SIPP of the Bintuhan District Court, accessed 5 October 2026, processed by the authors. Page numbers follow the page labels printed in the published judgments.

Two corrections follow from the chronology. The Bintuhan case cannot be described as decided under the old code merely because judgment was given in 2025. It belongs to the 1981 regime because every stage, including the appeal, ended before 2 January 2026, and Article 361 never comes into play. The Bandung case is not simply a case under the new code either. Its investigation was running on 2 January 2026, and letter a of Article 361 requires that investigation to be completed under the 1981 KUHAP. The delegation to court on 5 February 2026 falls outside letters c and d, which speak of cases already delegated when the new code entered into force. The indictment already invoked Article 165 paragraph (2) of the 2025 KUHAP to establish venue, and the court adjudicated under the 2025 KUHAP, a reading supported by the repeal of the 1981 KUHAP in Article 362 and by the immediate effect normally given to procedural rules, although the judgment still cites Article 193 paragraph (1) of the old code and treats *petunjuk*, a means of proof that Article 235 of the 2025 KUHAP no longer lists, as evidence. The accurate label for that case is mixed.

One further point matters for this study. Article 361 regulates investigation, prosecution, and examination, but not the execution of judgments. Where a judgment governed by the 1981 KUHAP is executed after 2 January 2026, the transitional rule gives no express answer on which code governs the destruction or auction of evidence. Neither the judgment nor the SIPP record of the Bintuhan case states when its evidence order was carried out, so the study cannot say whether that question arose there.

Statutory Framework for Removal, Access Termination, Evidence Disposition, and Victim Protection

The relevant provisions fall into four groups that answer to different authorities. The first group is criminal procedure. The trial court decides the disposition of each seized item, the prosecutor executes it after the judgment becomes final, and an official report (*berita acara*)

records the execution (Article 156 paragraph (1) letters l and n of the 2025 KUHAP). Objects confiscated for the state are auctioned within three months. Two provisions of the 2025 KUHAP treat destruction with caution: Article 132 paragraph (2) requires that part of any prohibited seized object be set aside for proof before the rest is destroyed, and Article 323 paragraph (1) provides that an application for case review, which otherwise does not suspend execution, does suspend the destruction of evidence. During proceedings, Article 140 allows investigators, prosecutors, and judges to block online platform accounts and electronic information with the approval of the chief of the district court, for one year with two possible six-month extensions.

The second group is the TPKS regime. The authority in Article 46 belongs to the central government, and Article 47 adds a judicial route that a prosecutor may open in the public interest by asking the chief of the district court to order the communications ministry to delete content. Government Regulation Number 30 of 2025 operationalizes the government route. The victim, the victim's family, or a companion may request removal from the police, the prosecution service, or the minister for women's empowerment and child protection (Article 78 paragraph (1)), and the Witness and Victim Protection Agency (LPSK), the regional technical unit for women and children (UPTD PPA), and social services units may file on their behalf (Article 78 paragraph (2)). The request must identify the specific content by screenshot and uniform resource locator (Article 79 paragraph (2)). The Attorney General's Office issues a removal decision within three times twenty-four hours (Article 80), the communications ministry executes within twenty-four hours (Article 82 paragraph (2)), and the victim is informed through the requesting institution (Article 83). For pornographic content the ministry may act before the Attorney General's decision (Article 81). Article 84 requires removal to take account of law enforcement and evidentiary interests. The implementing regulation required by Article 46 paragraph (2) has therefore been in force since 18 June 2025, about a year after the two-year deadline set by Article 91 paragraph (1) of the TPKS Law had passed.

The third group is the general regime of the ITE Law. Article 40 paragraphs (2a) to (2c) authorize access termination and self-moderation orders, and Government Regulation Number 71 of 2019 lets the public, ministries, law enforcement agencies, and courts trigger access termination (Article 97 paragraphs (1) to (4)). Article 26 paragraph (3) of the ITE Law, inserted by Law Number 19 of 2016, and Articles 15 to 17 of Government Regulation Number 71 of 2019 provide for the erasure of irrelevant personal data and for its delisting from search engines at the request of the person concerned, with delisting requiring a district court determination (Article 17). This regime applies whatever the victim profile of the offence, which makes it the only removal route for unlawful content that does not involve an identified victim of sexual violence.

The fourth group is data protection and victim protection. The PDP Law obliges controllers, including platform operators, to delete personal data processed unlawfully or on the subject's request (Article 43), to destroy data that are no longer connected with a legal process (Article 44), and to notify the subject (Article 45). The Law does not apply to processing by individuals in a purely personal or household context (Article 2 paragraph (2)), and that exclusion matters when copies sit on private telephones. Law Number 31 of 2014 provides the general framework for LPSK protection, which Government Regulation Number 30 of 2025 now links to removal requests.

Read together, the four groups do not refer to one another at the point where a criminal judgment disposes of evidence. The judgment speaks to the seized items listed in the case file. The TPKS route begins with a victim's request or a prosecutor's initiative, runs through the Attorney General's Office and the communications ministry, and does not depend on the trial court's disposition order. The ITE route is administrative. Article 84 of Government Regulation Number 30 of 2025 is the only provision found that expressly asks a removal authority to

consider evidentiary needs, and it does so in one general sentence. The resulting picture is regulatory fragmentation, not an absence of norms.

Comparative Analysis of the Two Decisions

Both judgments establish the elements of the ITE offence through witness testimony, expert evidence, and the defendant's statement, and both deal with electronic material without dispute over its admissibility. In the Bintuhan case an expert from the digital investigation directorate of the communications ministry explained that the account's contents had been examined through digital forensics of the device (pp. 8 to 11). In the Bandung case the prosecutor submitted an official report on the examination of digital evidence and its attachments (p. 22). The disposition of the evidence is where the analysis of this study begins. Table 2 compares the two cases, and Table 3 shows how each entry was coded.

Table 2. Disposition of Physical and Digital Evidence in the Two Cases

Aspect	Bintuhan case	Bandung case
Procedural regime (Table 1)	1981 KUHAP throughout	Mixed (investigation 1981 KUHAP, adjudication 2025 KUHAP)
Charge	Single charge: Article 45(1) jo. Article 27(1) ITE Law	Primary: Article 45(10) jo. Article 27B(1) ITE Law, as written in the judgment (the conduct described corresponds to Article 27B(2)). Subsidiary: Article 45(1) jo. Article 27(1) ITE Law, "menjadi Pasal 407 ayat (1)" Law Number 1 of 2023
Content and victim	14 reposted sexual videos of foreign nationals on a public account with 25 followers. No depicted person identified, no victim testimony	Non-consensual screen recording of a sexual video call, sent to a campus WhatsApp group of about 180 members, to other persons, and to the victim's parent. Identified victim
Sentence	First instance: 8 months, conditional with 1 year 6 months probation, release ordered. Appeal: 8 months and a fine of Rp5,000,000 (1 month in default), detention ordered	1 year 10 months, detention continued
Physical items	1 mobile telephone	1 mobile telephone, 2 SIM cards, 1 micro SD card (16 GB)
Intangible items	1 X (Twitter) account, 1 Gmail account	3 WhatsApp accounts, 1 Gmail account with its password, 3 videos, 12 photographs (15 files)
Disposition ordered	First instance: accounts "dirampas untuk dimusnahkan dengan cara dihapus", telephone "dirampas untuk negara". Appeal: accounts "dimusnahkan dengan cara dihapus", telephone "dimusnahkan"	All items "dirampas untuk dimusnahkan". The considerations add "tetap terlampir dalam berkas perkara"
Executing authority	Not specified	Not specified
Method of destruction or erasure	Not specified beyond "dengan cara dihapus"	Not specified
Copies outside the seized items	Not specified	Not specified, although the judgment records distribution to identified and unidentified recipients
Preservation of an evidentiary copy	Not specified	Partly specified ("tetap terlampir dalam berkas perkara"), without form or duration
Link to TPKS Articles 46 to 47 or ITE Article 40	Not specified	Not specified
Verification, report, or victim notice	Not specified	Not specified

Source: Decision Number 47/Pid.Sus/2025/PN Bhn, Decision Number 251/PID.SUS/2025/PT BGL, and Decision Number 74/Pid.Sus/2026/PN Bdg, coded by the authors according to Table 3.

The considerations behind the dispositions are short, and they are quoted here in full. On the accounts, the Bintuhan court held that *"barang bukti berupa 1 (satu) akun Twitter atas nama, 1 (satu) akun Gmail yang telah dipergunakan untuk melakukan kejahatan dan dikhawatirkan akan dipergunakan untuk mengulangi kejahatan maka terhadap barang bukti tersebut haruslah ditetapkan barang bukti tersebut dirampas untuk dimusnahkan dengan cara dihapus agar tidak dapat dipergunakan lagi"* (p. 18). The account name is anonymized in the published text. On the telephone it held that the device *"telah dipergunakan untuk melakukan kejahatan serta mempunyai nilai ekonomis maka perlu ditetapkan agar barang bukti tersebut dirampas untuk negara"* (pp. 18 to 19). Item 5 of the operative part repeats both orders.

The appeal changed the telephone order for a reason that goes to the core of this study. The prosecutor argued that a telephone confiscated for the state would be auctioned and that, once switched on again, the indecent videos on it could be seen by anyone. The Bengkulu High Court agreed: *"Majelis Hakim Tingkat Banding sependapat dengan Penuntut Umum bahwa barang bukti yang berupa 1 (satu) unit handphone OPPO AX7 ... harus dimusnahkan"* (p. 10), and the operative part orders the telephone *"dimusnahkan"*. The first-instance court had treated the device as an asset with resale value. The appellate court treated it as a container of unlawful content. The correction depended on the prosecutor's decision to appeal, an appeal that also challenged the leniency of the sentence.

In the Bandung case the court reasoned that the listed items *"merupakan alat yang digunakan Terdakwa untuk melakukan tindak pidana Informasi dan Transaksi Elektronik sebagaimana tersebut di atas, maka Majelis Hakim berpendapat bahwa barang bukti tersebut Tetap terlampir dalam berkas perkara dan dirampas untuk dimusnahkan"* (p. 32). The operative part lists the 15 files and ends with *"Dirampas Untuk Dimusnahkan"* (pp. 33 to 34). The phrase *tetap terlampir dalam berkas perkara* points toward keeping an evidentiary copy with the case file, but the operative part does not repeat it, and nothing says whether the copy is the original file, an extraction report, or a forensic image, or for how long it stays. The same judgment records that the defendant could not say to whom he had sent the content because his telephone had been reset (p. 22). The court therefore knew that copies existed beyond the seized items, yet its order reached only those items.

Table 3. Coding Matrix for Table 1 and Table 2

Table entry	Case	Source and exact location	Coding result and basis
Procedural regime	Both	Dated entries in Table 1. Article 361 letters a to d	Derived from the stage reached on 2 January 2026, not from the year of judgment
Charge	Bandung	Indictment (pp. 4 to 7), considerations and closing citation (pp. 31 to 33)	Specified. Mismatch between Article 45(10) and Article 27B(1) recorded as written
Sentence	Bintuhan	Operative part (p. 20). Appellate operative part (Directory metadata, SIPP appeal tab, appellate p. 11)	Specified
Disposition	Bintuhan	Considerations (pp. 18 to 19), operative part item 5 (p. 20), appellate considerations (p. 10)	Specified, quoted verbatim
Disposition	Bandung	Considerations (p. 32), operative part item 5 (pp. 33 to 34)	Specified, quoted verbatim. Divergence between considerations and operative part noted
Executing authority	Both	Full text and keyword search	Not specified. In the Bintuhan text "Kementerian" appears only in the expert's job title (p. 8)
Method of destruction or erasure	Both	Operative parts. Keyword search for "dihapus" and "penghapusan"	Not specified beyond "dengan cara dihapus" (Bintuhan, pp. 18, 20)

Table entry	Case	Source and exact location	Coding result and basis
Copies outside the seized items	Bandung	Findings (pp. 22, 29 to 30)	Not specified in the disposition, although distribution is found as fact
Preservation of an evidentiary copy	Both	Bandung considerations (p. 32). Bintuhan full text	Bandung partly specified, Bintuhan not specified
Link to removal channels	Both	Full text. Search for "pemutusan akses", "Penyelenggara Sistem Elektronik", "12 Tahun 2022"	Not specified. No result in either judgment
Verification, report, or victim notice	Both	Full text. Search for "berita acara pemusnahan" and "salinan"	Not specified. The word "korban" appears 65 times in the Bandung text, never in connection with notice
First examination	Bandung	Judgment pp. 1 to 2. SIPP of the Bandung District Court	Not available. Date not stated, SIPP not accessible on 5 October 2026
Appeal and finality	Bandung	Directory entry ("Putusan terkait: tidak ada"). SIPP	Not available
Finality	Bintuhan	SIPP case history, stages 24 to 26	Inferred from notification of the appellate decision and absence of a recorded cassation

Source: authors' coding sheet. Page numbers refer to the page labels printed in each published judgment.

The comparison supports a limited conclusion. The disposition formula in both cases was generic and tied to seized items, and it stayed generic in a case adjudicated under the 2025 KUHAP. Two cases cannot show that the change of code had no effect, and this study does not claim that it did. What they show is that Article 250 paragraph (1) letter i of the 2025 KUHAP, like its predecessor, leaves the content of the disposition to the court, and that nothing in the procedural framework prompted either court to address copies beyond the case file or the removal routes of the TPKS and ITE Laws. The cases also differ in a respect that bears directly on the available removal routes. The Bandung conduct fits the description of electronic-based sexual violence in Article 14 paragraph (1) letter a and Article 4 paragraph (2) letter d of the TPKS Law, so Articles 46 and 47 and Government Regulation Number 30 of 2025 were available in principle, although the case was charged under the ITE Law. The Bintuhan judgment identifies no depicted person and contains no finding on consent, so the ITE regime, not the TPKS regime, is the relevant removal route there.

Preservation and Disposition of Electronic Evidence

The phrase permanent deletion conceals at least three legally distinct objects. The first is the evidentiary record: the forensic image, the extraction report, and the hash values that let a court check that what was examined at trial is what the investigator seized. The second is the seized device or account under state control. The third is the unlawful content as it exists elsewhere, on platform servers, on recipients' telephones, in private backups, in caches, and on services hosted abroad. Each object needs a different legal treatment, and treating them as one leads to orders that either go too far or reach too little.

The evidentiary record has to survive the verdict. Appeal, cassation, and case review all depend on it, as does accountability for the investigation itself. The Bintuhan case shows why: the appellate court revisited the disposition and the sentence six weeks after the first judgment. The 2025 KUHAP already recognizes the irreversibility of destruction, since Article 323 paragraph (1) lets an application for case review suspend it and Article 132 paragraph (2) requires a portion of prohibited items to be set aside for proof. Authentication under Article 235 paragraph (3) presupposes a chain of custody that premature destruction would break (Karagiannis & Vergidis, 2021). The PDP Law points the same way, because Article 44 paragraph (1) letter c ties the destruction duty to data that no longer relate to a legal process and Article 15 paragraph (1) letter b exempts law enforcement processing from certain subject

rights. None of these provisions sets a retention period or access conditions for forensic copies of intimate content. The Bandung formula, which keeps the evidence attached to the case file while ordering it destroyed, shows the uncertainty in practice and leaves open who may see the file and for how long.

The seized device raises a different problem. Under both codes, an object confiscated for the state is auctioned and its value goes to the treasury. For a telephone holding sexual content, that route can put the content back into circulation, which is exactly the risk the Bengkulu High Court identified. Destruction of the device, once the evidentiary record has been secured, protects the victim better than auction, yet no rule excludes such devices from auction or prescribes how a device must be sanitized or physically destroyed. The *berita acara* required by Article 156 of the 2025 KUHAP records that execution took place, but it is not a forensic attestation that data cannot be recovered.

Accounts are harder still. An order that an X account or a Gmail account be *dirampas untuk dimusnahkan dengan cara dihapus* assumes that the state controls the account. Legally it may, but technically the account sits with a foreign provider, and the prosecutor can delete it only with credentials obtained during the investigation or with the provider's cooperation. Neither judgment says which. A Gmail account also holds correspondence and data of third parties, whose deletion engages Articles 43 to 45 of the PDP Law on the provider's side. These are questions of execution that the disposition order leaves to the prosecutor without guidance.

Platform Takedown, Access Termination, and De-indexing

Takedown, access termination, and de-indexing are often treated as synonyms for deletion, but they act on different things. Takedown removes a specific item from a platform, and only the operator can carry it out. Access termination blocks access from Indonesia or closes an account, and the elucidation of Article 40 paragraph (2b) of the ITE Law includes content deletion within it. De-indexing removes a search result without touching the hosted item, and Government Regulation Number 71 of 2019 conditions it on a court determination (Article 17 paragraph (1)). A victim may need all three, in a sequence that depends on where the content sits.

The two cases illustrate the difference. The Bintuhan reposts were public posts with stable addresses, which the URL-based procedure of Government Regulation Number 30 of 2025 or Article 40 of the ITE Law can reach, although the account itself was the object of the court's erasure order. The Bandung content moved through private WhatsApp groups and individual chats. Copies held there have no public address to block or delist, and the regulation's requirement of a specific locator (Article 79 paragraph (2) letter c) cannot be met for them. Comparative studies report the same limit: takedown works against hosted and indexed copies, while copies already downloaded by recipients remain beyond the reach of platform regulation (O'Connell, 2020; Hörnle, 2026; Sahak et al., 2026).

No Indonesian provision compels the erasure of copies held privately by recipients, apart from seizure in separate proceedings, and the PDP Law does not reach personal or household processing. Further distribution remains punishable under Article 27 paragraph (1) of the ITE Law and Article 14 of the TPKS Law, which deters onward circulation without retrieving copies already made. The law therefore cannot promise universal erasure from recipient devices, private backups, caches, or foreign-hosted services, and an honest framework has to say so to victims. What the law can do is reduce availability through takedown, access termination, and de-indexing, record what was done, and tell the victim what remains outside its reach.

Integration and Implementation Gaps

The findings point to several distinct gaps, and naming them separately matters because each calls for a different response. The first concerns triggers. A disposition order does not set the TPKS or ITE removal routes in motion: Government Regulation Number 30 of 2025 starts with a request from the victim or an institution acting for the victim, and Article 47 of the TPKS Law depends on a prosecutor deciding to apply. If no one makes the request, a final judgment can be fully executed against the seized items while the content stays online.

Authority after the verdict is divided. The prosecutor executes the judgment, the Attorney General's Office decides removal requests under the regulation, the communications ministry executes them, and the ministry for women's empowerment and child protection runs the information system. Each acts within its own statute, and none is assigned responsibility for confirming that the purpose of the disposition order, namely ending the circulation of the content, has been met. Verification is the next gap. The *berita acara* of execution records an act, Article 82 paragraph (4) of the regulation requires the ministry to report execution to the Attorney General's Office, and Article 83 requires notice to the victim, but no provision sets a technical standard for confirming that content has been removed or a device sanitized, or for checking re-uploads. Preservation, discussed above, lacks a retention rule. The transitional provision leaves the execution stage unaddressed.

Whether these gaps produced harm in the two cases cannot be determined from the judgments, which say nothing about requests to the communications ministry or the Attorney General's Office, and this study has no data on what the prosecutors did after finality. The implementation gap is therefore identified as a structural risk, not measured.

The theoretical lenses explain why the gaps matter. Legal certainty requires that the consequences of a judgment be predictable in their execution as well as their existence (Marzuki, 2021; Alex & Sulistiani, 2026), and an order to destroy "evidence" that does not say which object, by whom, and with what proof of completion fails that test. Corrective justice and Rawls's account of fairness (Rawls, 1999) both measure a remedy by whether it addresses the harm, and here the harm is continued exposure, which a sentence of imprisonment does not touch. Hadjon (1987) distinguishes preventive from repressive legal protection. Indonesian law now offers both in this field, the TPKS and ITE removal routes on one side and criminal sanctions on the other, so the weakness lies in the joint between them rather than in either side (Flora et al., 2023).

Proposed Operational Framework

Table 4 sets out an operational framework that replaces the single notion of deletion with distinct stages, each tied to its object. For every stage it states the legal basis in force, the trigger and competent authority, retention and verification, and victim notice, third-party safeguards, and remedies for non-compliance. Where positive law says nothing, the cell says so and labels the content as a proposal.

Table 4. Operational Framework for Electronic Evidence and Unlawful Sexual Content after a Criminal Verdict

Object and stage	Legal basis in force	Trigger and competent authority	Retention and verification	Victim notice, third-party safeguards, remedy
Preservation of the evidentiary record (forensic image, extraction report, hash values)	2025 KUHAP Arts. 130, 132(2), 156, 235(3), 323(1). PDP Law Arts. 15(1)(b), 44(1)(c). GR 30/2025 Art. 84	Seizure and examination by the investigator, custody passing to the prosecutor and the case file	No retention period in force. Proposed: hash-verified sealed copy kept until the judgment is final and review is no longer pending, then destroyed by court order, with an access log	No rule in force. Proposed: restricted access to intimate material in the case file, notice to the victim of retention and later destruction, objection to the supervising judge (2025 KUHAP Art. 353)

Object and stage	Legal basis in force	Trigger and competent authority	Retention and verification	Victim notice, third-party safeguards, remedy
Secure destruction of the seized device and storage media	1981 KUHAP Arts. 46(2), 197(1)(i), 270, 273(3). 2025 KUHAP Arts. 135, 250(1)(i), 342(1), 345(3)	Final judgment ordering destruction. The public prosecutor	Berita acara of execution (2025 KUHAP Art. 156(1)(l)). No technical standard. Proposed: certified wiping or physical destruction attested by a digital forensic examiner, and exclusion of such devices from auction	2025 KUHAP Art. 342(2) gives the victim a copy of the judgment only. Proposed: notice of destruction to the victim and a complaint route to the supervising judge
Erasure or closure of offender-controlled accounts	Disposition order in the judgment. 2025 KUHAP Arts. 1(37) and 140 (blocking during proceedings)	Final judgment. The public prosecutor. No rule on obtaining provider cooperation	Proposed: erasure only after preservation, with provider confirmation or documented account status attached to the berita acara	PDP Law Arts. 43 to 45 bind the provider for third-party data. Proposed: order limited to the account, not to unrelated correspondence
Platform takedown of hosted content	TPKS Law Arts. 46(1), 47, 68(g), 70(2)(l). GR 30/2025 Arts. 78 to 84. ITE Law Art. 40(2b)	Request by the victim, family, companion, LPSK, or UPTD PPA (GR 30/2025 Art. 78). Decision of the Attorney General's Office within 3 x 24 hours. Execution by the communications ministry within 24 hours. Alternatively a prosecutor's request to the district court chief (TPKS Law Art. 47)	Ministry reports execution to the Attorney General's Office (GR 30/2025 Art. 82(4)). No verification or re-upload standard. Proposed: periodic re-check of listed locators	Notice to the victim within 24 hours through the requesting institution (Art. 83). Remedy for platform non-compliance not specified in GR 30/2025, so the ITE sectoral regime applies
Access termination (blocking, account closure)	ITE Law Art. 40(2a) to (2c). GR 71/2019 Arts. 95 to 97. TPKS Law Art. 46(1)	The communications ministry, on its own initiative or at the request of the public, law enforcement, or a court (GR 71/2019 Art. 97)	No verification standard in force. Proposed: locator-level blocking recorded in a register linked to the case number	Risk of over-blocking lawful content. Proposed: blocking confined to identified locators, with notice to the victim
De-indexing from search engines	ITE Law Art. 26(3) to (5). GR 71/2019 Arts. 15 to 17	Application by the data subject to the local district court, executed by the search engine operator	Operator must provide an erasure mechanism (GR 71/2019 Art. 18). No public verification standard	The victim is the applicant. Proposed: prosecutors or LPSK inform victims of the route after conviction
Residual copies on recipient devices, private backups, caches, and foreign-hosted services	No provision compels erasure. ITE Law Art. 27(1) and TPKS Law Art. 14 penalize further distribution. PDP Law Art. 2(2) excludes household processing	No general authority. Seizure possible only in separate proceedings	Universal erasure cannot be guaranteed or verified	Proposed: warning to known recipients that onward distribution is an offence, record of voluntary deletion, and candid information to the victim about residual risk

Source: compiled by the authors from the legislation cited. Entries marked "Proposed" are reform proposals and are not positive law. GR means Government Regulation.

Sequence matters as much as allocation. Preservation has to come first, because takedown or destruction carried out before a verified copy exists can defeat appeal and review. Takedown and access termination need not wait for the verdict: the victim's rights to handling arise when the offence occurs (Article 66 of the TPKS Law), Government Regulation Number 30 of 2025 does not make a removal request depend on a verdict, and Article 84 asks the authorities only to respect evidentiary interests, which a prior forensic copy satisfies. Destruction of the seized device and erasure of offender accounts belong after finality. Verification and notice close each stage. A court can already contribute within existing law: Article 250 paragraph (1) letter i of the 2025 KUHAP does not limit how precisely the disposition of evidence may be stated, so an operative part could distinguish the evidentiary copy, the device, the accounts, and known locators, and could record that the victim may use the removal route of Government Regulation Number 30 of 2025. Any duty on the court or the

prosecutor to activate that route, as opposed to informing the victim of it, would require legislative or regulatory reform.

CONCLUSION AND RECOMMENDATIONS

Conclusion

The two decisions disposed of electronic evidence through a generic formula addressed to seized items. The Bintuhan case belongs entirely to the 1981 KUHAP, because every stage ended before 2 January 2026, and its appeal shows that disposition can change after the first judgment, as the telephone moved from confiscation for the state to destruction. The Bandung case is mixed: its investigation fell under letter a of Article 361 and its adjudication under the 2025 KUHAP. In neither case did the order name the executing authority, the method, the treatment of copies outside the case file, or a means of verification, and in neither case did it refer to the removal channels of the TPKS Law or the ITE Law. Two cases cannot establish a causal relationship between the procedural code and the content of disposition orders.

Indonesia does not suffer from a normative vacuum on content removal. The TPKS Law, Government Regulation Number 30 of 2025, Article 40 of the ITE Law, Government Regulation Number 71 of 2019, and the PDP Law together provide removal, access termination, de-indexing, and data deletion. The findings support a narrower diagnosis: regulatory fragmentation and a lack of integration between these channels and the disposition and execution of evidence, an unclear allocation of responsibility after the verdict, and the absence of verification and retention standards. Whether these gaps translate into failures of implementation cannot be measured from the judgments alone. The proposed framework separates preservation, secure destruction, platform takedown, access termination, and de-indexing, and it accepts that copies already held by private recipients lie beyond complete legal control.

Limitations

The study rests on two purposively selected decisions and on official records accessed on 5 October 2026. The first examination date, appeal status, and finality of the Bandung case could not be verified because the case-tracking system of the Bandung District Court was not accessible, and the finality of the Bintuhan case is inferred from the record rather than from a certificate. No field data were collected on execution reports, removal requests, or ministry actions, so the findings identify normative and structural gaps without measuring how often they occur.

Recommendations

Several measures are possible within existing law. Courts can use Article 250 paragraph (1) letter i of the 2025 KUHAP to specify the disposition of each object separately, keeping a sealed evidentiary copy while ordering the destruction of devices and the erasure of offender-controlled accounts, and listing known locators of the content. Prosecutors can use Article 47 of the TPKS Law, and victims or institutions acting for them can use Articles 78 to 84 of Government Regulation Number 30 of 2025, where the conduct qualifies as sexual violence. For content outside that regime, Article 40 of the ITE Law and Article 97 of Government Regulation Number 71 of 2019 already allow law enforcement agencies to request, and courts to order, access termination. Victims should also be told of the de-indexing route under Article 17 of Government Regulation Number 71 of 2019.

Other measures require reform and are presented as proposals. A joint guideline of the Supreme Court and the Attorney General's Office could set retention periods and access conditions for forensic copies of intimate content and require their destruction once review is no longer possible. A rule excluding devices that contain sexual content from auction under

Article 345 paragraph (3) of the 2025 KUHAP would codify the reasoning of the Bengkulu High Court. The *berita acara* of execution should carry a forensic attestation of sanitization or erasure, and the victim should receive notice of each completed stage, extending the notification practice of Article 83 of Government Regulation Number 30 of 2025 to post-verdict destruction. Platform orders should be confined to identified locators so that the rights of third parties are respected, with the PDP Law governing the provider's handling of unrelated data. Article 361 of the 2025 KUHAP, or its implementing guidance, should state which code governs the execution of evidence orders in cases decided under the 1981 KUHAP.

None of these measures can guarantee erasure from recipient devices, private backups, caches, or foreign servers. The realistic aim is to reduce availability, to document every step so that it can be verified, and to tell victims clearly what has been removed and what remains outside legal reach. Further research could examine execution reports and removal requests in a larger set of cases to measure how the channels described here operate in practice.

Author Contributions

The first author was responsible for the conceptualization of the research, the collection of legal materials, data analysis, and the preparation of the manuscript draft. The second and third authors, acting as academic supervisors, contributed to the development of the theoretical framework, provided critical review of the analysis, and revised the manuscript. All authors have read and approved the final version of the manuscript submitted for publication.

Acknowledgment

The authors would like to express their gratitude to the Faculty of Law, Universitas Brawijaya, for the academic support provided throughout the completion of this research.

REFERENCES

- Alex, L. E., & Sulistiani, L. (2026). Principles of justice and legal certainty in criminal law enforcement in Indonesia. *Awang Long Law Review*, 8(3), 859–867. <https://doi.org/10.56301/awl.v8i3.2162>
- Flora, H. S., Sitanggang, T., Simarmata, B., & Karina, I. (2023). Keadilan restoratif dalam melindungi hak korban tindak pidana cyber: Manifestasi dan implementasi. *Jurnal Ius Constituendum*, 8(2), 169–184. <https://doi.org/10.26623/jic.v8i2.6365>
- Hadjon, P. M. (1987). *Perlindungan hukum bagi rakyat di Indonesia*. Bina Ilmu.
- Hörnle, J. (2026). Fighting the beast of image-based sexual abuse. Part 1: The criminal law and platform regulation. *International Journal of Law and Information Technology*, 34, Article eaag006. <https://doi.org/10.1093/ijlit/eaag006>
- Huber, A. R. (2025). Image-based sexual abuse: Legislative and policing responses. *Criminology & Criminal Justice*, 25(3), 736–752. <https://doi.org/10.1177/17488958221146141>
- Karagiannis, C., & Vergidis, K. (2021). Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal. *Information*, 12(5), Article 181. <https://doi.org/10.3390/info12050181>
- Marzuki, P. M. (2021). *Pengantar ilmu hukum* (Rev. ed.). Kencana Prenada Media Group.
- Nesi, H., & Umar, R. (2025). Analisis unsur "tanpa hak" dalam delik kesusilaan UU ITE dalam kasus revenge porn. *Politika Progresif: Jurnal Hukum, Politik dan Humaniora*, 2(3), 51–58. <https://doi.org/10.62383/progres.v2i3.2491>
- O'Connell, A. (2020). Image rights and image wrongs: Image-based sexual abuse and online takedown. *Journal of Intellectual Property Law & Practice*, 15(1), 55–65. <https://doi.org/10.1093/jiplp/jpz150>

- Pengadilan Negeri Bandung. (2026). *Putusan Nomor 74/Pid.Sus/2026/PN Bdg*. Direktori Putusan Mahkamah Agung Republik Indonesia. <https://putusan3.mahkamahagung.go.id/direktori/putusan/zaf13eba274fcd7a9c97303931343236.html>
- Pengadilan Negeri Bintuhan. (2025). *Putusan Nomor 47/Pid.Sus/2025/PN Bhn*. Direktori Putusan Mahkamah Agung Republik Indonesia. <https://putusan3.mahkamahagung.go.id/direktori/putusan/zaf0c4f745ef8604bfe1313032343335.html>
- Pengadilan Negeri Bintuhan. (2026). *Sistem Informasi Penelusuran Perkara: Perkara Nomor 47/Pid.Sus/2025/PN Bhn*. Retrieved October 5, 2026, from <https://sipp.pn-bintuhan.go.id/>
- Pengadilan Tinggi Bengkulu. (2025). *Putusan Nomor 251/PID.SUS/2025/PT BGL*. Direktori Putusan Mahkamah Agung Republik Indonesia. <https://putusan3.mahkamahagung.go.id/direktori/putusan/zaf0a96dc7ea475c8327303932323231.html>
- Purnomo, Y., Sahuri, L., & Siregar, E. (2026). Pengaturan pemusnahan barang bukti digital berupa akun elektronik dalam sistem peradilan pidana di Indonesia. *Al-Sulthaniyah*, 15(1), 121–131. <https://doi.org/10.37567/al-sulthaniyah.v15i1.4536>
- Rawls, J. (1999). *A theory of justice* (Rev. ed.). The Belknap Press of Harvard University Press.
- Republic of Indonesia. (1981). *Law Number 8 of 1981 on Criminal Procedure Law*. <https://peraturan.bpk.go.id/Details/47041/uu-no-8-tahun-1981>
- Republic of Indonesia. (2008). *Law Number 11 of 2008 on Electronic Information and Transactions*. <https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun-2008>
- Republic of Indonesia. (2014). *Law Number 31 of 2014 on the Amendment to Law Number 13 of 2006 on the Protection of Witnesses and Victims*. <https://peraturan.bpk.go.id/Details/38701/uu-no-31-tahun-2014>
- Republic of Indonesia. (2016). *Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions*. <https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016>
- Republic of Indonesia. (2019). *Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions*. <https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019>
- Republic of Indonesia. (2022a). *Law Number 12 of 2022 on Sexual Violence Crimes*. <https://peraturan.bpk.go.id/Details/207944/uu-no-12-tahun-2022>
- Republic of Indonesia. (2022b). *Law Number 27 of 2022 on Personal Data Protection*. <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- Republic of Indonesia. (2023). *Law Number 1 of 2023 on the Penal Code*. <https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023>
- Republic of Indonesia. (2024). *Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions*. <https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024>
- Republic of Indonesia. (2025a). *Government Regulation Number 30 of 2025 on the Prevention of Sexual Violence Crimes and the Handling, Protection, and Recovery of Victims of Sexual Violence Crimes*. <https://peraturan.bpk.go.id/Details/338353/pp-no-30-tahun-2025>
- Republic of Indonesia. (2025b). *Law Number 20 of 2025 on the Code of Criminal Procedure*. <https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025>
- Rigotti, C., McGlynn, C., & Benning, F. (2024). Image-based sexual abuse and EU law: A critical analysis. *German Law Journal*, 25(9), 1472–1493. <https://doi.org/10.1017/glj.2024.49>

- Sahak, S., Rajamanickam, R., & Hassan, M. S. (2026). Liability of internet intermediaries and legal challenges: A comprehensive systematic review. *Quality & Quantity*, 60(1), 2435–2457. <https://doi.org/10.1007/s11135-025-02344-y>
- Samudra, A. H., Basu, S., & Perez, C. S. (2026). Digital challenge, analogue mind-set: Assessing Indonesia's electronic criminal evidence framework. *Journal of Indonesian Legal Studies*, 11(1), 257–298. <https://doi.org/10.15294/jils.v11i1.35378>
- Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review*, 14(2), 133–152. <https://doi.org/10.15742/ilrev.v14n2.4>
- Triyanti, N., Handayani, I. G. A. K. R., & Karjoko, L. (2025). Legal gaps in personal data protection: Reforming Indonesia's population administration law. *Hasanuddin Law Review*, 11(1), 132–147. <https://doi.org/10.20956/halrev.v11i1.6177>
- Vanessa, V., & Firmansyah, H. (2025). Analysis of the validity of electronic evidence in criminal trial proceedings and the implementation of its admissibility (judgment study). *Indonesian Journal of Law and Economics Review*, 20(4), Article 1395. <https://doi.org/10.21070/ijler.v20i4.1395>
- Yuwono, N. K. N., & Ikhsan, W. (2026). Legal protection against revenge porn: A comparative criminal law analysis of Indonesia and Laos. *Rechtsidee*, 14(2), 1–13. <https://doi.org/10.21070/jihr.v14i2.1164>