

BEYOND CRIMINALISATION: DIGITAL VICTIMISATION AND VICTIM PROTECTION AGAINST AI DEEPFAKES IN INDONESIA

Kus Rizkianto¹, Siswanto², Estiana Nabila³

Faculty of Law, Universitas Pancasakti Tegal, Indonesia

Corresponding author: 1 kus_rizkianto@upstegal.ac.id ; 2 siswanto@upstegal.ac.id ;
estiananabil@upstegal.ac.id

ABSTRACT

Artificial intelligence (AI) deepfakes enable the convincing imitation of an individual's image or voice, creating risks that extend beyond the identification and punishment of offenders. This article examines how Indonesian law responds to digital victimisation and whether its remedies address reputational, psychological and social harm. Using normative legal research and a focused interdisciplinary literature review, it analyses the Electronic Information and Transactions Law, Personal Data Protection Law, Sexual Violence Crimes Law, the Criminal Code and criminal procedure reforms, including the 2026 Witness and Victim Protection Law. The analysis identifies three interconnected problems: harm may arise before distribution; protection depends on fitting conduct within fragmented offences; and criminal proceedings alone do not ensure rapid content containment or sustained recovery. It proposes a victim-centred response linking accessible reporting, lawful evidence preservation, timely platform action, risk-sensitive support and restitution where legal conditions are met. Rather than claiming an absence of relevant laws, the article argues that coordination and remedies should reflect the continuous nature of technology-facilitated harm. This framework offers a policy-oriented contribution to debates on digital victimology and access to justice in Indonesia.

Keywords: deepfake; digital victimology; victim protection; artificial intelligence; Indonesia.

INTRODUCTION

Synthetic audiovisual media generated or manipulated through artificial intelligence have transformed the social meaning of visible and audible identity. A person's apparent voice, face or conduct can be reproduced without the underlying event having occurred. The resulting content can be satirical, educational or creative; its legal significance therefore cannot be inferred from the use of AI alone. The problem addressed here is harmful and unauthorised manipulation, especially when a recognisable individual is impersonated, demeaned or exposed to threats. The social consequences may emerge immediately upon discovery of an image, even before it is widely circulated. Digital identity is not merely information about an individual: it is also connected to personal autonomy, reputation, social relationships and the ability to participate safely in public life (Chesney and Citron 2019; Maddocks 2020).

Deepfake-related victimisation is increasingly discussed alongside image-based sexual abuse, technology-facilitated harassment and digital impersonation. These categories should not be collapsed into one offence. Fraudulent voice imitation, a manipulated political statement and non-consensual sexualised imagery can produce different elements of wrongdoing and different needs for remedies. Nevertheless, the cases share a vulnerability: control over identity representations may be lost to creators, uploaders, platforms and subsequent republishers. McGlynn, Rackley and Houghton (2017) show why isolated categories of image abuse can obscure an underlying continuum of coercion and exposure. Henry and Powell's (2018) review similarly suggests that technological mediation changes the form and reach of harm without eliminating its recognisable interpersonal dimensions.

A victim-centred understanding also requires attention to gendered and social inequalities. Research on sexualised deepfake abuse identifies patterns of targeting and social minimisation, while a scoping review emphasises the importance of the vocabulary used to name abuse (Flynn et al. 2025; Lazard et al. 2025). An experimental study of perceptions of image-based sexual abuse demonstrates the relevance of victim blaming to help-seeking and social support (Pacilli et al. 2024). These international findings cannot automatically be treated as prevalence estimates for Indonesia. They do, however, supply analytically relevant mechanisms: stigma, disbelief, fear of repeated exposure and delays in seeking assistance can compound an initial infringement.

For Indonesia, relevant offences and rights are not contained in one statute. The Electronic Information and Transactions Law (ITE Law), as amended by Law No. 1 of 2024, regulates specified unlawful electronic conduct. Law No. 27 of 2022 addresses personal-data processing and misuse. Law No. 12 of 2022 regulates sexual violence offences and the handling, protection and recovery of victims. Law No. 44 of 2008 on Pornography may also be relevant to certain content, subject to applicable elements and the amendments and partial repeals associated with the national Criminal Code. The Criminal Code under Law No. 1 of 2023 came into effect on 2 January 2026 and is affected by Law No. 1 of 2026 on Penal Adjustments. The new Criminal Procedure Code, Law No. 20 of 2025, also entered into effect on 2 January 2026 (Republic of Indonesia 2008, 2022a, 2022b, 2023, 2024, 2025, 2026a).

A further change is especially important to a victimology-focused analysis. Law No. 3 of 2026 on Witness and Victim Protection came into force on 20 May 2026 and repealed Law No. 13 of 2006 as amended by Law No. 31 of 2014. It introduces a renewed statutory framework for victim rights, restitution, compensation, recovery-related funding and the institutional functions of the Witness and Victim Protection Agency (LPSK). An assessment relying uncritically on the earlier protection law would therefore describe the wrong governing framework as of

October 2026 (Republic of Indonesia 2026b). Changes to substantive offences, criminal procedure and victim protection must be examined together rather than simply appending deepfake terminology to an older legal analysis.

The existing Indonesian literature provides an important starting point. Chairani, Yitawati and Pradhana (2024) examine the misuse of deepfake applications and the urgency of legal regulation; Hapid, Suntana and Royani (2024) concentrate on criminal responsibility and the principle of no punishment without fault; and Isnawan (2024) analyses offender liability in cases of non-consensual sexualised deepfakes. Haida and Nuriyatman (2024) highlight problems of victim protection, while Noviantama and Rahman (2025) review deepfake characteristics and victimological concerns. Ali et al. (2025) connect digital manipulation to victim harm and legal reform. Their contributions make it difficult to claim that Indonesian victimology scholarship has completely overlooked deepfakes.

A more defensible contribution is to ask how the various bodies of law can operate as a coordinated pathway of protection. Formal criminalisation is important, but a victim may seek immediate content containment, safe reporting, the preservation of evidence, emotional support or restitution before a prosecution is completed. Research published in the *International Journal of Society Reviews* has considered legal approaches to data privacy and cybersecurity and the relationship between technology regulation and social protection (Susilowati 2026). Building on this multidisciplinary orientation, the present article examines the interface between legal entitlements and practical protection needs rather than evaluating legislation solely by the severity of its criminal penalties.

The research question is therefore threefold. First, what forms of victimisation make harmful deepfakes a continuing social rather than merely a discrete criminal-law problem? Second, what protection and enforcement possibilities exist under Indonesia's legal framework as updated in 2026, and what doctrinal limits should be recognised? Third, how can those possibilities be organised into an implementable victim-centred response? The article argues that the principal problem is not simply a lack of a statute using the word 'deepfake'. It is a possible misalignment between the sequential harms of digitally fabricated identity and the fragmented procedures through which protection, criminal investigation and recovery are pursued.

This argument is deliberately limited. It does not present field interviews from Kabupaten Tegal or elsewhere, does not claim to measure the frequency of victimisation, and does not assess whether a proposed institutional pathway has already been implemented. It develops a normative and policy framework that should be tested subsequently through victim interviews, police and LPSK practice, platform procedures and appropriately anonymised case records. That distinction is especially important because conclusions about the availability of statutory powers

are different from conclusions about how effectively victims experience those powers in practice.

RESEARCH METHOD

This is a doctrinal and conceptual legal study, supplemented by a focused review of scholarship from criminology, gender studies, communication and technology law. Its purpose is prescriptive: to evaluate whether the available legal rules and institutional routes correspond to categories of harm recognised by victimology. It is not a systematic review, quantitative assessment or empirical study. No participant was recruited, no interview was undertaken and no unpublished case dataset was analysed for this article.

The primary legal materials are Indonesian statutes relevant to electronic conduct, personal data, sexual violence, criminal liability, criminal procedure and victim protection. They include Laws No. 44/2008, 12/2022, 27/2022, 1/2023, 1/2024, 20/2025, 1/2026 and 3/2026. Sources were checked against publicly available legislation databases, and their effective dates and repeal relationships are treated as analytically significant. Statutory categories are interpreted in context, without assuming that any synthetic-content activity automatically satisfies an offence definition. This is particularly necessary where intent, unlawfulness, distribution, public accessibility, harm or other constituent elements are required.

Secondary materials were purposively selected for their relevance to deepfakes, image-based abuse, victim experiences, criminal-law limitations and victim remedies. The analysis privileges identifiable peer-reviewed articles and verifiable publication metadata, including recent international studies and papers discussing Indonesia. The selection is critical rather than exhaustive: scholarship is compared for its central arguments, level of evidence and transferability to Indonesian institutions. The study avoids converting a finding from another country into an unsupported assertion about Indonesian victim prevalence.

Three analytical steps structure the examination. First, harm is mapped across the creation, dissemination and persistence of manipulated representations. Second, an issue-based statutory matrix asks whether criminal accountability, evidence handling, data protection and assistance can respond to each harm. Third, comparative European developments are used as policy examples, not as law binding Indonesia. The EU Directive 2024/1385 addresses non-consensual sharing of manipulated intimate material, while the EU AI Act provides transparency requirements for specified AI-generated or manipulated content; the two instruments have distinct purposes and conditions (European Union 2024a, 2024b).

The proposed response framework is evaluated through four criteria: clarity of legal threshold, timely accessibility for victims, preservation of procedural fairness and capacity to reduce recurring harm. These are normative criteria, not measured

service outcomes. The study's main limitation is the absence of institutional implementation data. The proposed coordination mechanisms consequently constitute reasoned recommendations requiring feasibility testing, not findings that Indonesian agencies currently operate an integrated deepfake support system.

RESULTS AND ANALYSIS

Understanding deepfake harm as continuing digital victimisation

The first finding of the doctrinal-conceptual analysis is that deepfake harm cannot be accurately represented by a single event of publication. Creation itself may breach a victim's sense of bodily or reputational autonomy, particularly where a person becomes aware of a manipulated depiction or receives a threat to disseminate it. McGlynn and Toparlak (2025) argue that legal responses focused solely on distribution can miss harm connected with creation. This does not entail that every private creative act should be criminalised: the legally relevant boundary must still be justified through sufficiently precise elements, purpose, context and safeguards for legitimate expression. It does mean that an analysis beginning only when material is uploaded can overlook earlier coercion and intimidation.

Dissemination adds a second mechanism of harm. When fabricated images or recordings are forwarded between accounts, reputational narratives can spread faster than factual correction. The victim may then have to address suspicion among colleagues, family members or educational institutions, even after falsity has been established. Chesney and Citron (2019) describe the wide range of personal and social risks associated with synthetic media. For targeted persons, harm does not depend on whether every observer believes the content is authentic: harassment, ridicule or opportunistic redistribution may continue despite public acknowledgement that a file was fabricated.

Persistence constitutes a third mechanism. Copies, reposts, search results, cached links and screenshots can make an initial response incomplete. Victims may need to report separate instances repeatedly, thereby encountering a cycle of documentation and distress. The literature on platform-mediated circulation stresses that the pathway through which content is replicated and encountered matters to the accumulation of harm (Gao 2026). Criminal conviction, although potentially significant for accountability, cannot in itself guarantee that all publicly accessible instances disappear. Victim protection must therefore operate on both an evidentiary timeline and a containment timeline.

These mechanisms are not restricted to non-consensual sexualised imagery. Impersonation intended to induce a financial transaction, the fabrication of political speech or manipulated media used for reputational sabotage can also implicate digital dignity and social trust. However, a victim-centred approach must retain differences among categories. The right institution, offence classification and

support needs can vary. Lazard et al. (2025) further show why gender-sensitive terminology matters when discussing image-based abuse. A generic 'fake content' label may fail to communicate how identity misuse, sexualised targeting and social power operate together.

For analytical purposes, the article distinguishes four needs without treating them as statutory rights available in every case: recognition of a credible report; containment of ongoing circulation; accountability where the elements of an offence are established; and recovery from material or non-material consequences. These needs are connected but not interchangeable. The ability to report a crime is not equivalent to access to specialist psychological assistance; an ability to request a platform review is not itself a guarantee of removal; and the existence of a restitution route does not predetermine its eligibility requirements or enforceability.

Indonesia's legal framework: available routes and doctrinal boundaries

The second finding is that Indonesian law already provides multiple legal entry points relevant to deepfake abuse, but their reach depends on the facts and applicable legal elements. The assertion that there is no legal regulation of deepfakes at all would be misleading. Equally, the existence of several statutes does not establish that all stages of harm are effectively remedied. A careful assessment must separate prohibited conduct, procedural powers, victim entitlements and recommendations for new inter-agency practice.

The ITE Law, as amended in 2024, remains relevant to electronic information, transmission and conduct falling under its current provisions. Yet legal analysis as of 2026 must consider changes made by the national Criminal Code and the Penal Adjustments Law rather than repeat the pre-2026 wording or numbering of provisions as though no repeal or adjustment occurred. A criminal-law conclusion requires matching alleged conduct to the operative provision and proving its elements. A deepfake that is offensive, false or socially damaging is not automatically a punishable violation of every electronic-content rule. The principle of legality and the protection of lawful expression remain essential constraints (Republic of Indonesia 2023, 2024, 2026a).

The Personal Data Protection Law provides a different analytical route. Facial imagery and voice-based identifiers can, depending on context and identifiability, raise issues of personal data or biometric data. The Act includes prohibitions concerning unlawful obtaining, disclosure or use of another person's personal data and falsification under specified conditions. Article 66 addresses falsification of personal data with the stated intent and potential harm requirements, illustrating why the technical production of a synthetic image cannot be equated mechanically with every statutory offence. Data-protection obligations and subject rights may

also be important outside a completed criminal prosecution (Republic of Indonesia 2022b).

For sexually targeted deepfakes, the Sexual Violence Crimes Law is central because it does not treat victim protection solely as an appendix to punishment. Its framework covers prevention, handling, protection and recovery. Whether an individual deepfake incident constitutes a particular electronic-based sexual violence offence under the law must nevertheless be examined against the relevant conduct and mental elements. Where the provisions do apply, safeguarding confidentiality and access to support should be addressed alongside evidence collection (Republic of Indonesia 2022a; McGlynn, Rackley and Houghton 2017). The Pornography Law has a distinct statutory focus; one must also consider relevant partial repeal of provisions by the 2023 Criminal Code before selecting a criminal charge (Republic of Indonesia 2008, 2023).

Criminal procedure has also changed. Law No. 20 of 2025 replaced the former Criminal Procedure Code and took effect on 2 January 2026. It includes stronger attention to the rights of victims and witnesses and to compensation and restitution arrangements, alongside powers and safeguards relevant to investigation. Accordingly, a proposal to preserve digital evidence should not imply that investigators may take unrestricted measures or that platforms must automatically transfer private user data to complainants. Evidence preservation should be lawful, proportionate, secured against alteration and compatible with data privacy and procedural fairness (Republic of Indonesia 2025).

The most consequential update for this article is Law No. 3 of 2026. The new Witness and Victim Protection Law supersedes the earlier statutory framework. Its subject matter includes witness and victim rights, the Witness and Victim Protection Agency, restitution, compensation and the Victim Endowment Fund. The new law strengthens the importance of treating recovery as a legal governance issue, not only a desirable social service. Nonetheless, not all assistance, compensation or procedural benefits attach automatically to every category of reported online harm. The operative eligibility rules, connections with relevant criminal offences and implementing regulations must be applied carefully (Republic of Indonesia 2026b).

Table 1 summarises the distinct roles of selected statutes. It is an analytical map rather than a statement that every listed provision applies to a typical or hypothetical deepfake incident. The appropriate route is contingent upon the particular allegation, the date of the act and subsequent legal changes.

Table 1. Issue-based mapping of Indonesian law relevant to harmful deepfakes

Instrument	Potential contribution	Key limitation / caution
ITE Law (Law 11/2008 as amended, including 1/2024)	Electronic conduct and offences, subject to current operative provisions	Check 2026 repeal/adjustment effects and each offence element.
Personal Data	Personal data rights;	Not every image or synthetic output

Instrument	Potential contribution	Key limitation / caution
Protection Law 27/2022	prohibitions on certain misuse and falsification	establishes unlawful processing or a criminal offence.
Sexual Violence Crimes Law 12/2022	Sexual-violence offences plus handling, protection and recovery	Applies where the requisite category and statutory elements are satisfied.
Pornography Law 44/2008 and Criminal Code 1/2023	Content-related prohibitions and general criminal-law framework	Account for partial repeal, legality, exceptions and case-specific proof.
Criminal Procedure Code 20/2025	Investigative procedure, victim and witness safeguards, relevant remedies	Procedural steps require lawful authority and evidence integrity.
Penal Adjustments Law 1/2026	Updates the relationship between criminal penalties and the new Code	Avoid reliance on superseded pre-2026 penalty rules.
Witness and Victim Protection Law 3/2026	Protection framework, LPSK, recovery-related mechanisms and restitution	Eligibility, implementation and special compensation rules still govern.

From legal fragmentation to a victim-centred response pathway

The third finding is a coordination problem rather than proof that Indonesian criminal justice is devoid of protection. Depending on the allegations, the same victim may need to communicate with police, a specialised assistance service, a data controller, an online platform and LPSK. If those interactions occur in isolation, the burden of navigating legal categories and repeating sensitive narratives may fall on the person already affected. In victimological terms, procedural repetition and avoidable exposure are potential sources of secondary harm. Evidence of the prevalence of these experiences in Indonesia would require separate empirical research, but their possibility is clear enough to inform procedural design (Henry, Flynn and Powell 2020; Ali et al. 2025).

An operational response should begin with a single, accessible first-contact pathway capable of identifying urgent safety and preservation issues without prematurely classifying every allegation as a specific criminal offence. A short initial record could identify the kind of synthetic content, where it was found, the person's consent concerns, any ongoing threat and whether the material remains accessible. Such an intake should minimise unnecessary reproduction of harmful files. It should provide information about possible police reporting, legally available specialist services and appropriate platform complaint mechanisms. This paragraph is a recommendation, not a claim that a national one-stop reporting portal presently exists.

Evidence and containment should follow parallel but coordinated tracks. The evidence track aims to document relevant URLs, timestamps, original reporting details and lawful forensic material, with controlled access and integrity safeguards. The containment track seeks prompt review or removal through available legal and

platform mechanisms, without assuming that a request is self-executing. The two tracks should be planned together so that necessary evidence is retained lawfully while public exposure is not prolonged merely because a file might be relevant to investigation. Retention periods and access restrictions must follow applicable law and appropriate institutional policy.

Next, decision-makers should apply a differentiated triage. A case involving impersonation for a monetary transaction may involve fraud and data misuse; a case involving fabricated statements may involve distinct questions of reputation, unlawfulness and lawful expression; a case involving coercive sexualised imagery may require urgent gender-sensitive protection. The triage should neither trivialise a non-sexual deepfake nor assume every forged representation justifies criminal sanction. McGlynn and Toparlak (2025) provide an important warning against waiting for distribution before recognising some forms of harm, while Flynn et al. (2025) show the need to attend to diverse victim experiences and contexts.

The recovery stage should be equally explicit. Victims may need guidance on avoiding repeated exposure, practical support in communicating with institutions, counselling referrals where appropriate, or documentation of identifiable losses. Restitution should be considered when the requirements under governing law are satisfied; it should not be promised automatically, and compensation should not be presented as a universal substitute. The 2026 Witness and Victim Protection Law provides an updated statutory basis for assessing these remedies alongside the Sexual Violence Crimes Law and the new Criminal Procedure Code (Republic of Indonesia 2022a, 2025, 2026b).

Finally, the response should incorporate review and accountability. Relevant institutions could track, without exposing victims' identities, whether referrals occurred, whether platform requests were acknowledged, whether evidence custody was secured and whether protection needs were reassessed. Such indicators describe a proposed evaluation agenda. No national implementation rates are reported here. The value of this approach is that it measures protection by the experiences and needs the system is intended to address, not by case disposal alone.

Table 2. Proposed victim-centred pathway (normative recommendation)

Stage	Priority action	Safeguard and evaluation question
1. Recognition	Accessible complaint intake; immediate safety and harm assessment	Was the account received without unnecessary repetition or blame?
2. Preservation	Lawful, secure documentation and chain-of-custody planning	Can evidence be authenticated without excessive storage or exposure?
3. Containment	Prompt, lawful platform reporting and response coordination	Was a remedy pursued without waiting unnecessarily for final conviction?
4.	Fact-sensitive offence	Were the operative 2026 laws and all

Stage	Priority action	Safeguard and evaluation question
Accountability	assessment and procedurally fair investigation	offence elements considered?
5. Recovery	Support referrals; consider restitution and eligible assistance	Did referrals address continuing harms rather than case closure alone?

Comparative lessons and limits

Comparative developments indicate that deepfake governance extends beyond criminal punishment. Directive (EU) 2024/1385 addresses certain non-consensual sharing of intimate or manipulated material through carefully formulated elements. The EU AI Act, Regulation (EU) 2024/1689, establishes transparency obligations for specified AI-generated or manipulated content, including deepfakes, subject to the relevant conditions and application framework. These two approaches should not be conflated: a disclosure rule deals primarily with transparency, whereas an offence of non-consensual sharing targets defined harmful conduct (European Union 2024a, 2024b).

Academic critique of EU measures is also relevant. Rigotti, McGlynn and Benning (2024) scrutinise image-based abuse provisions and their limits. Escobar Veas (2026) discusses the relationship between harm and privacy tests in the Directive's criminalisation framework. These analyses caution against transplanting isolated provisions without accounting for social harms, due-process guarantees and domestic legal structures. For Indonesia, the more portable lesson is institutional complementarity: regulation of synthetic-media transparency, criminal accountability for precisely defined wrongdoing, and service pathways for people affected should be assessed together.

A reform proposal should therefore proceed incrementally. First, legal guidance for investigators and services should map currently operative offences and remedies, including the 2026 updates. Second, cooperation protocols should enable lawful preservation and timely content responses while protecting user privacy and procedural rights. Third, authorities should gather anonymised evidence about delays, unmet support needs and the effects of repeat posting. Only after that evidence is collected should policymakers decide whether a new deepfake-specific criminal offence is necessary, and if so which distinct conduct existing offences cannot adequately capture. A blanket call for a new offence would risk duplicating existing provisions without fixing the main procedural barriers identified in this article.

This assessment also clarifies the conceptual contribution. Previous Indonesian studies have established that deepfakes raise questions of criminal liability and victimisation (Chairani, Yitawati and Pradhana 2024; Noviantama and Rahman 2025; Ali et al. 2025). The present framework does not claim to discover those harms for

the first time. Instead, it connects them to the post-2026 statutory environment and distinguishes recognition, preservation, containment, accountability and recovery as linked tasks. The relevant originality lies in this coordinated policy argument and in the explicit separation of victim needs from the elements of criminal offences. Whether such coordination improves outcomes is an empirical question that remains open.

CONCLUSION

Harmful AI deepfakes can create continuing digital victimisation through unauthorised identity manipulation, circulation, repeated exposure and associated social consequences. Their impact cannot be reduced to the moment an unlawful file is distributed or the date of an eventual criminal judgment. Victimology directs attention to autonomy, dignity, social standing, safe reporting and realistic recovery needs.

Indonesia has several potentially relevant legal mechanisms rather than a complete absence of regulation. The analysis must reflect the national Criminal Code and Criminal Procedure Code in force since January 2026, Penal Adjustments Law No. 1 of 2026, and particularly Witness and Victim Protection Law No. 3 of 2026, which replaced the earlier protection regime in May 2026. None of those statutes should be treated as automatically covering every deepfake allegation; offence elements and remedy eligibility remain case specific. The central weakness identified here is the risk that legally distinct mechanisms are experienced as fragmented responses to a connected sequence of harms.

A victim-centred framework should coordinate initial recognition, lawful evidence preservation, content containment, appropriate accountability and recovery services. Policy development should prioritise operating guidance and inter-agency coordination before assuming that more criminalisation is the only solution. Because this is normative research, the framework's feasibility and effectiveness require subsequent interviews, case analysis and institutional assessment. Those limitations do not negate its contribution: they establish the conditions under which a proposed protection pathway can be tested rather than accepted on assertion alone.

REFERENCES

- Ali, Mahrus, Zico Junius Fernando, Chairul Huda, and Mahmutarom. 2025. "Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims." *Substantive Justice International Journal of Law* 8 (1): 1–12. <https://doi.org/10.56087/substantivejustice.v8i1.306>.
- Chairani, Meirza Aulia, Krista Yitawati, and Angga Pramodya Pradhana. 2024. "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake." *Jurnal Rechtsens* 13 (1): 81–96. <https://doi.org/10.56013/rechtsens.v13i1.2668>.

- Chesney, Bobby, and Danielle Citron. 2019. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107 (6): 1753–1820. <https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security>.
- Escobar Veas, Javier. 2026. "The Criminalisation of Non-Consensual Sharing of Intimate Material under EU Law: Harm Matters, Privacy Doesn't." *New Journal of European Criminal Law* 17 (2): 235–50. <https://doi.org/10.1177/20322844261463534>.
- Flynn, Asher, Anastasia Powell, Asia Eaton, and Adrian J. Scott. 2025. "Sexualized Deepfake Abuse: Perpetrator and Victim Perspectives on the Motivations and Forms of Non-Consensually Created and Shared Sexualized Deepfake Imagery." *Journal of Interpersonal Violence*, online first. <https://doi.org/10.1177/08862605251368834>.
- Gao, Yongjie. 2026. "Sexualized Deepfake Abuse as Image-Based Sexual Abuse: A Scoping Review of Platform-Mediated Circulation and Cumulative Harm." *Trauma, Violence, & Abuse*, online first. <https://doi.org/10.1177/15248380261480163>.
- Haida, Rendi Syaputra Nur, and Eko Nuriyatman. 2024. "Urgensi Pengaturan Perlindungan Hukum terhadap Korban Deepfake melalui Artificial Intelligence (AI) dari Perspektif Hukum Pidana Indonesia." *Jurnal Hukum Respublica* 24 (1). <https://doi.org/10.31849/respublica.v24i01.23327>.
- Hapid, Fasa Muhamad, Ija Suntana, and Muhammad Yayan Royani. 2024. "Penerapan Asas Geen Straf Zonder Schuld dalam Penindakan terhadap Kejahatan Penyalahgunaan Teknologi Deepfake." *Jurnal USM Law Review* 7 (3): 1155–74. <https://doi.org/10.26623/julr.v7i3.9686>.
- Henry, Nicola, Asher Flynn, and Anastasia Powell. 2020. "Technology-Facilitated Domestic and Sexual Violence: A Review." *Violence Against Women* 26 (15–16). <https://doi.org/10.1177/1077801219875821>.
- Henry, Nicola, and Anastasia Powell. 2018. "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research." *Trauma, Violence, & Abuse* 19 (2): 195–208. <https://doi.org/10.1177/1524838016650189>.
- Isnawan, Fuadi. 2024. "Deepfake Pornography: How Criminal Liability of Perpetrators in the Indonesian Criminal Law Framework." *Jurnal Magister Hukum Udayana* 13 (3): 745–71. <https://doi.org/10.24843/JMHU.2024.v13.i03.p15>.
- Lazard, Lisa, Rose Capdevila, Emma L. Turley, Kathryn Gilfoyle, and Nelli Stavropoulou. 2025. "Deepfake Technology and Gender-Based Violence: A Scoping Review." *Trauma, Violence, & Abuse*, online first. <https://doi.org/10.1177/15248380251384271>.
- Maddocks, Sophie. 2020. "'A Deepfake Porn Plot Intended to Silence Me': Exploring Continuities between Pornographic and 'Political' Deep Fakes." *Porn Studies* 7 (4): 415–23. <https://doi.org/10.1080/23268743.2020.1757499>.
- McGlynn, Clare, Erika Rackley, and Ruth Houghton. 2017. "Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse." *Feminist Legal Studies* 25 (1): 25–46. <https://doi.org/10.1007/s10691-017-9343-2>.

- McGlynn, Clare, and Rüya Tuna Toparlak. 2025. "The 'New Voyeurism': Criminalizing the Creation of 'Deepfake Porn'." *Journal of Law and Society* 52 (2): 204–28. <https://doi.org/10.1111/jols.12527>.
- Noviantama, Doni, and Alif Alfani Rahman. 2025. "Deepfake: A Review from the Victimology Perspective." *Contemporary Issues in Criminal Law* 1 (2): 107–28. <https://doi.org/10.20885/CICL.vol1.iss2.art1>.
- Pacilli, Maria Giuseppina, Stefano Pagliaro, Ilaria Giovannelli, Federica Spaccatini, Elisa Berlin, and Chiara Rollero. 2024. "From Non-Traditional Sexual Behavior to Non-Legitimate Victims: Moral Virtue, Victim Blame, and Helping Intentions toward a Woman Victim of Image-Based Sexual Abuse." *Archives of Sexual Behavior* 53: 4079–88. <https://doi.org/10.1007/s10508-024-02970-x>.
- Rigotti, Carlotta, Clare McGlynn, and Franziska Benning. 2024. "Image-Based Sexual Abuse and EU Law: A Critical Analysis." *German Law Journal* 25 (9): 1472–93. <https://doi.org/10.1017/glj.2024.49>.
- Susilowati, Indah. 2026. "Legal Perspectives on Data Privacy and Cybersecurity in the Digital Age." *International Journal of Society Reviews* 3 (7). <https://injoqast.net/index.php/INJOSER/article/view/1444>.
- LEGAL INSTRUMENTS
- European Union. 2024a. Directive (EU) 2024/1385 on Combating Violence against Women and Domestic Violence. <https://eur-lex.europa.eu/eli/dir/2024/1385/oj>.
- European Union. 2024b. Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.
- Republic of Indonesia. 2008. Law No. 44 of 2008 on Pornography. <https://peraturan.bpk.go.id/Details/39740/uu-no-44-tahun-2008>.
- Republic of Indonesia. 2022a. Law No. 12 of 2022 on Sexual Violence Crimes. <https://peraturan.bpk.go.id/Details/207944>.
- Republic of Indonesia. 2022b. Law No. 27 of 2022 on Personal Data Protection. <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>.
- Republic of Indonesia. 2023. Law No. 1 of 2023 on the Criminal Code. <https://peraturan.bpk.go.id/Details/234935>.
- Republic of Indonesia. 2024. Law No. 1 of 2024 on the Second Amendment to the Electronic Information and Transactions Law. <https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024>.
- Republic of Indonesia. 2025. Law No. 20 of 2025 on the Criminal Procedure Code. <https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025>.
- Republic of Indonesia. 2026a. Law No. 1 of 2026 on Penal Adjustments. <https://peraturan.bpk.go.id/Details/337869/uu-no-1-tahun-2026>.
- Republic of Indonesia. 2026b. Law No. 3 of 2026 on Witness and Victim Protection. <https://peraturan.bpk.go.id/Details/349942/uu-no-3-tahun-2026>.