Adagium: Jurnal Ilmiah Hukum
E-ISSN: 2985-5128
Volume 4 Number 2 (2026), pp. 2018-2045
DOI: https://doi.org/10.70308/jez1gf79

Criminalization of AI-Based Sexual Deepfakes in Indonesian Criminal Law: The Urgency of Victim Protection in the Generative AI Era

Andi Barkan Mardianto[1*], M. Fakih[2], Zulkarnain Ridlwan[3]
[1,2,3] Universitas Lampung, Bandar Lampung, Indonesia
*Correspondence: andi_barkanm@yahoo.co.id

Received: 08 September 2026	Accepted: 22 October 2026	Published: 06 November 2026

Abstrak

Perkembangan sexual deepfake berbasis kecerdasan artifisial (AI) telah mengubah bentuk penyalahgunaan citra intim karena memungkinkan terciptanya representasi seksual yang realistis terhadap orang yang dapat diidentifikasi, meskipun korban tidak pernah terlibat dalam aktivitas yang digambarkan. Penelitian ini bertujuan menilai apakah hukum pidana Indonesia setelah berlakunya KUHP Nasional pada 2 Januari 2026 telah memadai untuk mengkriminalkan penciptaan dan peredaran representasi seksual sintetis tanpa persetujuan serta memberikan perlindungan efektif kepada korban. Penelitian menggunakan metode hukum normatif dengan pendekatan peraturan perundang-undangan, konseptual, dan perbandingan, didukung literatur ilmiah mutakhir. Hasil penelitian menunjukkan bahwa perlindungan masih terfragmentasi antara KUHP, UU TPKS, UU PDP, dan rezim elektronik; khususnya terdapat kekosongan terhadap penciptaan privat dan permintaan pembuatan sexual deepfake. Penelitian mengusulkan delik yang bersifat technology-neutral untuk penciptaan dan solicitation tanpa persetujuan, dengan pertanggungjawaban terpisah dan pemberatan bagi distribusi, ancaman, monetisasi, perbuatan berulang, dan korban anak. Model tersebut menempatkan otonomi seksual, martabat, dan identitas digital sebagai kepentingan hukum utama yang dilindungi.

Kata Kunci: deepfake seksual; kecerdasan artifisial generatif; kriminalisasi; perlindungan korban.

Abstract

Sexual deepfakes generated by artificial intelligence (AI) have transformed image-based sexual abuse by enabling realistic intimate depictions of identifiable persons who never participated in the depicted acts. This study examined whether Indonesian criminal law, as applicable after the national Criminal Code took effect on 2 January 2026, adequately criminalized the non-consensual creation and circulation of AI-generated sexual representations and protected victims. The study addressed a gap in Indonesian scholarship by evaluating the post-2026 interaction among the Criminal Code, the Sexual Violence Crime Law, the Personal Data Protection Law, and the amended Electronic Information and Transactions Law, while comparing recent European Union and United Kingdom approaches. A normative legal method was used with statutory, conceptual, and comparative approaches, supported by thirty recent Scopus-indexed journal articles published in 2022-2026. The analysis found fragmented protection: pornography provisions can reach circulation but do not

clearly capture private creation; electronic sexual violence provisions presuppose recording, transmission to a recipient, or electronic stalking; and personal-data offences protect data processing rather than sexual autonomy as such. The study proposes a technology-neutral offence covering intentional creation and solicitation of synthetic intimate depictions without consent, with separate and aggravated liability for distribution, threats, monetization, repeated conduct, and child victims. It contributes a victim-centered model that treats the primary protected interests as sexual autonomy, dignity, and digital identity, rather than deception alone.

Keywords: *Sexual Deepfake; Generative AI; Criminalization; Victim Protection.*

Introduction

The development of generative artificial intelligence (Generative AI) has transformed the nature of intimate-image abuse. Whereas image-based sexual abuse (IBSA) traditionally involved intimate photographs or videos that were actually created by or of the victim, deepfake technology, face-swapping tools, diffusion models, and nudification applications now enable perpetrators to construct convincing sexual representations from ordinary photographs, profile pictures, voice recordings, or facial data available online. In this setting, the victim never participated in the depicted sexual activity, yet the victim's identity is appropriated to portray nudity, sexual acts, or pornographic content as if they were authentic. Recent scholarship therefore increasingly uses the concept of AI-generated image-based sexual abuse (AI-IBSA) to emphasize that the central wrong is not merely falsity or deception, but the non-consensual production and circulation of sexual representations.[1]

This technical accessibility has expanded the scale of risk. A cross-national survey in Australia, the United Kingdom, and the United States found that 3.2% of 7,231 respondents reported having perpetrated AI-IBSA and 18.0% reported intentionally viewing AI-generated sexual images; men were more likely than women to report perpetration. Another survey of 7,230 respondents found that 7.0% reported AI-IBSA victimization, with women reporting broader emotional and social impacts even though overall victimization prevalence was higher among men. These findings establish two points: sexual deepfakes are no longer hypothetical, and their harm cannot be reduced to whether audiences actually believe the images are authentic. Victims may experience shame, loss of control, fear of dissemination, disruption of relationships, self-silencing in digital spaces, employment consequences, and threats of extortion or further violence.[2]

---

[1] Y. Gao, "Sexualized Deepfake Abuse as Image-Based Sexual Abuse: A Scoping Review of Platform-Mediated Circulation and Cumulative Harm", *Trauma, Violence, & Abuse* (2026), advance online publication, https://doi.org/10.1177/15248380261480163; M. Samaha and N. S. Hawi, "AI-Generated Image-Based Sexual Abuse: A Scoping Review", *Computers in Human Behavior Reports* 24 (2026): 101306, https://doi.org/10.1016/j.chbr.2026.101306; N. Henry et al., "'It's Still Abuse': Community Attitudes and Perceptions on AI-Generated Image-Based Sexual Abuse", *Information, Communication & Society* 29, no. 12 (2026): 3708-3728, https://doi.org/10.1080/1369118X.2026.2613437.

[2] R. Umbach et al., "AI-Generated Image-Based Sexual Abuse: Perpetration and Consumption across Three Regions", *Computers in Human Behavior* 179 (2026): 108935, https://doi.org/10.1016/j.chb.2026.108935; N. Henry et al., "'That Experience Still Haunts Me to This Day': A Multi-Region Survey on AI-Generated Image-Based Sexual Abuse Victimization",

Conceptualizing sexual deepfakes as a form of technology-facilitated sexual violence is also important because the term 'deepfake pornography' can obscure the non-consensual nature of the conduct. Pornography ordinarily concerns the production or consumption of sexual material, whereas a sexual deepfake that uses the face, body, or voice of a particular person without consent constitutes an intrusion into sexual autonomy and identity. McGlynn and Toparlak characterize the creation of sexual deepfakes as a form of 'new voyeurism' because technology creates a new form of taking or constructing intimate imagery without permission, even before the content is distributed. Viola and Voto likewise emphasize that technological design and affordances can facilitate intimate-image abuse, while Karagianni and Doh locate sexualized deepfakes within a broader spectrum of gender-based violence reinforced by digital infrastructure. The legal framework should therefore begin from the violation experienced by the person represented, rather than only from categories of obscenity or media authenticity.[3]

The need for legal reform is particularly relevant in Indonesia in 2026. Law No. 1 of 2023 on the Criminal Code took effect on January 2, 2026 and was subsequently adjusted through Law No. 1 of 2026 on Criminal Adjustment. Article 407 of the Criminal Code criminalizes producing, making, reproducing, duplicating, disseminating, broadcasting, offering, selling, renting, or providing pornography. However, the elucidation of Article 407 states that 'making pornography' does not include making it for oneself or for one's own interests. This formulation creates a problem when an offender produces a sexual deepfake for private gratification without distribution, because the representational harm to the victim has already arisen at the creation stage while the pornography provisions of the Criminal Code may leave that conduct outside criminal liability.[4]

Law No. 12 of 2022 on Sexual Violence Crimes recognizes electronic-based sexual violence. Article 14(1), among other matters, regulates the recording or taking of sexual images or screenshots without the consent of the person who is the object, the transmission of sexual electronic information or documents against the recipient's will for sexual purposes, and electronic stalking or tracking for sexual

---

International Journal of Human-Computer Interaction (2026), advance online publication, https://doi.org/10.1080/10447318.2026.2723677; D. Mahr, "Sexualized Deepfakes as a Socio-Technical Continuation of Gendered Power", *AI & Society* 41 (2026): 7407-7419, https://doi.org/10.1007/s00146-026-03080-z; C. Yavuz, "Adverse Human Rights Impacts of Dissemination of Nonconsensual Sexual Deepfakes in the Framework of European Convention on Human Rights: A Victim-Centered Perspective", *Computer Law & Security Review* 56 (2025): 106108, https://doi.org/10.1016/j.clsr.2025.106108.

[3] C. McGlynn and R. T. Toparlak, "The 'New Voyeurism': Criminalizing the Creation of 'Deepfake Porn'", *Journal of Law and Society* 52, no. 2 (2025): 204-228, https://doi.org/10.1111/jols.12527; M. Viola and C. Voto, "Designed to Abuse? Deepfakes and the Non-Consensual Diffusion of Intimate Images", *Synthese* 201 (2023): 30, https://doi.org/10.1007/s11229-022-04012-2; A. Karagianni and M. Doh, "A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes: Contextualizing Its Impact as AI-Generated Image-Based Violence under EU Law", *Porn Studies* (2024): 1-18, advance online publication, https://doi.org/10.1080/23268743.2024.2408277.

[4] Republic of Indonesia, Law No. 1 of 2023 on the Criminal Code [Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana] (2023); Republic of Indonesia, Law No. 1 of 2026 on Criminal Adjustment [Undang-Undang Republik Indonesia Nomor 1 Tahun 2026 tentang Penyesuaian Pidana] (2026).

purposes. These provisions are progressive, but their structure still proceeds from recording or taking an existing sexual image, transmitting material to a recipient, or stalking. In a sexual deepfake, by contrast, the sexual material may be synthesized from a lawful non-sexual photograph, and no sexual event ever existed to be recorded. An excessively expansive interpretation that treats 'recording' or 'taking an image' as including AI synthesis risks violating the principle of legality and the prohibition on analogy to the detriment of the accused.[5]

The next layer is Law No. 27 of 2022 on Personal Data Protection. A facial image may constitute biometric data when it enables unique identification, and Article 65 prohibits the unlawful acquisition, disclosure, and use of another person's personal data. Article 66 also prohibits creating or falsifying personal data with the intention of benefiting oneself or another person in a manner that may cause harm. These rules are relevant to obtaining source images, creating face embeddings, or using a victim's identity data, but their primary orientation is the lawfulness of data processing and the interests harmed by data falsification. They do not directly characterize the act of turning a person into the object of a synthetic sexual representation as an attack on sexual autonomy.[6]

Positive-law analysis must also account for changes to the Electronic Information and Transactions Law regime. Law No. 1 of 2024 once contained Article 27(1), which addressed broadcasting, displaying, distributing, transmitting, or making publicly accessible content that violated decency. Article II of that law, however, expressly provided that Article 27(1) and its related criminal provisions would apply only until the 2023 Criminal Code entered into force. Because the Criminal Code became effective on January 2, 2026, an analysis of sexual deepfakes undertaken at the time of this article should no longer treat Article 27(1) of the Electronic Information and Transactions Law as the principal standalone legal basis. This change makes a remapping of the applicable norms essential so that academic discussion does not continue to rely on a transitional provision whose period of operation has ended.[7]

Recent Indonesian scholarship has identified problems surrounding deepfake pornography, the right to be forgotten, and the challenges of victim protection. Yet the entry into force of the new Criminal Code in 2026, the criminal-law adjustment introduced by Law No. 1 of 2026, and comparative developments toward criminalizing both the creation and the commissioning of sexual deepfakes require a more specific evaluation. The European Union, through Directive (EU) 2024/1385, regulates the creation or manipulation of material that makes a person appear to

[5] Republic of Indonesia, Law No. 12 of 2022 on Sexual Violence Crimes [Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual] (2022).

[6] Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection [Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi] (2022); A. V. A. Nasution, Suteki, and A. D. Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse", *International Journal for the Semiotics of Law* 38, no. 7 (2025): 2489-2517, https://doi.org/10.1007/s11196-025-10265-0.

[7] Republic of Indonesia, Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions [Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik] (2024).

engage in sexual activity when that material is subsequently made publicly accessible without consent and is likely to cause serious harm. The United Kingdom has gone further: the Data (Use and Access) Act 2025 introduced an offence, effective February 6, 2026, covering the creation or request for creation of a 'purported intimate image' of an adult without consent or a reasonable belief in consent. These developments provide an important comparative benchmark for Indonesian criminal policy.[8]

The novelty of this study lies in its integrated evaluation of Indonesian criminal law after the national Criminal Code took effect on January 2, 2026 and in its formulation of an offence model that clearly separates the criminalization of creation or solicitation from the distribution of sexual deepfakes. Unlike approaches that merely map pornography, decency, or personal-data protection, this study places sexual autonomy, dignity, and digital identity at the center of the legally protected interests.

On that basis, this study has two objectives: first, to assess the adequacy and overlap of the Criminal Code, the Sexual Violence Crime Law, the Personal Data Protection Law, and the electronic-law regime after the amendment of the Electronic Information and Transactions Law in responding to AI-based sexual deepfakes; and second, to formulate a criminalization design that satisfies the principles of legality and proportionality, uses the criminal law as a rational ultima ratio, and provides effective victim protection in the era of Generative AI.

Research Method

This study employs normative legal research (doctrinal legal research) using three principal approaches: the statutory approach, the conceptual approach, and the comparative approach. The statutory approach is used to examine the construction of offences applicable at the time of the research, particularly the Criminal Code after its entry into force on January 2, 2026 and its adjustment through Law No. 1 of 2026, the Sexual Violence Crime Law, the Personal Data Protection Law, and the second amendment to the Electronic Information and Transactions Law. The conceptual approach distinguishes sexual deepfakes from ordinary misinformation and places them within the concepts of AI-generated image-based sexual abuse, sexual autonomy, dignity, digital identity, coercive control, and intimate intrusions. The comparative approach is used functionally to examine how the European Union and the United Kingdom construct offence elements for intimate or manipulated images without assuming that foreign models can be transplanted mechanically into Indonesia.

Primary legal materials consist of relevant Indonesian legislation and comparative instruments in force or adopted during 2024-2026. Their legal status was checked through October 10, 2026 so that the analysis would not rely on

[8] A. V. A. Nasution, Suteki, and A. D. Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse", *International Journal for the Semiotics of Law* 38, no. 7 (2025): 2489-2517, https://doi.org/10.1007/s11196-025-10265-0; European Parliament and Council, "Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence against Women and Domestic Violence", *Official Journal of the European Union* (2024); United Kingdom, Data (Use and Access) Act 2025, c. 18, sec. 138 (creating, or requesting the creation of, purported intimate image of adult) (2025), commenced February 6, 2026.

transitional norms that had already ceased to apply. The main secondary legal materials consist of thirty peer-reviewed journal articles published in 2022-2026 and directly relevant to sexual deepfakes, AI-IBSA, image-based sexual abuse, technology-facilitated sexual violence, criminalization, human rights, and platform governance. The articles were purposively selected from Scopus-indexed journals across quartiles Q1-Q4, with priority given to legal scholarship, systematic or scoping reviews, and cross-national empirical research capable of explaining forms of conduct, patterns of victimization, impacts, and regulatory responses.

Materials were collected through searches using combinations of the keywords 'sexual deepfake,' 'deepfake pornography,' 'AI-generated image-based sexual abuse,' 'non-consensual intimate deepfake,' 'image-based sexual abuse,' 'technology-facilitated sexual violence,' 'criminalisation,' and 'victim protection.' This study is not presented as a systematic literature review because its primary purpose is doctrinal analysis; empirical literature is used as an evidence base for assessing harm, the need for criminalization, and proportionality. Validation was undertaken by matching publisher metadata and DOI information and by checking the substantive relevance of each source to the research questions.

The legal analysis uses grammatical, systematic, and teleological interpretation. First, each conduct element in Indonesian law is mapped against the stages of AI-IBSA: obtaining a source image or data, creating or requesting the creation of content, retaining it, threatening, transmitting, and disseminating. Second, the fit of those elements is tested against the principle of lex certa and the prohibition on analogy. Third, the legal interests intended to be protected are compared with evidence of victim harm in the literature. Fourth, comparative models are used to formulate technology-neutral and victim-centered offence options. Because this study does not involve human participants, sensitive personal data, or experiments involving victims, human-subject research ethics approval was not required.

The comparative jurisdictions were selected for functional, not formal, equivalence: Directive (EU) 2024/1385 establishes a transposition obligation for Member States, while the United Kingdom supplies a more targeted offence concerning purported intimate images of adults. Neither model can be imported without assessing Indonesian constitutional legality, the protected legal interest, institutional capacity, and the distinction between creating and distributing content. The legal mapping uses the texts of Law No. 12/2022, Law No. 27/2022, Law No. 1/2023 as adjusted in 2026, and the relevant electronic-information provisions; the assessment is current through October 2026. The cited cross-national survey is not Indonesian prevalence evidence; the literature selection is doctrinal and purposive rather than an audited systematic review of precisely 30 Scopus-ranked journals.

Results and Discussion

Sexual Deepfakes as AI-Generated Image-Based Sexual Abuse

The literature analysis shows that, for legal purposes, the most adequate concept is not simply 'fake pornography' but AI-generated image-based sexual abuse. Gao's review shows that recent scholarship increasingly understands sexualized deepfake abuse as a form of IBSA whose harm accumulates through platform-mediated circulation. Samaha and Hawi identify three recurring features

in definitions of AI-IBSA involving an identifiable person: lack of consent, AI mediation, and sexual representation. This framework is important because it frees the law from dependence on any particular technique such as GANs, diffusion models, face swapping, or nudification. If an offence is defined by reference to a specific technology, the rule will quickly become obsolete as new generative systems produce photographs, videos, animations, or multimodal media without traditional 'swap' processes.[9]

The harm of a sexual deepfake also differs from the harm of misinformation. Mahr emphasizes that the core injury does not depend on successfully deceiving an audience, but on the creation and circulation of a non-consensual sexual representation that objectifies the victim's identity. Community-attitude research likewise shows that AI-IBSA continues to be understood as abuse, supporting the view that its synthetic character does not erase its sexual violation. In other words, an 'AI-generated' label or watermark may matter to information integrity, but it does not restore the victim's consent. Even material that is widely known to be false can still be used to humiliate, degrade, threaten, or control the person represented.[10]

The broader IBSA evidence strengthens this approach. Henry, Gavey, and Johnson demonstrate how intimate images can operate as instruments of coercive control within intimate relationships; Lucas explains how deepfakes can provide an additional tool for domestic abusers to threaten, extort, and undermine victims. Multi-country research also links IBSA perpetration with attitudes that minimize harm, while other studies show that victim-blaming and minimization remain significant. A legal design that intervenes only after distribution or viral circulation therefore risks overlooking an earlier stage that may already function as control: an offender can create the image, show it to the victim, and then use the threat of dissemination to secure compliance without ever publishing it widely.[11]

In terms of prevalence and impact, AI has made the creation stage cheaper and faster. Fido and colleagues found variation in public judgments about the creation and distribution of deepfake pornography according to the status and sex of the

---

[9] Y. Gao, "Sexualized Deepfake Abuse as Image-Based Sexual Abuse: A Scoping Review of Platform-Mediated Circulation and Cumulative Harm", *Trauma, Violence, & Abuse* (2026), advance online publication, https://doi.org/10.1177/15248380261480163; M. Samaha and N. S. Hawi, "AI-Generated Image-Based Sexual Abuse: A Scoping Review", *Computers in Human Behavior Reports* 24 (2026): 101306, https://doi.org/10.1016/j.chbr.2026.101306.

[10] D. Mahr, "Sexualized Deepfakes as a Socio-Technical Continuation of Gendered Power", *AI & Society* 41 (2026): 7407-7419, https://doi.org/10.1007/s00146-026-03080-z; N. Henry et al., "'It's Still Abuse': Community Attitudes and Perceptions on AI-Generated Image-Based Sexual Abuse", *Information, Communication & Society* 29, no. 12 (2026): 3708-3728, https://doi.org/10.1080/1369118X.2026.2613437.

[11] N. Henry, N. Gavey, and K. Johnson, "Image-Based Sexual Abuse as a Means of Coercive Control: Victim-Survivor Experiences", *Violence Against Women* 29, no. 6-7 (2023): 1206-1226, https://doi.org/10.1177/10778012221114918; K. T. Lucas, "Deepfakes and Domestic Violence: Perpetrating Intimate Partner Abuse Using Video Technology", *Victims & Offenders* 17, no. 5 (2022): 647-659, https://doi.org/10.1080/15564886.2022.2036656; A. Powell et al., "Perpetration of Image-Based Sexual Abuse: Extent, Nature and Correlates in a Multi-Country Sample", *Journal of Interpersonal Violence* 37, no. 23-24 (2022): NP22864-NP22889, https://doi.org/10.1177/08862605211072266; A. Flynn et al., "Victim-Blaming and Image-Based Sexual Abuse", *Journal of Criminology* 56, no. 1 (2023): 7-25, https://doi.org/10.1177/26338076221135327.

person depicted, including a tendency to judge creation for private gratification more leniently than creation for sharing. That result demonstrates precisely why an exemption for private consumption requires critical scrutiny when another person's sexual identity is being used. Henry and Beard further emphasize that IBSA perpetration encompasses taking, creating, sharing, threatening, coercing, and sending intimate images, while Paradiso and colleagues show that psychological, relational, and social factors interact in both victimization and perpetration.[12]

Mapping Indonesian Positive Law and the Normative Gaps

Mapping the applicable law reveals that protection is dispersed across several legal regimes. First, Article 407 of the Criminal Code, as adjusted in 2026, may reach conduct consisting of producing, making, duplicating, disseminating, broadcasting, offering, selling, renting, or providing pornographic material. Where a sexual deepfake has already been publicly distributed, these conduct elements can be linked relatively easily to dissemination. The problem arises at two levels. Conceptually, pornography rules are primarily oriented toward the character of the material rather than the non-consensual misuse of a specific person's identity. Normatively, the elucidation of Article 407 excludes 'making pornography' for oneself or one's own interests, so an undistributed sexual deepfake may escape the victim-protection rationale even though the victim's face or identity has already been synthetically sexualized.[13]

Second, Article 14 of the Sexual Violence Crime Law is the closest existing rule because it expressly recognizes electronic-based sexual violence. Yet the phrases 'recording,' 'taking an image,' or taking a sexual screenshot grammatically presuppose an existing sexual object or event that is recorded or captured. In AI-IBSA, an offender may upload a graduation photograph, workplace photograph, or ordinary selfie into a nudification service, and a new 'sexual image' emerges through computational inference and synthesis. Forcing the terms 'recording' or 'taking an image' to encompass generative synthesis risks sacrificing lex certa. In addition, Article 14(1)(b) focuses on the transmission of sexual content against the recipient's will for sexual purposes, so the structure of the protected victim may differ from the person whose identity is exploited and whose content is disseminated to the public.[14]

Third, the Personal Data Protection Law can address part of the production chain where an offender unlawfully obtains or uses personal data. A facial photograph processed for unique identification may qualify as biometric data, and

---

[12] D. Fido, J. Rao, and C. A. Harper, "Celebrity Status, Sex, and Variation in Psychopathy Predicts Judgements of and Proclivity to Generate and Distribute Deepfake Pornography", *Computers in Human Behavior* 129 (2022): 107141, https://doi.org/10.1016/j.chb.2021.107141; N. Henry and G. Beard, "Image-Based Sexual Abuse Perpetration: A Scoping Review", *Trauma, Violence, & Abuse* 25, no. 5 (2024): 3981-3998, https://doi.org/10.1177/15248380241266137; M. N. Paradiso, L. Rollè, and T. Trombetta, "Image-Based Sexual Abuse Associated Factors: A Systematic Review", *Journal of Family Violence* 39 (2024): 931-954, https://doi.org/10.1007/s10896-023-00557-z.

[13] Republic of Indonesia, Law No. 1 of 2023 on the Criminal Code [Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana] (2023); Republic of Indonesia, Law No. 1 of 2026 on Criminal Adjustment [Undang-Undang Republik Indonesia Nomor 1 Tahun 2026 tentang Penyesuaian Pidana] (2026).

[14] Republic of Indonesia, Law No. 12 of 2022 on Sexual Violence Crimes [Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual] (2022).

its use without a lawful basis may raise personal-data protection issues. However, not every source image used for a sexual deepfake is obtained unlawfully; a victim may have lawfully made the photograph public on social media, while the later processing that synthesizes nudity or sexual activity constitutes the new violation. Article 66 on creating or falsifying personal data also requires an intention to benefit oneself or another person in a manner that may cause harm. Motives such as sexual gratification, humiliation, revenge, control, or a supposed 'joke' are not always easily reduced to a legally certain concept of benefit. The Personal Data Protection Law is therefore important as a layer of data protection, but it is not an adequate substitute for an offence protecting sexual autonomy.[15]

Fourth, the amendment of the Electronic Information and Transactions Law reinforces the urgency of legal consolidation after 2026. Article II of Law No. 1 of 2024 limited the operation of Article 27(1) until the Criminal Code entered into force. Because that deadline has passed, law-enforcement practice and academic analysis should no longer treat Article 27(1) as the principal answer to digital indecency content. This does not mean that no other digital rules may apply to particular facts, such as threats or extortion, but the core issue of sexual deepfakes requires a more specific construction aligned with the national Criminal Code. More broadly, scholarship on deepfake regulation shows that rules fragmented across privacy, expression, data protection, and criminal law can undermine legal certainty.[16]

Table 1. Mapping the Stages of Sexual Deepfake Abuse and the Adequacy of Indonesian Law

Stage/ Conduct	Relevant Rule	Strength	Limitation for Sexual Deepfakes
Obtaining a photograph/ face as AI input	Personal Data Protection Law, Arts. 65-68	Reaches unlawful acquisition or use of personal data	A source image may come from a public source; the rule does not directly protect sexual autonomy
Creation/ nudification/ face swap without distribution	Criminal Code Art. 407; Sexual Violence Crime Law Art. 14	The Criminal Code recognizes 'making' pornography; the Sexual Violence Crime Law protects against recording/taking sexual images	The Criminal Code elucidation excludes production for oneself; the Sexual Violence Crime Law does not expressly cover AI synthesis from non-sexual imagery

[15] Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection [Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi] (2022).

[16] Republic of Indonesia, Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions [Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik] (2024); B. van der Sloot and Y. Wagensveld, "Deepfakes: Regulatory Challenges for the Synthetic Society", *Computer Law & Security Review* 46 (2022): 105716, https://doi.org/10.1016/j.clsr.2022.105716.

Stage/ Conduct	Relevant Rule	Strength	Limitation for Sexual Deepfakes
Request/ commission to a person or AI service	Not specifically regulated	May be connected to participation liability in particular circumstances	A request that does not result in content may not be reached; automated AI systems complicate the traditional construction of participation
Distribution/ provision to the public	Criminal Code Art. 407; other rules depending on the facts	Can readily be linked to dissemination or provision of pornographic content	A focus on pornographic material does not fully capture the violation of the victim's sexual identity
Threats, extortion, coercive control	Sexual Violence Crime Law Art. 14(2) and applicable threat/extortion offences	Allows aggravation and protection where content is used as a tool of control	Requires proof of particular purpose elements; initial creation may still fall outside the scope

Source: Authors' analysis based on Indonesian legislation in force as of October 10, 2026.

Comparative Regulation and the Direction of Criminalization

Comparative analysis reveals two policy directions. The European Union model, through Article 5 of Directive (EU) 2024/1385, criminalizes the creation, manipulation, or alteration of material that makes a person appear to engage in sexual activity where the conduct is followed by making the material publicly accessible without consent and where serious harm is likely. This model expressly recognizes manipulated material but still links production to publication. Karagianni and Doh regard the EU framework as an important step in contextualizing sexualized deepfakes as AI-generated image-based violence, while Rigotti and McGlynn had already warned that reforms focusing too narrowly on sharing may fail to address the broader spectrum of IBSA.[17]

The United Kingdom has moved further. Section 138 of the Data (Use and Access) Act 2025 introduced new offences into the Sexual Offences Act 2003 concerning the creation of, or request for the creation of, a purported intimate image of an adult. The offence centers on intentionally creating an intimate representation that appears to be a photograph or film of another person, the absence of consent,

[17] European Parliament and Council, "Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence against Women and Domestic Violence", *Official Journal of the European Union* (2024); A. Karagianni and M. Doh, "A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes: Contextualizing Its Impact as AI-Generated Image-Based Violence under EU Law", *Porn Studies* (2024): 1-18, advance online publication, https://doi.org/10.1080/23268743.2024.2408277; C. Rigotti and C. McGlynn, "Towards an EU Criminal Law on Violence against Women: The Ambitions and Limitations of the Commission's Proposal to Criminalise Image-Based Sexual Abuse", *New Journal of European Criminal Law* 13, no. 4 (2022): 452-477, https://doi.org/10.1177/20322844221140713.

and the absence of a reasonable belief that the person consented. The offence of requesting creation may be complete even if the final image is never successfully produced. The provision took effect on February 6, 2026. This design accords with the argument that creation and solicitation constitute independent sources of harm and should not be made contingent on subsequent distribution.[18]

Research on the United Kingdom's Online Safety Act shows that relying on platform moderation only after content has circulated may come too late because the harms of virality and replication have already occurred. Work on synthetic-content moderation further cautions that institutional design must distinguish among misinformation, impersonation, and non-consensual intimate media, while scholarship on nude and sexually explicit deepfakes describes the problem as multifaceted and incapable of being solved through a single instrument. The lesson for Indonesia is therefore not simply to increase criminal penalties, but to construct a chain of response: prevent identity-abusive creation, punish distribution and threats, enable rapid removal, preserve evidence, and support victim recovery.[19]

A human-rights perspective further strengthens this approach. Non-consensual sexual deepfakes may interfere with privacy, dignity, freedom of expression, and victims' participation in digital spaces. The harm may also take the form of a chilling effect: victims may reduce their use of social media, close accounts, avoid online public spaces, or restrict self-expression because they fear that their photographs will be used for nudification. Properly designed criminalization therefore does not merely restrict offenders' expression; it can also protect victims' freedom to be present and participate in digital spaces without the threat of forced sexualization.[20]

Justifying Criminalization: Harm, Sexual Autonomy, and Digital Identity

Criminalizing sexual deepfakes requires a substantive justification so that criminal law does not become a symbolic response to every technological innovation. First, the harm is real and distinguishable. Research across different methods documents psychological, reputational, relational, social, and economic consequences of IBSA and AI-IBSA. These consequences may arise even when the content is known to be false because the central problem is the loss of control over how a person's body and sexual identity are represented. Second, there is an

[18] United Kingdom, Data (Use and Access) Act 2025, c. 18, sec. 138 (creating, or requesting the creation of, purported intimate image of adult) (2025), commenced February 6, 2026; C. McGlynn and R. T. Toparlak, "The 'New Voyeurism': Criminalizing the Creation of 'Deepfake Porn'", *Journal of Law and Society* 52, no. 2 (2025): 204-228, https://doi.org/10.1111/jols.12527.

[19] B. Kira, "When Non-Consensual Intimate Deepfakes Go Viral: The Insufficiency of the UK Online Safety Act", *Computer Law & Security Review* 54 (2024): 106024, https://doi.org/10.1016/j.clsr.2024.106024; S. A. Fisher, J. W. Howard, and B. Kira, "Moderating Synthetic Content: The Challenge of Generative AI", *Philosophy & Technology* 37 (2024): 133, https://doi.org/10.1007/s13347-024-00818-9; M.-H. Maras and K. Logie, "Countering the Complex, Multifaceted Nature of Nude and Sexually Explicit Deepfakes: An Augean Task?", *Crime Science* 13 (2024): 31, https://doi.org/10.1186/s40163-024-00226-6.

[20] F. Romero Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content", *International Review of Law, Computers & Technology* 38, no. 3 (2024): 297-326, https://doi.org/10.1080/13600869.2024.2324540; C. Yavuz, "Adverse Human Rights Impacts of Dissemination of Nonconsensual Sexual Deepfakes in the Framework of European Convention on Human Rights: A Victim-Centered Perspective", *Computer Law & Security Review* 56 (2025): 106108, https://doi.org/10.1016/j.clsr.2025.106108.

infringement of sexual autonomy: the offender unilaterally decides that the victim will be placed in a particular sexual scene or body and creates an artifact that can be stored, displayed, used as a threat, or circulated at any time.[21]

Third, the harm of creation is independent from the harm of distribution. Creating a sexual deepfake establishes a continuing possibility of dissemination, extortion, and control, while leaving the victim uncertain about whether the file is being retained, replicated, or will eventually be published. The 'new voyeurism' analysis argues that legal models focused only on sharing fail to capture the wrong inherent in production itself. Public-attitude research may show that private creation is sometimes judged more leniently, but differences in social judgment are not a sufficient basis for disregarding the absence of consent by the person whose identity is used. If the Criminal Code exempts pornography made for oneself, another rule is needed that locates the wrong not in pornography as such but in creating an intimate representation of an identifiable person without consent.[22]

Fourth, digital identity should be recognized as part of the protected interest. The Personal Data Protection Law establishes that a face may constitute biometric data in certain circumstances, but a sexual deepfake combines identity data with a sexual context that was never consented to. The result is a form of 'synthetic intimacy': the material does not record the victim's actual body, but it attributes an intimate condition to the victim's identity. Indonesian scholarship has linked deepfake pornography with the right to be forgotten, while broader regulatory research shows that deepfakes often intensify pre-existing harms rather than always creating entirely new categories of injury. The preferred design is therefore to protect identity as the point of entry while treating sexual autonomy as the core protected interest.[23]

Fifth, criminalization must respect proportionality and subsidiarity. Not every digital manipulation depicting a person should become a criminal offence. The object of the offence should be limited to an intimate or sexual representation that reasonably depicts an identifiable person as nude, exposing intimate parts, or engaging in sexual activity. The mens rea should require intentional creation or

---

[21] N. Henry et al., "'Devastating, Like It Broke Me': Responding to Image-Based Sexual Abuse in Aotearoa New Zealand", *Criminology & Criminal Justice* 23, no. 5 (2023): 861-879, https://doi.org/10.1177/17488958221097276; M. M. R. Sheikh and M. M. Rogers, "Technology-Facilitated Sexual Violence and Abuse in Low and Middle-Income Countries: A Scoping Review", *Trauma, Violence, & Abuse* 25, no. 2 (2024): 1614-1629, https://doi.org/10.1177/15248380231191189; L. Lazard et al., "Deepfake Technology and Gender-Based Violence: A Scoping Review", *Trauma, Violence, & Abuse* (2025), advance online publication, https://doi.org/10.1177/15248380251384271.

[22] C. McGlynn and R. T. Toparlak, "The 'New Voyeurism': Criminalizing the Creation of 'Deepfake Porn'", *Journal of Law and Society* 52, no. 2 (2025): 204-228, https://doi.org/10.1111/jols.12527; D. Fido, J. Rao, and C. A. Harper, "Celebrity Status, Sex, and Variation in Psychopathy Predicts Judgements of and Proclivity to Generate and Distribute Deepfake Pornography", *Computers in Human Behavior* 129 (2022): 107141, https://doi.org/10.1016/j.chb.2021.107141.

[23] A. V. A. Nasution, Suteki, and A. D. Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse", *International Journal for the Semiotics of Law* 38, no. 7 (2025): 2489-2517, https://doi.org/10.1007/s11196-025-10265-0; A. Birrer and N. Just, "What We Know and Don't Know about Deepfakes: An Investigation into the State of the Research and Regulatory Landscape", *New Media & Society* 27, no. 12 (2025): 6819-6838, https://doi.org/10.1177/14614448241253138.

intentional solicitation, while the absence of consent must be a central element. Lawful conduct for law enforcement, health care, research, education, or a genuine public interest should receive narrowly defined exceptions, but labels such as satire or artistic expression should not automatically excuse conduct whose substance is the non-consensual sexualization of an identifiable individual. The concept of intimate intrusions provides a useful way to balance future-proofing with the requirements of legal certainty.[24]

A Proposed Offence Model for Indonesian Criminal Law

Based on the analysis, the proposed criminalization model is technology-neutral and layered. The first layer is an offence of creation or solicitation. Its core formulation could target any person who intentionally, without the consent of the person represented or without a reasonable belief in that person's consent, makes, generates, manipulates, or requests the creation through an electronic system of a synthetic intimate representation that reasonably makes an identifiable person appear nude, exposes intimate parts, or depicts that person engaging in sexual activity. 'Using AI' need not be an exclusive element of the offence; a formulation such as 'through an electronic system or digital technology, including artificial intelligence' would be more resilient to technological change.

Separating creation from distribution is necessary so that degrees of culpability and punishment remain proportionate. Private creation without distribution is appropriately criminalized because it violates sexual autonomy, but its penalty should be lower than the penalty for public distribution, monetization, or mass dissemination. The second layer should therefore cover distributing, transmitting, making accessible, offering, selling, or intentionally facilitating public access to the representation without consent. Distribution should not require proof that recipients believed the content to be authentic. The legally protected harm is not deception alone; it is sufficient that the material attributes a sexual condition to an identifiable person and is circulated without consent.[25]

The third layer consists of aggravating circumstances. Aggravation is appropriate where the victim is a child; where the offender is a current or former partner, a person in a position of power, an educator, an employer, or someone who obtained the image through a relationship of trust; where the conduct is undertaken for extortion, threats, revenge, economic exploitation, or coercive control; where the content is repeatedly or massively disseminated or used for profit; or where provable serious consequences result. In cases involving children, an adult-consent model cannot be applied because capacity and the protective interests of children are different. Research on broader IBSA confirms that relational context and control

[24] C. McGlynn, "Towards a New Criminal Offence of Intimate Intrusions", *Feminist Legal Studies* 32, no. 2 (2024): 189-212, https://doi.org/10.1007/s10691-024-09547-y.

[25] D. Mahr, "Sexualized Deepfakes as a Socio-Technical Continuation of Gendered Power", *AI & Society* 41 (2026): 7407-7419, https://doi.org/10.1007/s00146-026-03080-z; N. Henry et al., "'It's Still Abuse': Community Attitudes and Perceptions on AI-Generated Image-Based Sexual Abuse", *Information, Communication & Society* 29, no. 12 (2026): 3708-3728, https://doi.org/10.1080/1369118X.2026.2613437; C. McGlynn and R. T. Toparlak, "The 'New Voyeurism': Criminalizing the Creation of 'Deepfake Porn'", *Journal of Law and Society* 52, no. 2 (2025): 204-228, https://doi.org/10.1111/jols.12527.

significantly shape harm, so courts should be able to treat abuse of trust or power as an aggravating factor.[26]

The fourth layer concerns threats and solicitation. A threat to create or distribute a sexual deepfake can function as a tool of control even when the file does not yet exist. If an offender threatens to create a synthetic nude in order to force the victim to surrender money, maintain a relationship, send authentic images, or perform another act, the criminal-law structure should interact with extortion, threat offences, and the Sexual Violence Crime Law. For solicitation, the United Kingdom provides a useful lesson: requesting another person or a particular service to generate a purported intimate image may constitute a completed offence without waiting for the final output. This matters because an AI model may refuse a prompt, yet the act of commissioning still demonstrates the offender's intention to sexualize the victim without consent and contributes to a market demand that stimulates supply.

The fifth layer consists of narrow exceptions and defenses. The United Kingdom uses the concept of a 'reasonable excuse,' but transplanting an excessively open-ended phrase may create uncertainty. For Indonesia, it would be preferable to define objective categories of exception or justification connected to legitimate legal interests, such as authorized law enforcement, controlled medical or scientific use, and production necessary for self-defense or proof of a criminal offence accompanied by safeguards against distribution. The exception should not extend to a bare claim that the material was created as a private fantasy, because that is precisely the principal gap that arises when the identity of a real person is used without consent.

The model must also avoid overbreadth. Fictional representations that do not make a real person identifiable fall outside the proposed offence, unless another rule applies, such as child-protection law. Non-sexual editing, political parody, memes, or transformative works that do not place the subject in an intimate state should not be captured. Identifiability may be established through a face, voice, bodily mark, name, metadata, posting context, or a combination of characteristics that would allow a reasonable person to recognize the subject. With these limits, criminal law remains focused on the appropriation of sexual identity rather than synthetic media in general.

Table 2. Proposed Model for the Criminalization of Sexual Deepfakes

Component	Proposed Formulation/Principle	Victim-Protection Rationale
Protected interests	Sexual autonomy, dignity, intimate privacy, and digital identity	Shifts the focus from 'falsity' or 'pornography' to the violation suffered by the represented person

[26] N. Henry, N. Gavey, and K. Johnson, "Image-Based Sexual Abuse as a Means of Coercive Control: Victim-Survivor Experiences", *Violence Against Women* 29, no. 6-7 (2023): 1206-1226, https://doi.org/10.1177/10778012221114918; A. Powell et al., "A Multi-Country Study of Image-Based Sexual Abuse: Extent, Relational Nature and Correlates of Victimisation Experiences", *Journal of Sexual Aggression* 30, no. 1 (2024): 25-40, https://doi.org/10.1080/13552600.2022.2119292.

Component	Proposed Formulation/Principle	Victim-Protection Rationale
Object of the offence	A synthetic intimate representation of an identifiable person	Technology-neutral; covers deepfakes, face swaps, nudification, diffusion, and future technologies
Initial-stage actus reus	Creating, generating, manipulating, or requesting creation without consent	Closes the pre-distribution gap and reaches commissioning/solicitation
Distribution actus reus	Distributing, transmitting, providing, offering, selling, or making accessible	Captures the harms of circulation, virality, and monetization
Mens rea and consent	Intentional conduct; absence of consent and absence of a reasonable belief in consent	Preserves culpability and avoids strict liability for lawful creators
Aggravating circumstances	Child victim; power/intimate relationship; extortion; profit; mass/repeated distribution; serious impact	Differentiates degrees of culpability and harm
Narrow exceptions	Law enforcement, medical/scientific use, lawful evidentiary/self-defense use with safeguards	Preserves proportionality and legitimate freedoms
Victim remedies	Rapid takedown, de-indexing, evidence preservation, anonymity, restitution, psychosocial support	Reduces replication and secondary victimization

Source: Authors' formulation based on normative and comparative analysis.

Victim Protection, Platforms, and Digital Evidence

Criminalization will not be effective without rapid remedial mechanisms. Sexual deepfakes are highly replicable: once uploaded, a file can be downloaded, re-uploaded, cropped, given a new watermark, moved across platforms, or used as input for further generation. Research on viral non-consensual intimate deepfakes demonstrates the weakness of a response that depends too heavily on notice-and-takedown after widespread circulation. Victims therefore need a simple takedown route with clear response deadlines for non-consensual intimate content, together with de-indexing from search engines and hash-matching or perceptual-matching mechanisms to prevent re-upload where technically feasible. These duties are better framed as administrative or regulatory obligations for platforms rather than as automatic criminal liability for intermediaries for every item of user-generated content.[27]

[27] B. Kira, "When Non-Consensual Intimate Deepfakes Go Viral: The Insufficiency of the UK Online Safety Act", *Computer Law & Security Review* 54 (2024): 106024, https://doi.org/10.1016/j.clsr.2024.106024.

Procedural protection must also prevent secondary victimization. The reporting process should not require victims to prove that the audience believed the image to be authentic, because that standard misunderstands the legally relevant harm. It should be sufficient for the victim to show that the victim's identity is recognizable and that the intimate representation was created or circulated without consent. The victim's identity should be protected in public documents; court proceedings should adopt safeguards against unnecessary exposure of intimate material; and the examination of evidence should minimize reproduction of the files. The Sexual Violence Crime Law already provides a victim-rights orientation that can support integrated services, while the Personal Data Protection Law reinforces principles of data minimization and security during law enforcement.

From an evidentiary perspective, law-enforcement authorities need not always identify the specific AI model used. The critical elements are the synthetic or manipulated nature of the material, identifiability, mens rea, and absence of consent. Evidence may include the original file, metadata, provenance information or watermarks where available, platform logs, prompt history, service transactions, hashes, communications by the offender, the source image, devices, and forensic examination. Deepfake detectors can produce both false positives and false negatives; their output should therefore form only one part of the evidentiary chain rather than operate as the sole proof. Scholarship on synthetic-media governance likewise demonstrates the complexity of these systems, requiring criminal proof to remain based on comprehensive and contestable evaluation in court.[28]

The right to be forgotten and content removal are important, but they are not the same as destroying evidence. Indonesian scholarship has emphasized the difficulty faced by victims of deepfake pornography in obtaining removal. A more appropriate solution is a dual-track system: platforms and search engines remove or restrict public access as quickly as possible, while any forensic copy required for criminal proceedings is stored securely, with limited access and auditability. This approach prevents evidentiary needs from becoming a justification for leaving the content publicly available.[29]

Victim protection also requires compensation or restitution that accounts for the costs of digital recovery. Losses may include not only psychological treatment and lost income, but also the costs of content-removal services, internet monitoring, legal assistance, account security, and digital relocation. Because circulation may continue for years, remedies need to remain flexible. Research on the social rupture that can follow IBSA shows that a justice response focused solely on punishing the offender does not necessarily restore victims' social relationships or sense of

[28] S. A. Fisher, J. W. Howard, and B. Kira, "Moderating Synthetic Content: The Challenge of Generative AI", *Philosophy & Technology* 37 (2024): 133, https://doi.org/10.1007/s13347-024-00818-9; M.-H. Maras and K. Logie, "Countering the Complex, Multifaceted Nature of Nude and Sexually Explicit Deepfakes: An Augean Task?", *Crime Science* 13 (2024): 31, https://doi.org/10.1186/s40163-024-00226-6.

[29] A. V. A. Nasution, Suteki, and A. D. Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse", *International Journal for the Semiotics of Law* 38, no. 7 (2025): 2489-2517, https://doi.org/10.1007/s11196-025-10265-0.

control. A victim-centered approach must therefore combine punishment, recovery, and technological prevention.[30]

Limitations, Cautions, and Policy Implications

Several cautions should guide implementation of the proposed model. First, deepfake regulation can fall into technological exceptionalism, as if every problem created by synthetic media were entirely new. Research shows that many of the risks intensify pre-existing problems such as non-consensual pornography, disinformation, and privacy violations. Indonesian reform should therefore integrate any new offence into the structure of electronic-based sexual violence or a broader intimate-image-abuse regime rather than create an isolated legal island. The concept of intimate intrusions similarly supports future-proofing by targeting the right violated rather than the brand or type of technology used.[31]

Second, criminal law should not replace responsibility for technological design. Research on AI-generated pornography platforms shows varied governance practices and risks of producing illegal or exploitative material. Preventive measures may include restricting nudification involving identifiable persons, detecting prompt patterns that clearly seek non-consensual intimate imagery, limiting the use of children's faces, implementing abuse-reporting mechanisms, and conducting compliance audits. Technical controls must nevertheless respect user privacy, data security, and the risk of overblocking. The most effective policy model is layered governance: criminal law for culpable offenders, administrative obligations for platforms, and support services for victims.[32]

Third, the gendered context must be recognized without excluding other victims. Research on sexualized deepfakes demonstrates a strong dimension of gendered power, while recent empirical findings also show that patterns of victimization and impact may differ among groups, including men, LGBTQ+ persons, BIPOC communities, persons with disabilities, and younger people. The elements of an Indonesian offence should therefore be gender-neutral as to the victim, while prevention, support, and data-collection policies should remain gender-responsive. This avoids two extremes: ignoring structural patterns of violence against women or erasing protection for other groups of victims.[33]

---

[30] N. Henry et al., "'Devastating, Like It Broke Me': Responding to Image-Based Sexual Abuse in Aotearoa New Zealand", *Criminology & Criminal Justice* 23, no. 5 (2023): 861-879, https://doi.org/10.1177/17488958221097276.

[31] A. Birrer and N. Just, "What We Know and Don't Know about Deepfakes: An Investigation into the State of the Research and Regulatory Landscape", *New Media & Society* 27, no. 12 (2025): 6819-6838, https://doi.org/10.1177/14614448241253138; C. McGlynn, "Towards a New Criminal Offence of Intimate Intrusions", *Feminist Legal Studies* 32, no. 2 (2024): 189-212, https://doi.org/10.1007/s10691-024-09547-y.

[32] V. A. Lapointe et al., "The Governance of AI-Generated Pornography Platforms: A Content Analysis", *New Media & Society* (2026), advance online publication, https://doi.org/10.1177/14614448261421873.

[33] A. Karagianni and M. Doh, "A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes: Contextualizing Its Impact as AI-Generated Image-Based Violence under EU Law", *Porn Studies* (2024): 1-18, advance online publication, https://doi.org/10.1080/23268743.2024.2408277; D. Mahr, "Sexualized Deepfakes as a Socio-Technical Continuation of Gendered Power", *AI & Society* 41 (2026): 7407-7419, https://doi.org/10.1007/s00146-026-03080-z; L. Lazard et al., "Deepfake Technology and Gender-Based Violence: A Scoping Review", *Trauma, Violence, & Abuse* (2025), advance online publication,

Fourth, criminalization must preserve freedom of expression. A human-rights approach to harmful deepfakes requires carefully defined boundaries. The limits proposed in this study - an intimate state, an identifiable person, absence of consent, intentional conduct, and narrow exceptions - are designed to prevent the offence from becoming a general prohibition on media manipulation. A political satire that edits a facial expression is not equivalent to placing a political opponent in an explicit sexual scene; the law can distinguish the two through the nature of the content and the protected interest. Precision in the elements of the offence is therefore essential to compatibility with legal certainty and proportionality.[34]

Fifth, empirical research in Indonesia remains necessary. This study relies on an international evidence base and normative analysis, so it cannot measure the prevalence of sexual deepfakes in Indonesia, offender patterns, distribution channels, or victims' experiences of reporting. Future research should include survivor-centered qualitative studies, national surveys, analysis of judicial decisions after 2026, studies of investigative practice, and audits of Indonesian-language platform mechanisms. The absence of domestic empirical data does not, however, remove the normative problem already identifiable in the current legal framework: existing offence structures do not explicitly and clearly capture the creation or solicitation of synthetic sexual representations of identifiable persons without consent.

The Principle of Legality and the Limits of Interpretation in Response to New Technology

The principle of legality is the most important methodological limit when criminal law confronts technology that emerged after legislation was drafted. The fact that a sexual deepfake may be morally analogous to non-consensual intimate recording does not automatically authorize law-enforcement authorities to stretch the words 'record' or 'take an image' to encompass every generative process. Extensive interpretation may remain permissible where it stays within the reasonable linguistic meaning and purpose of the rule, but analogy that effectively creates a new criminal offence must be avoided. In a nudification case, for example, the offender does not record the victim's naked body; the system predicts or synthesizes pixels depicting a body that was never recorded. This ontological distinction is not merely technical. It determines whether the actus reus described by statute has actually occurred. Legislative reform is therefore safer for both victims and defendants than case-by-case interpretive creativity.

Legal certainty also requires a definition that does not depend too heavily on the term 'deepfake.' The term initially referred to particular deep-learning techniques, but public usage now includes face swaps, synthetic nudes, voice cloning, diffusion-generated images, and multimodal compositions. An offence should instead use the concept of a 'synthetic or manipulated intimate

https://doi.org/10.1177/15248380251384271; N. Henry et al., "'That Experience Still Haunts Me to This Day': A Multi-Region Survey on AI-Generated Image-Based Sexual Abuse Victimization", *International Journal of Human-Computer Interaction* (2026), advance online publication, https://doi.org/10.1080/10447318.2026.2723677.

[34] F. Romero Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content", *International Review of Law, Computers & Technology* 38, no. 3 (2024): 297-326, https://doi.org/10.1080/13600869.2024.2324540.

representation' and define it by outcome: an image, video, audiovisual file, or other form of digital media that reasonably depicts an identifiable person as being in an intimate state or engaging in sexual activity that was not authentically recorded. An outcome-based definition would make the law more resilient to changes in model architecture and avoid the need to prove that a file was created by a particular type of AI. This technology-neutral approach is consistent with scholarship emphasizing continuity between deepfake abuse and other forms of IBSA.[35]

The element of identifiability should be formulated objectively but contextually. The victim need not be recognizable to everyone; it is sufficient if identity can reasonably be determined from the face, voice, account name, tattoos, uniform, background, caption, or a combination of information available to the relevant audience. This is important because an offender may deliberately obscure part of the face while naming the victim in the accompanying text, or may create material for a school or workplace community that is still able to identify the subject. Conversely, wholly fictional synthetic sexual works that do not refer to a real person fall outside the proposed offence. This boundary keeps the focus on appropriation of individual identity and avoids a general criminal prohibition on digital sexual expression.

Consent must be understood as specific to both act and context. Consent to upload a facial photograph to social media is not consent to use that photograph as input for nudification; consent to create one intimate image is not consent to manipulate it into another sexual scene; and consent to creation is not automatically consent to distribution. The creation offence and the distribution offence should therefore each contain their own consent element. This prevents an offender from arguing that because the victim 'once sent a photograph,' all later transformations were authorized. It is also consistent with the character of IBSA, in which the loss of control over the creation and circulation of intimate imagery is a principal source of harm.[36]

Harmonizing the Criminal Code, the Sexual Violence Crime Law, the Personal Data Protection Law, and Case-Handling Stages

Reform need not always take the form of an entirely new standalone statute. Systematically, sexual deepfakes fit more coherently within electronic-based sexual violence or a broader category of intimate-image abuse under the Sexual Violence Crime Law because the principal protected interests are the victim and sexual autonomy. The Criminal Code can continue to address pornography and other general offences, while the Personal Data Protection Law protects the use of identity and biometric data. This division of functions prevents a single course of conduct from being forced into a rule that was not designed to address the relevant wrong.

---

[35] Y. Gao, "Sexualized Deepfake Abuse as Image-Based Sexual Abuse: A Scoping Review of Platform-Mediated Circulation and Cumulative Harm", *Trauma, Violence, & Abuse* (2026), advance online publication, https://doi.org/10.1177/15248380261480163; N. Henry and G. Beard, "Image-Based Sexual Abuse Perpetration: A Scoping Review", *Trauma, Violence, & Abuse* 25, no. 5 (2024): 3981-3998, https://doi.org/10.1177/15248380241266137.

[36] A. Powell et al., "A Multi-Country Study of Image-Based Sexual Abuse: Extent, Relational Nature and Correlates of Victimisation Experiences", *Journal of Sexual Aggression* 30, no. 1 (2024): 25-40, https://doi.org/10.1080/13552600.2022.2119292; N. Henry et al., "'Devastating, Like It Broke Me': Responding to Image-Based Sexual Abuse in Aotearoa New Zealand", *Criminology & Criminal Justice* 23, no. 5 (2023): 861-879, https://doi.org/10.1177/17488958221097276.

If the legislature instead chooses to place the new provision in the Criminal Code, the offence should still be connected to the victim rights and remedial mechanisms of the Sexual Violence Crime Law so that legal recognition does not stop at punishment of the offender.

In practice, a single sexual-deepfake episode may generate several distinct violations. An offender may unlawfully download the victim's photograph, upload it to a nudification service, purchase a premium package, generate dozens of images, send a sample to the victim for extortion, and then sell a collection through a closed channel. Each stage involves a different object and form of wrongdoing: data processing, creation of an intimate representation, threats or coercion, distribution, and economic gain. Law enforcement should therefore use a conduct- and protected-interest approach so that concurrence of offences does not produce disproportionate duplicate punishment while still recognizing distinct harms. Prosecutorial guidance can assist in determining when cumulative, alternative, or subsidiary charges are most appropriate.

The reporting stage should be designed on the assumption that a victim may have only a screenshot, a dead link, a notification from another person, or a threatening message without the original file. Police and platforms need rapid-preservation channels so that account data, IP information, transactions, lawfully obtainable prompt or log data, and upload metadata are not lost because of short retention periods. A preservation order is different from an obligation to disclose all data; access must remain subject to authorization and procedural law. In cross-border cases, international cooperation and data requests to foreign service providers become critical because the model, server, offender, and victim may be located in different jurisdictions.

The investigative stage requires protocols for handling intimate evidence. Files should be stored in a restricted, encrypted environment with access auditing; working copies should be minimized; and investigators should not use informal communication channels that increase the risk of leakage. Victim identity and content details should not be included unnecessarily in letters or documents that may circulate. This practice is not merely administrative privacy protection; it is part of preventing revictimization. Research on technology-facilitated sexual violence demonstrates that harms may persist over the long term, so poor legal-process practices may compound the injury that the justice system is intended to remedy.[37]

At the prosecution and trial stages, proof that a file is synthetic must be distinguished from proof attributing the conduct to a particular offender. Establishing that media is synthetic does not automatically prove who created it; conversely, an admission or account log may establish creation even when an AI detector is inconclusive. The evidentiary chain may include control of an account, payment for a service, lawfully obtained prompt history, a matching source image, communications with the victim, upload times, a forensic image of a device, and recipient witnesses. This distinction matters because the accuracy of deepfake detectors may change as generative models evolve or files are compressed. Judicial

[37] M. M. R. Sheikh and M. M. Rogers, "Technology-Facilitated Sexual Violence and Abuse in Low and Middle-Income Countries: A Scoping Review", *Trauma, Violence, & Abuse* 25, no. 2 (2024): 1614-1629, https://doi.org/10.1177/15248380231191189.

decisions should explain evidentiary reasoning transparently rather than make proof depend on a single automated tool.

Recovery should proceed in parallel with the criminal process rather than wait for a final and binding judgment. Takedown, de-indexing, account security, psychological support, legal assistance, and initial restitution may be needed immediately. Within the Sexual Violence Crime Law framework, the orientation toward victims' rights provides a normative basis for this parallel model. Accordingly, the success of sexual-deepfake policy should not be measured only by the number of suspects or convictions, but also by the speed with which circulation is halted, the reduction in re-upload, platform response times, victims' access to services, and the restoration of control over their digital identities.

As a matter of criminal policy, public education is also necessary to change social norms that minimize the creation of sexual deepfakes as 'just a joke' or a 'private fantasy.' Research on public judgments shows that creation may be viewed more leniently in certain contexts, while studies of victim-blaming show how minimization can weaken prevention. Criminal penalties without a corresponding change in social norms may therefore have limited preventive effect. Digital literacy in schools and universities should explain that public availability of a photograph does not grant a license to create a synthetic nude, that re-sharing can prolong harm, and that recipients can choose not to save or forward the material and can use reporting mechanisms instead.[38]

Finally, harmonization requires periodic, data-based evaluation. The government could create a specific AI-IBSA statistical category within electronic-based sexual-violence reporting without waiting for the next technological change. Data collection should distinguish creation, threats, distribution, monetization, the offender-victim relationship, age, and platform, while applying strict privacy safeguards. Such evaluation would allow the legislature to assess whether a creation offence is being applied proportionately, whether particular groups experience disproportionate effects, and whether platform duties are effective. An evidence-based approach is important to avoid both under-criminalization, which leaves victims without redress, and over-criminalization, which extends criminal law beyond the harm it is intended to address.

Proportionality of Sanctions and the Orientation of Sentencing

The structure of sanctions should reflect differences in seriousness among creation, circulation, and exploitation. For creation without distribution, extremely severe imprisonment may be disproportionate, particularly for a first-time offender whose conduct is not accompanied by threats or profit. The legislature could provide a combination of fines, supervision, court-ordered restrictions on the use of particular devices or services, educational programs, and imprisonment according to the degree of culpability. Mass distribution, monetization, extortion, or abuse of a relationship of trust, by contrast, warrants more serious punishment. This differentiation is important so that recognizing that creation itself can be harmful

[38] D. Fido, J. Rao, and C. A. Harper, "Celebrity Status, Sex, and Variation in Psychopathy Predicts Judgements of and Proclivity to Generate and Distribute Deepfake Pornography", *Computers in Human Behavior* 129 (2022): 107141, https://doi.org/10.1016/j.chb.2021.107141; A. Flynn et al., "Victim-Blaming and Image-Based Sexual Abuse", *Journal of Criminology* 56, no. 1 (2023): 7-25, https://doi.org/10.1177/26338076221135327.

does not automatically equate every form of conduct with the most extreme cases. Proportionality also allows courts to consider audience reach, duration of circulation, efforts to remove the material, the number of files, and proven consequences without making actual harm an absolute element of the basic offence.

Sentencing should also have a restorative orientation compatible with the nature of digital harm. Orders requiring an offender to delete all copies under the offender's control, provide access or information necessary for takedown, pay restitution, and refrain from contacting the victim may reduce continuing risk more directly than imprisonment alone. Restorative justice, however, must not be used to pressure victims into reconciliation in cases involving coercive control, power imbalances, or repeated threats. Decisions about resolution mechanisms must take victim safety and freely given consent into account. Research on intimate-image abuse as coercive control demonstrates that poorly designed mediation can reproduce the very dynamics of control that the legal process is intended to address.[39]

For corporations or service providers that knowingly build a business around creating non-consensual sexual deepfakes, criminal and administrative responses may differ from those appropriate to general-purpose platforms that are misused by users. Research on AI-pornography platforms highlights the need to examine platform governance, while work on viral intimate deepfakes shows the limitations of platform response after circulation. Indonesian law could impose due-diligence duties, complaint systems, transparency reporting, and administrative sanctions on providers that disregard systemic risk, while corporate criminal liability should be reserved for circumstances involving intent, business policy, or deliberate tolerance that satisfies an appropriate culpability standard. This distinction protects incentives for lawful innovation while preventing business models that profit from the non-consensual sexualization of other people's identities.[40]

Legislative Reform and Implementation Agenda

Institutionally, the most coherent reform option is to place sexual deepfakes within the regime of electronic-based sexual violence by adding a specific provision to the Sexual Violence Crime Law or an amending statute that expressly recognizes synthetic intimate representations. This is preferable to merely expanding pornography offences because the principal object of protection is not public morality, but consent, sexual autonomy, dignity, and a person's control over representations of the body and digital identity. A new rule could reach any person who intentionally creates or requests the creation of an image, video, or other digital media that reasonably depicts an identifiable person in an intimate state or engaging in sexual activity that is not authentic, where that person did not consent to the creation. Distribution, threats of distribution, extortion, monetization, repeated or

[39] N. Henry, N. Gavey, and K. Johnson, "Image-Based Sexual Abuse as a Means of Coercive Control: Victim-Survivor Experiences", *Violence Against Women* 29, no. 6-7 (2023): 1206-1226, https://doi.org/10.1177/10778012221114918.

[40] V. A. Lapointe et al., "The Governance of AI-Generated Pornography Platforms: A Content Analysis", *New Media & Society* (2026), advance online publication, https://doi.org/10.1177/14614448261421873; B. Kira, "When Non-Consensual Intimate Deepfakes Go Viral: The Insufficiency of the UK Online Safety Act", *Computer Law & Security Review* 54 (2024): 106024, https://doi.org/10.1016/j.clsr.2024.106024.

mass creation, abuse of power, and child victims could be structured as separate offences or aggravating circumstances. This design would avoid forcing the concept of 'recording' to carry a meaning for which it was not linguistically designed, thereby preserving the principle of legality while giving victims a more certain legal basis for protection.

The legislature should also establish operational parameters for consent. Consent to an ordinary photograph, a social-media upload, use of a profile picture, or creation of non-sexual content should not be treated as consent to synthetic sexual transformation. Likewise, consent to create an intimate representation does not by itself constitute consent to upload, sell, or send it to another person. Separating consent by act - creation, retention, distribution, and commercial use - would help investigators and courts avoid assuming that one form of consent applies universally. At the same time, the mens rea element should be drafted so that a person who unknowingly receives a file or uses a system that unexpectedly produces problematic content is not automatically criminalized. The focus should remain on knowledge or intent regarding identifiability, intimate character, and absence of consent. This structure is consistent with comparative developments that shift attention away from media authenticity and toward the victim's control over sexual representation.[41]

At the implementation level, joint guidance is needed for the Police, the Prosecutor's Office, the courts, the Ministry of Communication and Digital Affairs, victim-protection institutions, and platform providers regarding evidence preservation, takedown, de-indexing, electronic-data requests, and the handling of intimate material. The guidance should distinguish securing evidence from reproducing content. Every access to a synthetic sexual file should be logged, restricted to relevant personnel, and conducted through secure storage. When a victim reports a case, the first steps should include securing the URL, hash, account data, upload time, available metadata, and communications evidence, together with a preservation request to the platform before public access is removed. In this way, the victim's right to stop circulation is not artificially placed in conflict with evidentiary needs, and victims are less likely to be asked repeatedly to download or resend the same intimate material to multiple officials.

The legality test is conduct-specific. Acquisition of a source photograph may engage personal-data rules, but an ordinary photograph is not automatically biometric data: unique identification and the processing context matter. AI synthesis of an identifiable intimate representation without consent raises a distinct sexual-autonomy concern; the interpretation of Article 14 of the Sexual Violence Crime Law must nevertheless be grounded in its textual elements rather than an assumed absolute exclusion. Dissemination, threats, extortion and commercial exploitation may trigger additional existing provisions according to their facts. Article 407 of the Criminal Code must be read with the statutory elucidation

[41] C. McGlynn and R. T. Toparlak, "The 'New Voyeurism': Criminalizing the Creation of 'Deepfake Porn'", *Journal of Law and Society* 52, no. 2 (2025): 204-228, https://doi.org/10.1111/jols.12527; C. Yavuz, "Adverse Human Rights Impacts of Dissemination of Nonconsensual Sexual Deepfakes in the Framework of European Convention on Human Rights: A Victim-Centered Perspective", *Computer Law & Security Review* 56 (2025): 106108, https://doi.org/10.1016/j.clsr.2025.106108.

excluding pornography made for oneself or one's own interests, without equating that exception to immunity under every other law. These distinctions support a targeted possible legislative gap, not the proposition that sexual deepfakes are universally unregulated.

For any new offence, the legislature should expressly define: a recognizable living person or protected child; a materially sexual synthetic representation; absence of valid consent; intentional creation or knowing dissemination; a narrowly defined exemption for legitimate investigative, medical, evidentiary or clearly authorized uses; and differentiated penalties proportionate to actual exposure and harm. A private creation never circulated should not automatically attract the same severity as mass distribution or extortion. Platform responsibility should require separate evidence of knowledge, control and culpable participation; generalized availability of image-generation software is insufficient for criminal attribution. Digital investigation must separately verify file integrity, provenance, identity of the operator, synthetic manipulation, and lack of consent, using preserved originals, hashes, logs, witness evidence and expert assessment.

Table 3. Element-Based Test for Proposed Sexual-Deepfake Liability

Element	Proof and interpretive limit	Proposed legal consequence
Identifiable subject	Reliable comparison to an actual person; context matters for recognition	Exclude generic fictional depictions not attributable to a protected person
Sexual synthetic content	Expert review of alterations and sexual nature of representation	Do not equate all image editing with intimate abuse
Intent and consent	Requests, logs, communications, express authorization or justified belief	Avoid strict liability for service providers and innocent users
Conduct and exposure	Creation, commissioning, distribution, extortion or monetization must be separately proven	Tier penalties by conduct, risk and established harm
Digital integrity	Original files, cryptographic hash, acquisition trail and provenance evidence	Proof of synthesis does not alone identify the perpetrator

Conclusion

This study concludes that Indonesian criminal law in 2026 provides several legal entry points for responding to sexual deepfakes, but protection remains fragmented. Article 407 of the Criminal Code may reach the production and distribution of pornography, yet its orientation toward pornographic material and its elucidation excluding production for oneself or one's own interests leave a problem where a privately created deepfake uses the victim's identity. Article 14 of the Sexual Violence Crime Law provides a victim-centered foundation for electronic-based sexual violence, but its structure of recording or taking images, transmission to a recipient, and stalking does not expressly address AI synthesis from non-sexual images. The Personal Data Protection Law protects source data and the use of identity, but it does not replace protection of sexual autonomy. Following the entry

into force of the Criminal Code, the transitional Article 27(1) of the Electronic Information and Transactions Law should likewise no longer be treated as the principal solution.

The recommended model is a technology-neutral offence that criminalizes the creation of, and requests to create, synthetic intimate representations of identifiable persons without consent, accompanied by separate offences or aggravating circumstances for distribution, threats, extortion, monetization, repeated or mass conduct, abuse of power relationships, and child victims. The law should not require proof that audiences were deceived about authenticity because the principal harm lies in sexual autonomy, dignity, and digital identity. Criminalization should be combined with rapid takedown, de-indexing, secure preservation of evidence, victim anonymity, restitution, psychosocial services, and proportionate platform-governance obligations.

The academic contribution of this study is a post-2026 Criminal Code reconstruction that analytically separates 'pornography harm' from 'non-consensual synthetic sexual representation' and treats the latter as a form of intimate intrusion or AI-IBSA. This framework moves Indonesian criminal-law discourse beyond the question of which existing provision can be applied and toward the design of protected interests, actus reus, consent, mens rea, aggravating circumstances, defenses, and an integrated remedial architecture. Methodologically, the study also demonstrates the value of a statute-concept-comparison approach for assessing the adequacy of law in response to rapidly changing technology without abandoning the principle of legality.

The study is limited by its doctrinal character and the absence of primary data from victims, investigators, prosecutors, judges, platforms, or AI developers in Indonesia. Journal quartiles and indexing status may also change across years and subject categories, so bibliometric metadata should be rechecked at the time of submission. Future research should test the proposed model through empirical studies and analysis of the implementation of the Criminal Code and the Sexual Violence Crime Law after 2026, including how courts interpret 'making,' 'pornography,' 'sexually charged images,' 'consent,' and the use of facial data in cases involving synthetic media.

References

Birrer, A., and N. Just. "What We Know and Don't Know about Deepfakes: An Investigation into the State of the Research and Regulatory Landscape." *New Media & Society* 27, no. 12 (2025): 6819-6838. https://doi.org/10.1177/14614448241253138.

European Parliament and Council. "Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence against Women and Domestic Violence." *Official Journal of the European Union* (2024).

Fido, D., J. Rao, and C. A. Harper. "Celebrity Status, Sex, and Variation in Psychopathy Predicts Judgements of and Proclivity to Generate and Distribute Deepfake Pornography." *Computers in Human Behavior* 129 (2022): 107141. https://doi.org/10.1016/j.chb.2021.107141.

Fisher, S. A., J. W. Howard, and B. Kira. "Moderating Synthetic Content: The Challenge of Generative AI." *Philosophy & Technology* 37 (2024): 133. https://doi.org/10.1007/s13347-024-00818-9.

Flynn, A., E. Cama, A. Powell, and A. J. Scott. "Victim-Blaming and Image-Based Sexual Abuse." *Journal of Criminology* 56, no. 1 (2023): 7-25. https://doi.org/10.1177/26338076221135327.

Gao, Y. "Sexualized Deepfake Abuse as Image-Based Sexual Abuse: A Scoping Review of Platform-Mediated Circulation and Cumulative Harm." *Trauma, Violence, & Abuse* (2026). Advance online publication. https://doi.org/10.1177/15248380261480163.

Henry, N., and G. Beard. "Image-Based Sexual Abuse Perpetration: A Scoping Review." *Trauma, Violence, & Abuse* 25, no. 5 (2024): 3981-3998. https://doi.org/10.1177/15248380241266137.

Henry, N., N. Gavey, and K. Johnson. "Image-Based Sexual Abuse as a Means of Coercive Control: Victim-Survivor Experiences." *Violence Against Women* 29, no. 6-7 (2023): 1206-1226. https://doi.org/10.1177/10778012221114918.

Henry, N., N. Gavey, C. McGlynn, and E. Rackley. "'Devastating, Like It Broke Me': Responding to Image-Based Sexual Abuse in Aotearoa New Zealand." *Criminology & Criminal Justice* 23, no. 5 (2023): 861-879. https://doi.org/10.1177/17488958221097276.

Henry, N., R. Umbach, R. Shelby, G. Beard, and L. M. Given. "'It's Still Abuse': Community Attitudes and Perceptions on AI-Generated Image-Based Sexual Abuse." *Information, Communication & Society* 29, no. 12 (2026): 3708-3728. https://doi.org/10.1080/1369118X.2026.2613437.

Henry, N., R. Umbach, R. Shelby, and K. Gonzalez-Pons. "'That Experience Still Haunts Me to This Day': A Multi-Region Survey on AI-Generated Image-Based Sexual Abuse Victimization." *International Journal of Human-Computer Interaction* (2026). Advance online publication. https://doi.org/10.1080/10447318.2026.2723677.

Karagianni, A., and M. Doh. "A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes: Contextualizing Its Impact as AI-Generated Image-Based Violence under EU Law." *Porn Studies* (2024): 1-18. Advance online publication. https://doi.org/10.1080/23268743.2024.2408277.

Kira, B. "When Non-Consensual Intimate Deepfakes Go Viral: The Insufficiency of the UK Online Safety Act." *Computer Law & Security Review* 54 (2024): 106024. https://doi.org/10.1016/j.clsr.2024.106024.

Lapointe, V. A., S. Dubé, A. Petit, T. Kessai, S. Rukhlyadyev, V. Gravel, and D. Lafortune. "The Governance of AI-Generated Pornography Platforms: A Content Analysis." *New Media & Society* (2026). Advance online publication. https://doi.org/10.1177/14614448261421873.

Lazard, L., R. Capdevila, E. L. Turley, K. Gilfoyle, and N. Stavropoulou. "Deepfake Technology and Gender-Based Violence: A Scoping Review." *Trauma, Violence, & Abuse* (2025). Advance online publication. https://doi.org/10.1177/15248380251384271.

Lucas, K. T. "Deepfakes and Domestic Violence: Perpetrating Intimate Partner Abuse Using Video Technology." *Victims & Offenders* 17, no. 5 (2022): 647-659. https://doi.org/10.1080/15564886.2022.2036656.

Mahr, D. "Sexualized Deepfakes as a Socio-Technical Continuation of Gendered Power." *AI & Society* 41 (2026): 7407-7419. https://doi.org/10.1007/s00146-026-03080-z.

Maras, M.-H., and K. Logie. "Countering the Complex, Multifaceted Nature of Nude and Sexually Explicit Deepfakes: An Augean Task?." *Crime Science* 13 (2024): 31. https://doi.org/10.1186/s40163-024-00226-6.

McGlynn, C. "Towards a New Criminal Offence of Intimate Intrusions." *Feminist Legal Studies* 32, no. 2 (2024): 189-212. https://doi.org/10.1007/s10691-024-09547-y.

McGlynn, C., and R. T. Toparlak. "The 'New Voyeurism': Criminalizing the Creation of 'Deepfake Porn'." *Journal of Law and Society* 52, no. 2 (2025): 204-228. https://doi.org/10.1111/jols.12527.

Nasution, A. V. A., Suteki, and A. D. Lumbanraja. "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse." *International Journal for the Semiotics of Law* 38, no. 7 (2025): 2489-2517. https://doi.org/10.1007/s11196-025-10265-0.

Paradiso, M. N., L. Rollè, and T. Trombetta. "Image-Based Sexual Abuse Associated Factors: A Systematic Review." *Journal of Family Violence* 39 (2024): 931-954. https://doi.org/10.1007/s10896-023-00557-z.

Powell, A., A. J. Scott, A. Flynn, and S. McCook. "Perpetration of Image-Based Sexual Abuse: Extent, Nature and Correlates in a Multi-Country Sample." *Journal of Interpersonal Violence* 37, no. 23-24 (2022): NP22864-NP22889. https://doi.org/10.1177/08862605211072266.

Powell, A., A. J. Scott, A. Flynn, and S. McCook. "A Multi-Country Study of Image-Based Sexual Abuse: Extent, Relational Nature and Correlates of Victimisation Experiences." *Journal of Sexual Aggression* 30, no. 1 (2024): 25-40. https://doi.org/10.1080/13552600.2022.2119292.

Republic of Indonesia. Law No. 12 of 2022 on Sexual Violence Crimes [Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual]. 2022.

Republic of Indonesia. Law No. 27 of 2022 on Personal Data Protection [Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi]. 2022.

Republic of Indonesia. Law No. 1 of 2023 on the Criminal Code [Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana]. 2023.

Republic of Indonesia. Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions [Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik]. 2024.

Republic of Indonesia. Law No. 1 of 2026 on Criminal Adjustment [Undang-Undang Republik Indonesia Nomor 1 Tahun 2026 tentang Penyesuaian Pidana]. 2026.

Rigotti, C., and C. McGlynn. "Towards an EU Criminal Law on Violence against Women: The Ambitions and Limitations of the Commission's Proposal to Criminalise Image-Based Sexual Abuse." *New Journal of European Criminal Law* 13, no. 4 (2022): 452-477. https://doi.org/10.1177/20322844221140713.

Romero Moreno, F. "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content." *International Review of Law, Computers &*

Technology 38, no. 3 (2024): 297-326. https://doi.org/10.1080/13600869.2024.2324540.

Samaha, M., and N. S. Hawi. "AI-Generated Image-Based Sexual Abuse: A Scoping Review." *Computers in Human Behavior Reports* 24 (2026): 101306. https://doi.org/10.1016/j.chbr.2026.101306.

Sheikh, M. M. R., and M. M. Rogers. "Technology-Facilitated Sexual Violence and Abuse in Low and Middle-Income Countries: A Scoping Review." *Trauma, Violence, & Abuse* 25, no. 2 (2024): 1614-1629. https://doi.org/10.1177/15248380231191189.

Umbach, R., N. Henry, R. Shelby, G. Stevens, and K. Gonzalez-Pons. "AI-Generated Image-Based Sexual Abuse: Perpetration and Consumption across Three Regions." *Computers in Human Behavior* 179 (2026): 108935. https://doi.org/10.1016/j.chb.2026.108935.

United Kingdom. Data (Use and Access) Act 2025, c. 18, sec. 138 (creating, or requesting the creation of, purported intimate image of adult). 2025. Commenced February 6, 2026.

van der Sloot, B., and Y. Wagensveld. "Deepfakes: Regulatory Challenges for the Synthetic Society." *Computer Law & Security Review* 46 (2022): 105716. https://doi.org/10.1016/j.clsr.2022.105716.

Viola, M., and C. Voto. "Designed to Abuse? Deepfakes and the Non-Consensual Diffusion of Intimate Images." *Synthese* 201 (2023): 30. https://doi.org/10.1007/s11229-022-04012-2.

Yavuz, C. "Adverse Human Rights Impacts of Dissemination of Nonconsensual Sexual Deepfakes in the Framework of European Convention on Human Rights: A Victim-Centered Perspective." *Computer Law & Security Review* 56 (2025): 106108. https://doi.org/10.1016/j.clsr.2025.106108.