

Criminalizing Non-Consensual Sexual Deepfakes in Indonesia: Reconstructing Consent, Harm, and Digital Sexual Violence

Muhammad Fachrul Aljamili^{1*}, Novita Saputri², Wida Mustianingsih³,
Wirantomas⁴, Yoga Setiawan⁵

^{1,2,3,4,5} Faculty of Law, Universitas Merangin

*Correspondence: aljamilifachrul@gmail.com

Received: 31 August 2026

Accepted: 03 September 2026

Published: 16 September 2026

Abstrak

Perkembangan kecerdasan artifisial generatif memungkinkan pembuatan representasi seksual sintesis yang menampilkan identitas seseorang tanpa pernah terjadi peristiwa seksual yang nyata. Artikel ini menilai kecukupan hukum pidana Indonesia setelah berlakunya KUHP nasional pada 2 Januari 2026 dengan penelitian hukum normatif melalui pendekatan perundang-undangan, konseptual, dan komparatif terbatas. Setiap rezim diuji berdasarkan kepentingan hukum yang dilindungi, kata kerja perbuatan, mens rea, unsur korban dan persetujuan, tahap perilaku, serta bentuk pemulihan. Hasil penelitian menunjukkan kekosongan parsial: UU TPKS, UU ITE, UU Pornografi, dan UU PDP dapat menjangkau distribusi, pemrosesan data, atau bentuk perilaku tertentu, tetapi Pasal 14 UU TPKS belum secara *lex certa* mencakup penciptaan file seksual sintesis baru. Artikel ini mengusulkan secara *de lege ferenda* delik berbasis otonomi seksual yang mensyaratkan identifiabilitas, sifat seksual, kesengajaan, dan ketiadaan persetujuan yang spesifik. Model membedakan penciptaan/manipulasi, ancaman atau pemaksaan, distribusi, monetisasi, dan penyebaran berulang; menempatkan kerugian aktual sebagai faktor pemberat; serta memisahkan pertanggungjawaban pidana dari kewajiban regulatif berupa removal, preservation, dan anti-reupload. Pengecualian diuji melalui *necessity* dan *proportionality* untuk mencegah overcriminalization.

Kata Kunci: deepfake seksual; hukum pidana; kekerasan seksual berbasis elektronik; persetujuan; kecerdasan artifisial.

Abstract

*Generative artificial intelligence enables the creation of synthetic sexual representations depicting an identifiable person even though no real sexual event occurred. This article evaluates the adequacy of Indonesian criminal law after the national Criminal Code entered into force on 2 January 2026 through normative legal research using statutory, conceptual, and limited comparative approaches. Each regime is tested against the protected legal interest, conduct verbs, mens rea, victim and consent elements, stage of conduct, and available remedies. The study finds a partial normative gap: the Sexual Violence Crimes Law, Electronic Information and Transactions Law, Pornography Law, and Personal Data Protection Law can reach distribution, unlawful data processing, or particular forms of conduct, but Article 14 of the Sexual Violence Crimes Law does not, consistently with *lex certa*, clearly cover the creation of a new synthetic sexual file. As a *de lege ferenda* proposal, the article*

formulates a sexual-autonomy-based offence requiring identifiability, sexual character, intent, and specific absence of consent. The model distinguishes creation/manipulation, threats or coercive use, distribution, monetization, and repeated dissemination; treats actual harm as an aggravating factor; and separates criminal liability from regulatory duties concerning removal, preservation, and anti-reupload measures. Exceptions are assessed through necessity and proportionality to avoid overcriminalization.

Keywords: *criminal law; deepfake sexual abuse; electronic sexual violence; consent; generative artificial intelligence.*

INTRODUCTION

Deepfake technology has transformed image manipulation from an editing activity requiring high levels of expertise into a process that can be carried out through consumer applications, web-based services, and generative models capable of producing new images from a small number of source photographs. Legally, this shift matters because the object that harms the victim is not always a recording of an event that actually occurred. The content may be entirely synthetic, yet the victim's visual identity may still be recognizable to family members, co-workers, communities, or the public. Recent literature places sexual deepfakes within the spectrum of image-based sexual abuse because the harm does not depend on the authenticity of the sexual scene, but on the appropriation of the victim's identity and sexual autonomy without consent.¹ Consequently, criminal law that proceeds only from the paradigm of recording, possession, or dissemination of authentic intimate images risks failing to capture the character of this new form of abuse.

The need to formulate a criminal-law response has become increasingly urgent because deepfakes separate factual truth from representational harm. In conventional intimate-image cases, the victim was actually present in the situation that was recorded, whereas in a sexual deepfake the victim may never have engaged in the depicted conduct at all. Even so, recipients may perceive the representation as possibly true, while distribution algorithms accelerate reproduction and reduce the cost of dissemination. Comparative scholarship shows that legal frameworks designed for fraud, defamation, or pornography often provide partial but inconsistent protection against the non-consensual creation of deepfake pornography.² The central problem is therefore not merely a new technology, but a mismatch between older offence structures and a form of harm that does not require any real sexual event.

In Indonesia, the principal entry points lie in several legal regimes with different protective purposes. Law Number 12 of 2022 concerning Sexual Violence Crimes treats electronic-based sexual violence as a criminal offence, and Article 14 is

¹ Asher Flynn, Anastasia Powell, Adrian J. Scott, and Elena Cama, "Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging Form of Image-Based Sexual Abuse," *The British Journal of Criminology* 62, no. 6 (2022): 1341–1358, <https://doi.org/10.1093/bjc/azab111>.

² Ngonidzaishe T. Gotoro, "Unmasking Deception: Deepfake Regulation in the Context of South African Law, Could a Rethinking of Performers' Protection Rights Be the Answer?," *International Journal of Law and Information Technology* 32 (2024): eaee026, <https://doi.org/10.1093/ijlit/eaee026>.

framed around recording or taking images or screenshots of sexual content and certain transmissions without consent. Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law regulates the distribution, transmission, or making accessible of content that violates decency. Law Number 44 of 2008 concerning Pornography uses broader conduct verbs such as producing, creating, reproducing, and disseminating pornography. Law Number 27 of 2022 concerning Personal Data Protection adds protection against the unlawful acquisition, use, disclosure, and falsification of personal data. Recent Indonesian scholarship likewise shows that protection against deepfake pornography remains dispersed across several regimes and has not yet been constructed as a single, consistent victim-centred category.³⁴⁵⁶⁷

The issue became more complex after Law Number 1 of 2023 concerning the Criminal Code entered into force on 2 January 2026. On the same date, Law Number 1 of 2026 concerning Criminal Adjustment also took effect to harmonize criminal provisions outside the Criminal Code with Book One of the Criminal Code. The principle of legality requires criminal offences to be formulated predictably, while the principle of culpability requires a fair connection between mental state and conduct. Therefore, extensions of terms such as "create," "pornography," "content that violates decency," or "take an image" must not become analogies detrimental to the defendant. Systematic interpretation may still explain relationships among norms, but the creation of a new synthetic file must be distinguished from recording or taking an image of an object that already exists.⁸⁹

The proper dimension of protection must also be determined. A public-morality approach questions the pornographic character of material, but does not always place the consent of the person whose identity is used at the center. A privacy approach may require a violation of personal data or a private sphere, even though a deepfake can be created solely from photographs that are publicly available. A reputational approach requires an assessment of honor and social consequences, while a victim may experience a sexual attack on identity even before the content is widely disseminated. European legal scholarship shows a shift from the term "revenge pornography" toward image-based sexual abuse to emphasize that the core harm lies in the non-consensual creation, capture, or distribution of intimate material, including manipulated media.¹⁰ This conceptual shift provides an important basis for testing the architecture of Indonesian criminal law.

³Komang Bagus Wicaksana Putra and Gusti Ayu Arya Prima Dewi, "Urgensi Pengaturan Tindak Pidana Deepfake Pornografi di Indonesia," *Kertha Wicara: Jurnal Ilmu Hukum* 13, no. 10 (2024): 530–541, <https://doi.org/10.24843/KW.2024.v13.i10.p5>.

⁴Indonesia, Law Number 27 of 2022 concerning Personal Data Protection.

⁵Indonesia, Law Number 44 of 2008 concerning Pornography.

⁶Indonesia, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

⁷Indonesia, Law Number 12 of 2022 concerning Sexual Violence Crimes, art. 14.

⁸Indonesia, Law Number 1 of 2026 concerning Criminal Adjustment.

⁹Indonesia, Law Number 1 of 2023 concerning the Criminal Code.

¹⁰ Carlotta Rigotti, Clare McGlynn, and Franziska Benning, "Image-Based Sexual Abuse and EU Law: A Critical Analysis," *German Law Journal* 25, no. 9 (2024): 1472–1493, <https://doi.org/10.1017/glj.2024.49>.

Deepfakes also create evidentiary problems that cannot be separated from substantive law. A defendant may claim that the content is satire, fantasy, fiction, or the automatic output of a generative model; conversely, the victim must prove the connection between their identity and a digital output that can be altered or deleted within minutes. At the same time, the ability to generate false content produces what is often called the liar's dividend: the possibility that authentic evidence may itself be dismissed as a deepfake. A systematic review of deepfakes in the criminal justice system identifies pornography, fraud, information manipulation, erosion of trust, and falsification of evidence as interconnected categories of risk.¹¹ Accordingly, offence design must operate together with rules on metadata preservation, forensic assessment, and platform responsibility to preserve evidence when a report is received.

In criminal law, not every wrongful behavior should be criminalized. The principles of *ultimum remedium*, proportionality, freedom of expression, artistic freedom, research, and the public interest require carefully defined limits. An exception should not be granted merely because a work is labelled satire, parody, artistic, or research. A safer test consists of five questions: whether there is a legitimate public interest; whether use of a real person's identity is genuinely necessary; whether the sexual element has a real connection to that purpose; whether a less intrusive alternative such as anonymization is available; and whether the risk of harm is reduced through access restrictions, labelling, or other safeguards. The weaker the public interest and the easier it is to recognize the victim's identity in a sexual context, the stronger the justification for criminalization or regulatory intervention. Conversely, fictional works that do not identify a particular person, coincidental resemblance, or uses that are genuinely necessary and proportionate should fall outside the core offence.¹²

This article proceeds from the thesis that Indonesian law has a gap not because no applicable norm exists at all, but because the available norms are built around fragmented protected interests. The Sexual Violence Crimes Law is oriented toward sexual violence, the ITE Law toward certain electronic conduct, the Pornography Law toward control of pornographic material, and the PDP Law toward personal-data processing. When a single act involves creating a synthetic face, compositing another person's body, distribution through a platform, monetization, and threats against the victim, several statutes may overlap without providing a consistent answer as to the principal offence. This fragmentation creates a risk that charging depends on the selected normative forum rather than the underlying nature of the harm.

The novelty of this study lies in a reconstruction that shifts the center of gravity of criminalization from image authenticity and public morality to sexual autonomy and consent to the use of identity in synthetic sexual representations. In this article, sexual autonomy is positioned at two levels. Under positive law, it is derived from

¹¹ Maria-Paz Sandoval, Maria de Almeida Vau, John Solaas, and Luano Rodrigues, "Threat of Deepfakes to the Criminal Justice System: A Systematic Review," *Crime Science* 13 (2024): 41, <https://doi.org/10.1186/s40163-024-00239-1>.

¹² Dominika Kuźnicka-Błaszczowska and Nadiya Kostyuk, "Emerging Need to Regulate Deepfakes in International Law: The Russo-Ukrainian War as an Example," *Journal of Cybersecurity* 11, no. 1 (2025): tyaf008, <https://doi.org/10.1093/cybsec/tyaf008>.

the consent and victim-protection orientation of the Sexual Violence Crimes Law and the constitutional protection of dignity and personhood. At the *de lege ferenda* level, sexual autonomy is used as the primary protected legal interest for formulating an offence that expressly reaches synthetic representations. Dignity and privacy serve as supporting interests, while reputational harm is treated primarily as a possible consequence rather than a constitutive element of the offence. This hierarchy prevents overlap among sexual violations, data violations, and defamation.¹³

Against that background, this article addresses three questions. First, to what extent can existing criminal-law categories reach the non-consensual creation and dissemination of sexual deepfakes? Second, where does disharmony arise among the protection of sexual autonomy, decency, personal data, and legal certainty after the national Criminal Code entered into force? Third, what model of criminalization can fill the gap without excessively expanding criminal law? The answers are directed toward an offence design that is operational for investigators and judges while providing predictable boundaries for the public and electronic-system operators.

The debate on sexual deepfakes also shows that the protected interest of criminal law cannot be reduced to reputation. A victim may suffer a violation even when people around them know that the image is fake. What is taken away is control over the sexual representation of the self, namely the ability to determine whether, when, and in what context one's identity is placed in sexual material. Sexual autonomy is therefore the primary interest; dignity, privacy, and security are supporting interests; while job loss, social stigma, discrimination, or blackmail are forms of actual harm relevant to aggravation and sentencing. This distinction also explains why a content-morality-based offence is not identical to an offence based on non-consensual sexual representation.

The next question is whether actual harm must be proven as an element. This article argues that the core offence may be designed as a conduct offence because the protected legal interest is already violated when the identity of a particular person is intentionally placed in a sexual representation without specific consent. Actual harm need not be a constitutive element, but remains important for determining aggravation, restitution, and sentencing proportionality. To prevent overcriminalization, a *de minimis* threshold should exclude coincidental resemblance, unintended outputs or outputs that cannot reasonably identify a particular person, experiments that do not produce a sexual representation of the target, and situations in which the actor reasonably possesses valid consent. The law therefore need not wait until content goes viral, but it should not punish thoughts or technical failures that have not yet produced a prohibited object.

RESEARCH METHOD

This study is normative legal research using statutory, conceptual, and limited comparative approaches. The regimes are selected functionally because each regulates one part of the problem: the 1945 Constitution as a standard of rights and

¹³ Clare McGlynn and Carlotta Rigotti, "From Virtual Rape to Meta-rape: Sexual Violence, Criminal Law and the Metaverse," *Oxford Journal of Legal Studies* 45, no. 3 (2025): 554–582, <https://doi.org/10.1093/ojls/gqaf009>.

legal certainty; the Sexual Violence Crimes Law for electronic-based sexual violence and victim recovery; the ITE Law for electronic conduct and access to content; the Pornography Law for the production and distribution of pornographic material; the PDP Law for identity and data processing; and the 2023 Criminal Code together with the 2026 Criminal Adjustment Law for general principles of criminal responsibility. The study does not use surveys, interviews, case counts, or statistics as empirical proof. Factual literature is used only to understand the characteristics of the technology and typologies of harm, so the article does not draw conclusions regarding case frequency or enforcement effectiveness in Indonesia.

Each norm is tested using the same six parameters so that conclusions regarding the partial gap can be reproduced: (1) the protected legal interest; (2) the prohibited conduct verb; (3) the form of mens rea; (4) the position of the victim, identifiability, and consent; (5) the stage of conduct reached—creation/manipulation, possession, threat/coercion, distribution, monetization, or repeat dissemination; and (6) the remedy or legal consequence. The conceptual approach distinguishes privacy harm, reputational harm, public morality, and sexual autonomy. The limited comparative approach uses literature on image-based sexual abuse, deepfake regulation, and platform governance from Europe, the United Kingdom, South Africa, and cross-country scholarship as design benchmarks rather than as transplanted law. Each comparative option is reassessed against legality, culpability, proportionality, and Indonesia's institutional structure.¹⁴

The analysis proceeds in three stages. First, a normative-adequacy matrix is constructed using the six parameters above to distinguish rules that can already be applied from areas requiring reform. Second, horizontal and vertical synchronization is undertaken with respect to protected legal interests, *lex specialis*, legality, dignity, and protection of the person. Third, a prescriptive construction is developed that separates the normative status of each instrument: the core offence as a matter of criminal legislation; removal/preservation and anti-reupload as regulatory duties of platforms or electronic-system operators; restitution and protection as a victim-recovery regime; and digital evidence as a matter of procedural law and forensic practice. A recommendation is considered adequate only if it can reach non-consensual synthetic creation, continues to require culpability, contains an identifiability threshold, and provides a necessity-proportionality exception.

Table 1. Normative Adequacy Matrix

Parameter	Test Question	Analytical Function
Protected legal interest	Does the norm protect sexual autonomy, privacy/data, reputation, or public morality?	Determines the justification for criminalization and <i>lex specialis</i> .
Conduct	Which conduct verbs are covered: recording, creating, manipulating, sending, disclosing, or processing?	Tests whether synthetic creation is covered without analogy.
Mens rea	Is intent, knowledge, or another form of fault required?	Preserves the principle of culpability and limits strict liability.

¹⁴ Julia Hörnle, "Fighting the Beast of Image-Based Sexual Abuse. Part 1—the Criminal Law and Platform Regulation," *International Journal of Law and Information Technology* 34 (2026): eaag006, <https://doi.org/10.1093/ijlit/eaag006>.

Victim/consent	Are identifiability and absence of consent elements of the offence?	Tests the victim-centred character of the norm.
Stage of conduct	Creation, possession, coercion, distribution, monetization, repeat dissemination?	Separates the core offence from aggravating factors or additional conduct.
Remedy	Criminal sanction, restitution, takedown, preservation, or systemic duties?	Prevents all solutions from being forced into criminal sanctions.

RESULTS AND DISCUSSION

Deepfake Sexual Abuse and the Limits of Existing Criminal-Law Categories

Sexual deepfakes fundamentally reveal a mismatch between "event reality" and "representational reality." The primary focus of this article is visual and audiovisual representation; synthetic voice is included only when it contextually forms part of a sexual representation or sexual coercion directed at a particular person. The identifiability standard operates across all three through a combination of face, voice, name, attributes, captions, accounts, or other context linking the output to the victim. The evidentiary methods differ, however: visual material can be analyzed through source images, compositing, metadata, and frames; synthetic voice depends more heavily on audio characteristics, model or voice-cloning logs, comparison recordings, and communication context. Outside a sexual context, ordinary voice cloning falls outside the proposed offence.¹⁵

Article 14 of Law Number 12 of 2022 concerning Sexual Violence Crimes is the positive-law norm closest to the victim's protected legal interest. However, the verbs "record," "take an image," and "take a screenshot" grammatically presuppose an object, event, or display that is already available to be recorded or captured. Synthetic generation differs because the system creates a new file from a model, prompt, source image, or combination of data. Systematic interpretation may still cover screen recording of existing sexual content or recapturing a digital output that has already been created, but treating the initial generative process as "taking an image" risks becoming an analogy that expands the offence. Because the principle of legality prohibits analogy to the detriment of the defendant, the safe approach to initial synthetic creation is an explicit statutory amendment rather than stretching the meaning of Article 14.¹⁶

Table 2. Article 14 TPKS and Synthetic-Creation Gap

Article 14 Element/Issue	Relatively Clear Coverage	Problem in Synthetic Creation	Consequence
Recording	Recording sexual activity/representation that has already occurred or is already available.	A generative model can produce a new file without recording any sexual event involving the victim.	It is unsafe to extend "recording" to initial synthetic generation.

¹⁵ Asher Flynn, Anastasia Powell, Adrian J. Scott, and Elena Cama, "Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging Form of Image-Based Sexual Abuse," *The British Journal of Criminology* 62, no. 6 (2022): 1341–1358, <https://doi.org/10.1093/bjc/azab111>.

¹⁶Indonesia, Law Number 12 of 2022 concerning Sexual Violence Crimes, art. 14.

Taking an image	Taking a photograph/image of an existing object or representation.	The source photograph may be non-sexual; the system creates a new sexual output.	Verbs such as "create/manipulate/generate" are needed if creation is to be covered.
Screenshot	Capturing a sexual display that has already appeared on a screen.	Not identical to the process that creates the first output.	May cover certain reproduction, but not the entire generative process.
Transmission	Sending/distributing certain electronic information or documents.	Does not resolve the gap where a new deepfake is created but not yet sent.	Distribution may remain a separate offence/aggravating factor.
Consent	Central to victim protection within the structure of the Sexual Violence Crimes Law.	Consent to an ordinary photograph is not the same as consent to sexual representation.	Consent must be specific to the category of sexual use.

This gap matters because the creation stage can independently violate a victim's control over their sexual representation. The justification for a conduct offence is not that every synthetic file necessarily causes demonstrable trauma, but that the identity of a particular person has intentionally been placed in a sexual context without relevant consent. Actual harm such as widespread dissemination, job loss, blackmail, or serious disturbance remains relevant as an aggravating factor and a basis for restitution. A *de minimis* threshold should exclude outputs that do not identify the target, coincidental resemblance, technical failure, and experiments that do not produce a sexual representation of a particular person. With these limits, criminalizing creation can be justified before distribution without turning all uses of AI into criminal offences.¹⁷

Law Number 1 of 2024 concerning the Second Amendment to the ITE Law provides a route for addressing the distribution, transmission, or making accessible of certain electronic content. The protected legal interest of the decency provision is not identical to that of the proposed deepfake offence. A content-morality-based offence assesses the nature of the content and the protected public order, whereas an offence based on non-consensual sexual representation assesses the appropriation of a particular person's sexual identity without consent. This difference in protected interest matters so that reform does not merely add charges for the same conduct. The ITE Law can continue to operate where the electronic-distribution elements are satisfied, while a consent-based offence becomes central when the principal wrong is the sexual exploitation of identity.

Law Number 44 of 2008 concerning Pornography contains a broad range of conduct verbs, including producing, creating, reproducing, duplicating, disseminating, broadcasting, and making pornography available. Textually, the verb "create" is closer to deepfake production than the verbs in Article 14 of the Sexual Violence Crimes Law. The pornography regime, however, was not designed with the absence of consent of the person whose identity is used as a central element. Indonesian research on criminal liability for deepfakes likewise shows that the pornography regime may provide a basis in certain circumstances, but still leaves

¹⁷ Carlotta Rigotti, Clare McGlynn, and Franziska Benning, "Image-Based Sexual Abuse and EU Law: A Critical Analysis," *German Law Journal* 25, no. 9 (2024): 1472–1493, <https://doi.org/10.1017/glj.2024.49>.

problems concerning the victim, mens rea, and normative fragmentation. The existence of the verb "create" therefore does not eliminate the need for a victim-centred offence explaining why misuse of a real person's identity constitutes a distinct wrong.¹⁸

Law Number 27 of 2022 concerning Personal Data Protection adds a layer of protection when facial images, biometric data, or personal information are unlawfully acquired, used, disclosed, or falsified. A data violation, however, is not identical to sexual deepfake abuse. A source photograph may be publicly available and still be processed into a non-consensual sexual representation. Indonesian scholarship on the protection of deepfake victims confirms that privacy and data are important parts of protection, but do not fully replace a consent-based construction of sexual violence. Accordingly, the PDP Law may operate cumulatively when the elements of data processing are satisfied, while the proposed offence protects sexual autonomy regardless of the initial legality of acquiring the photograph.¹⁹

The limitations of existing categories are also apparent in the victim element. The proposed standard is whether the representation "reasonably identifies a particular person in the context of its use." This test does not require recognition by the entire public, but demands more than generic resemblance. Courts may cumulatively assess the face, voice, name, tags, captions, uniform, tattoos, accounts, location, metadata, prompts, and the perpetrator's communications. If the output merely resembles a generic facial type and there is no evidence that the actor targeted a particular person, identifiability is not established. This boundary is important for *lex certa* and prevents the criminalization of fictional characters or coincidental resemblance.

The law must also distinguish between deepfakes that deceive and deepfakes that cause harm even when labelled. An "AI-generated" label may reduce the risk of public deception, but it does not necessarily eliminate the sexual violation. A victim may still suffer abuse when their name and face are used in a synthetic sexual scene that clearly states the content is fictional. In this context, transparency is an important mechanism against disinformation, but it is not an automatic defence to identity-based sexual violence. Scholarship on international deepfake regulation shows that the technological threat is not singular; it may affect information, reputation, security, and individual rights in different ways.²⁰

Taken as a whole, this mapping shows that Indonesian law has the capacity to reach several manifestations of sexual deepfakes, particularly the dissemination of content that violates decency, blackmail, threats, or unlawful use of data. No single provision, however, expressly states that creating a synthetic sexual representation depicting an identifiable person without that person's consent is a distinct criminal

¹⁸Fuadi Isnawan, "Deepfake Pornography: How Criminal Liability of Perpetrators in the Indonesian Criminal Law Framework," *Jurnal Magister Hukum Udayana* (Udayana Master Law Journal) 13, no. 3 (2024): 745–771, <https://doi.org/10.24843/JMHU.2024.v13.i03.p11>.

¹⁹Siti Nur Hidayah and Gunawan Hadi Purwanto, "Legal Protection of Victims of AI-Driven Deepfake Pornography: An Analysis within Indonesian Law," *Al-Risalah Jurnal Ilmu Syariah dan Hukum* 26, no. 1 (2026): 917–935, <https://doi.org/10.24252/al-risalah.vi.59043>.

²⁰ Dominika Kuźnicka-Błaszczowska and Nadiya Kostyuk, "Emerging Need to Regulate Deepfakes in International Law: The Russo–Ukrainian War as an Example," *Journal of Cybersecurity* 11, no. 1 (2025): tyaf008, <https://doi.org/10.1093/cybsec/tyaf008>.

offence. The gap is described as partial because it is not equivalent to the absence of all sanctions. The problem is uncertainty about which norm should be central, when protection begins, and which legal interest is actually violated.

The mapping of conduct must consistently distinguish among creation/manipulation, possession, threat or use for coercion, distribution, monetization, and repeat dissemination. Not all categories warrant the same degree of criminal-law weight. Creation/manipulation involving an identifiable person without consent is a candidate for the core *de lege ferenda* offence. Private possession, particularly where a file is received unsolicited, should not automatically be criminalized; responsibility becomes stronger only when possession forms part of threats, distribution, procurement, or a relevant child-protection regime. Threat/coercion, distribution, monetization, and repeat dissemination increase the harmfulness or exploitation and are therefore better treated as additional offences or aggravating factors.

Table 3. Tiered Conduct and Proportionality

Conduct Category	Proposed Status	Proportionality Rationale
Creation / manipulation	Core <i>de lege ferenda</i> offence where identifiability + sexual nature + intent + no specific consent are established.	Sexual autonomy is already violated at the creation stage.
Possession	Not automatically a general offence.	Risk of overcriminalization where a file is received unsolicited or there is no further purpose.
Threat / coercive use	Additional offence or aggravating factor.	Adds coercion, fear, and abuse of power.
Distribution	Additional offence/aggravating factor when carried out with the required knowledge.	Expands exposure and replication of harm.
Monetization	Aggravating factor and basis for confiscating proceeds.	Adds economic exploitation.
Repeat dissemination	Aggravating factor.	Shows repetition and increases harm after knowledge/reporting.

This distinction affects when an offence is considered complete. If the principal protected legal interest is sexual autonomy over identity, the creation offence is complete when a non-consensual representation capable of identifying the victim has been generated with the required intent, even if it has not yet been sent. Distribution becomes a separate act or an aggravating factor because it broadens exposure. Under this structure, investigators need not wait for publication before acting when strong evidence shows that the perpetrator has created the material and is preparing its dissemination. Attempt liability, however, should remain limited to acts directly aimed at producing the representation, not merely searching for software or harboring a fantasy that has not been realized. Such a boundary maintains the balance between prevention and the principle that criminal law does not punish thoughts.

Normative Fragmentation after the TPKS Law, the ITE Law, the Pornography Law, the PDP Law, and the New Criminal Code

Normative fragmentation creates a *lex specialis* problem more complex than simply choosing the statute carrying the heaviest penalty. The Sexual Violence Crimes Law is *lex specialis* for sexual violence and contains a victim-oriented framework, restitution, handling, and adapted evidentiary rules. The ITE Law is *lex*

specialis for electronic conduct. The Pornography Law is a substantive regime governing pornographic material, while the PDP Law governs data control. A single sexual deepfake may satisfy parts of several regimes simultaneously. Without a clear center, enforcement may shift from sexual protection to debates over decency, or vice versa, depending on the construction of the indictment.

The principle of *lex specialis systematis* requires interpreters to consider the system of norms, the subjects, the protected object, and the purpose of the legislation. For non-consensual sexual deepfakes, the Sexual Violence Crimes Law should serve as the principal framework when the conduct is sexualized abuse directed at a particular person. That choice becomes effective, however, only if the conduct formulation reaches synthetic creation. Otherwise, law-enforcement authorities are pushed toward the ITE Law or the Pornography Law, weakening the centrality of consent. This demonstrates that the problem cannot be resolved through rules of legal preference alone; the elements of the offence must be amended so that the *lex specialis* system contains a norm genuinely compatible with the technology.

The entry into force of the national Criminal Code on 2 January 2026 heightens the importance of consistency in principle. Deepfake reconstruction must not create strict liability for every AI user. For the core offence, the safest form of fault is intent: the perpetrator knows that the representation is intended to depict a particular person and knows that specific consent is absent. The term reckless disregard should not be imported as an independent standard without legislative definition. If the legislature wishes to reach conscious risk-taking, that element should be formulated expressly as awareness of a real risk that consent is absent, rather than equated with ordinary negligence. Model errors, unexpected outputs, or coincidental resemblance do not meet that standard.

The principle of legality also requires that the formulation not depend on technical terms that quickly become obsolete. If legislation refers only to generative adversarial networks, diffusion models, or the term "deepfake," technological development may soon outrun the definition. A more durable formulation should be function-oriented: "creating or manipulating a visual, audiovisual, or voice representation that reasonably depicts or resembles a particular person in a sexual context, using digital technology or other synthetic means." A functional definition preserves legal certainty because the prohibited elements remain identifiable without being tied to a single AI architecture.

In determining *mens rea*, a purpose of obtaining profit should not be required. Many sexual deepfakes are created for humiliation, revenge, intimidation, experimentation within online groups, or the perpetrator's sexual gratification. If profit is made an element, highly harmful non-commercial conduct may fall outside the offence. Conversely, a sexual motive is not always easy to prove. The formulation may therefore combine the objective sexual character of the representation with the intent to place the victim in a sexual context, with aggravation where the conduct is carried out for blackmail, commercial gain, mass dissemination, against a child, or by a person in a position of power.

The absence of consent should be positioned as a normative element, not merely as a ground for aggravation. Consent must be free, specific, informed, and directed to the relevant category of sexual representation. Consent to an ordinary

photograph does not amount to consent to the creation of synthetic sexual material; consent to one production likewise does not automatically extend to new manipulation or distribution. Consent may be withdrawn for future use, but withdrawal does not retroactively transform previously lawful conduct into a criminal offence; the prospective legal consequences for storage, distribution, or subsequent use must be clearly formulated. In relationships of power, courts must assess whether consent was genuinely free from pressure, threats, dependency, or abuse of position.

The legal framework should treat the use of a child's identity more strictly while still distinguishing the object and elements of the offence. A synthetic sexual representation that reasonably identifies a child creates protection risks different from disputes over adult consent. Under the proposed offence, a child's consent cannot justify synthetic sexual exploitation of the child's identity. Not every synthetic item depicting a child, however, automatically has a sexual character or satisfies the same offence elements; sexual character, identifiability, *mens rea*, and the relationship with the child-protection regime must still be examined. This distinction preserves a high level of protection without sacrificing legality.

The freedom-of-expression dimension requires a limited defence or exception tested through necessity and proportionality rather than profession or genre labels. Courts should assess the legitimacy of the public interest; the necessity of using a real person's identity; the relevance of the sexual element to the public purpose; the availability of less intrusive alternatives; the degree of identifiability; and the safeguards employed. Satire, art, journalism, education, security research, or law enforcement do not receive automatic immunity. Conversely, a representation genuinely necessary for the public interest, proportionately limited, and not intended to sexually exploit the target may fall outside the offence. This test leaves room for expression without opening an overly broad excuse.

Fragmentation also appears in the available remedies. Victim recovery should not depend on a final criminal judgment. A credible report may trigger parallel regulatory pathways of temporary restriction or removal and preservation, provided that verification, objection, and data-security procedures are available. Restitution, services, and victim protection remain within the Sexual Violence Crimes Law regime and other applicable recovery instruments. Anti-reupload measures, trusted flaggers, hashing, and retention rules are better designed as systemic duties of platform operators rather than elements of an offence committed by users. Under this division, criminal law addresses perpetrators who satisfy the offence elements, while platform governance reduces dissemination without waiting for a final judgment.²¹

Evidentiary problems should be anticipated through four distinct stages. Preservation ensures that files, metadata, logs, prompt history, account information, payment records, and cloud records are not lost. Authentication tests the integrity of the file, source, hash, acquisition time, and chain of custody. Attribution links the defendant to creation, procurement, threats, or distribution through accounts,

²¹ Julia Hörnle, "Fighting the Beast of Image-Based Sexual Abuse. Part 1—the Criminal Law and Platform Regulation," *International Journal of Law and Information Technology* 34 (2026): eaag006, <https://doi.org/10.1093/ijlit/eaag006>.

devices, transactions, communications, and post-event behavior. Identifiability establishes that the output reasonably refers to a particular victim. Indonesian scholarship on electronic evidence emphasizes the importance of handling procedures that preserve evidentiary integrity, so AI-detection tools should not be treated as the sole conclusive evidence.²²

Table 4. Digital-Evidence Framework

Evidentiary Stage	Primary Question	Examples of Evidence
Preservation	What must be secured immediately to prevent loss?	Original file, URL/content ID, metadata, server/account logs, prompt/model history, payment record.
Authentication	Is the evidentiary object intact and reliable?	Hash, chain of custody, source acquisition record, encoding/container data.
Attribution	Who created, commissioned, threatened, or distributed it?	Account linkage, device artefacts, messages, transactions, login/IP records, admissions.
Identifiability	Does the representation reasonably refer to a particular victim?	Face/voice comparison, tags, captions, context, social-circle recognition, prompt/source image.

This evidentiary construction also responds to the liar's dividend. As deepfake technology becomes more widely known, it becomes easier for a party disadvantaged by authentic digital evidence to claim that the evidence is false. Systematic reviews of the threat posed by deepfakes to the justice system warn that the issue concerns not only new crimes but also the integrity of evidence.²³ Indonesia therefore needs forensic protocols that explain chain of custody, examination of original sources, hashes, metadata, encoding characteristics, and the limitations of AI-detection tools. Probabilistic detectors should not be treated as "truth machines"; they should constitute only one component of the overall evidentiary inference.

Accordingly, disharmony in Indonesian law is both substantive and procedural. Substantively, no offence yet clearly identifies synthetic sexual impersonation as an attack on sexual autonomy. Procedurally, there is no integrated pathway connecting victim reporting, rapid takedown, preservation of evidence, forensic examination, and prosecution. Legal reform that merely increases criminal penalties without improving that pathway will produce symbolic rules that are difficult to implement.

Fragmentation also creates a problem of concurrence of offences. A single act may simultaneously involve unauthorized access, data processing, creation of synthetic sexual material, threats, and distribution. Prosecutors must distinguish concurrence that protects different legal interests from duplicative punishment for the same conduct. A consent-based deepfake offence can serve as the center for sexual exploitation of identity; illegal access or blackmail may still be charged where

²²Rizki Zakariya, Yogi Prastia, and Siti Ismaya, "Revitalisasi Pengaturan Penanganan Bukti Elektronik dalam Proses Perkara Pidana di Indonesia," *Legislatif* 3, no. 1 (2020): 134–150, <https://doi.org/10.20956/jl.v3i1.10211>.

²³Maria-Paz Sandoval, Maria de Almeida Vau, John Solaas, and Luano Rodrigues, "Threat of Deepfakes to the Criminal Justice System: A Systematic Review," *Crime Science* 13 (2024): 41, <https://doi.org/10.1186/s40163-024-00239-1>.

there is additional, independent conduct. Prosecutorial guidance should explain these relationships so that the choice of charges is not driven solely by the highest available penalty. Accurate legal characterization matters because it affects victims' rights, evidentiary regimes, restitution, access termination, and the legal narrative of what is actually wrongful about the conduct.

The cross-border dimension adds further complexity. Generative models, servers, payment accounts, victims, and perpetrators may be located in different jurisdictions. Indonesian law needs a jurisdictional basis that can operate when the victim is in Indonesia or the principal effects occur in Indonesia, without disregarding the Criminal Code's principles of criminal jurisdiction. Cooperation in digital investigations is important for preserving logs and identifying accounts because data may disappear long before mutual legal assistance is completed. Procedural design should therefore distinguish rapid preservation requests from requests for production of evidence that require a fuller legal basis. This limitation also protects due process: the need for speed must not become cross-border data access without proper authorization and oversight.

Victims' procedural rights should be formulated as part of the criminal-law response rather than as an ancillary service. Victims should have access to a reporting channel that does not require repeated resubmission of the content, information on preservation and takedown, identity protection, and the opportunity to obtain restitution for recovery costs. Officials receiving reports should also prevent secondary victimization. Questions blaming victims for uploading photographs, maintaining social-media accounts, or previously creating lawful intimate material are irrelevant to the absence of consent for a new deepfake. Scholarship on image-based sexual abuse shows that focusing on consent and harm helps avoid unduly narrow legal categories and strengthens recognition of victims' experiences.²⁴

Reconstructing a Consent-Based Offence and an Integrated Enforcement Model

The proposed reconstruction places either a new offence or an explicit extension of Article 14 of the Sexual Violence Crimes Law as the principal option. Conceptually, the core formulation could provide that any person who intentionally creates, manipulates, generates, or commissions the creation of a visual, audiovisual, or voice representation of a sexual nature that reasonably depicts or resembles a particular person, without that person's consent, commits an offence where the conduct is carried out for a sexual purpose, serious humiliation, intimidation, exploitation, or with knowledge of a real risk of harm to the victim's dignity and sexual autonomy. This formulation separates creation from distribution and places consent at the center.

The element "reasonably depicts or resembles" functions as the identifiability test. The standard need not require recognition by the public at large. It is sufficient if a relevant group can connect the representation to the victim on the basis of the face, name, voice, tattoos, uniform, social-media account, or a combination of

²⁴ Carlotta Rigotti, Clare McGlynn, and Franziska Benning, "Image-Based Sexual Abuse and EU Law: A Critical Analysis," *German Law Journal* 25, no. 9 (2024): 1472–1493, <https://doi.org/10.1017/glj.2024.49>.

characteristics. This test addresses minor technical modifications deliberately made to evade responsibility while preventing the criminalization of fictional characters not intended to represent any particular person. In practice, courts may assess the context of the upload, captions, tags, prompts, and the perpetrator's communications as indicators of an intent to identify.

Consent should be defined as free, specific, informed, and demonstrable consent to the creation or use of a synthetic sexual representation. The absence of protest after content is created must not be treated as consent. Consent to a source photograph is likewise insufficient. Where the defendant relies on consent, the principal burden remains on the prosecution to prove the elements of the offence, but the defendant may be required to identify a reasonable factual basis for the consent claim once the prosecution has shown circumstances that objectively indicate non-consensual creation. This model preserves the presumption of innocence without imposing an unrealistic burden on victims to prove a negative.

The level of fault should be differentiated among primary perpetrators, distributors, and platforms. A deepfake creator who intentionally targets a victim is a primary perpetrator. A person who receives and then redistributes material may be liable if they know or ought to realize that it is a non-consensual sexual representation and nevertheless distribute it. Platforms, however, should not automatically be criminally liable merely because their systems are used. Corporate criminal liability should follow the Criminal Code's principles on corporate offences, including the connection to corporate activities, benefit, policy, failure of prevention, or culpable omission. This approach is more consistent than strict platform liability.

Criminal aggravation should be based on harm and abuse of power. Aggravating factors include a child victim or a victim with disabilities; a family, educational, employment, professional, or other power relationship between the perpetrator and victim; mass distribution; use of the content for blackmail or financial gain; repeat offending; or conduct causing exceptionally serious harm. Conversely, the maximum penalty need not apply to every case. The system can provide a sentencing range allowing judges to consider the scale of distribution, removal efforts, remorse, restitution, and the risk of repetition.

Non-custodial sanctions should play an important role. Sexual deepfakes often require digital remediation more than imprisonment alone. Courts should be able to order removal of the material, surrender or destruction of copies, no-contact orders, prohibitions on using the victim's identity, confiscation of profits, restitution, and certain rehabilitation obligations. For corporate offenders, sanctions may include improvements to moderation systems, audits, turnover-based fines where relevant, and publication of the judgment. The aim is to remove incentives and reduce the possibility of reproducing the harm.

Procedurally, a victim's report should trigger two parallel pathways: preservation and removal. Preservation means that the electronic-system operator retains a limited copy, metadata, access logs, and account information for evidentiary purposes under strict safeguards. Removal means that public access to the content is promptly suspended after adequate initial verification. These two pathways prevent a dilemma between protecting the victim and preserving evidence. If only removal occurs, evidence may be lost; if only preservation occurs, the content continues to circulate. The mechanism should also regulate retention

periods and access so that victim material is not unnecessarily replicated by authorities or third parties.

Platform regulation may use trusted-flagger systems for reports of sexual deepfakes, fingerprinting of verified material, and bans on monetization. Automated algorithms, however, must not be the sole decision-maker because they may wrongly remove educational, journalistic, or artistic content. Permanent-removal decisions should include an objection mechanism, while victims should have access to a rapid escalation pathway. Recent scholarship on image-based sexual abuse regards the integration of criminal law and platform obligations as necessary because the scale and cross-border nature of distribution cannot be addressed by individual prosecution alone.²⁵

To protect freedom of expression, the offence should include a defence or limited exception for activities genuinely serving the public interest, security research, law enforcement, or artistic work where use of a real person's sexual identity is necessary and proportionate. The exception should not apply where the dominant purpose is humiliation, sexual gratification, harassment, or commercial exploitation lacking a reasonable connection to the public interest. This assessment is consistent with the need to balance rights and to prevent deepfake regulation from becoming general censorship of synthetic content.²⁶

Prevention also requires design obligations for providers of generative technology. Model providers that expressly offer "nudify" functions, sexual face swaps, or services specifically optimized to produce pornography involving real people occupy a different position from general-purpose models. The law may require reasonable safeguards, including prohibitions on using children's identities, reporting mechanisms, proportionate logging, watermarks or provenance signals where technically feasible, and suspension of accounts proven to misuse the service. Failure to implement safeguards does not automatically constitute a criminal offence, but it may be evidence of organizational fault where a corporation knowingly allows the model to be used for crimes that form part of its business model.

The reconstruction must not disregard the relationship with the PDP Law. Facial and biometric data may serve as source material for generating a deepfake, so data violations may still be charged cumulatively when their elements are satisfied. The sexual-deepfake offence, however, should stand independently so that protection does not depend on whether the source photograph was lawfully obtained. Under this design, a person who lawfully uses a public photograph but then turns it into non-consensual synthetic pornography may still be held responsible for the attack on sexual autonomy, rather than having the conduct forced into the category of unlawful data acquisition.

The relationship with the ITE Law and the Pornography Law should also be clarified through concordance rules. Where the principal conduct is a non-

²⁵ Julia Hörnle, "Fighting the Beast of Image-Based Sexual Abuse. Part 1—the Criminal Law and Platform Regulation," *International Journal of Law and Information Technology* 34 (2026): eaag006, <https://doi.org/10.1093/ijlit/eaag006>.

²⁶ Dominika Kuźnicka-Błaszczowska and Nadiya Kostyuk, "Emerging Need to Regulate Deepfakes in International Law: The Russo–Ukrainian War as an Example," *Journal of Cybersecurity* 11, no. 1 (2025): tyaf008, <https://doi.org/10.1093/cybsec/tyaf008>.

consensual sexual representation directed at a particular victim, the Sexual Violence Crimes Law should provide the principal offence. The ITE Law may apply to distribution that contains additional elements, and the Pornography Law may apply where the protected legal interest and conduct elements are genuinely different. Prosecutorial guidance should prevent disproportionate cumulative sanctions for the same conduct. The objective is not to multiply charges, but to ensure that each dimension of harm has an appropriate legal basis.

Finally, reform should be accompanied by digital-evidence guidance. Investigators should document the file source, hash, acquisition time, originating account, URL or content identifier, metadata, and forensic process. Experts should explain the probability and limitations of detection rather than merely declare that material is or is not a "deepfake." In some cases, technically proving that content is synthetic is not difficult because the perpetrator admits the generation process; the principal issues are attribution and consent. Excessive focus on detection may distract from communication evidence, motive, power relationships, and conduct after the victim requests removal.

The proposed model consists of four layers with different normative statuses and institutional responsibilities. The first layer is the core offence and aggravating factors, which require legislative action and are applied through investigators, public prosecutors, and courts. The second layer comprises removal, preservation, and anti-reupload measures within the governance of electronic-system operators, reporting mechanisms, and lawful regulatory or enforcement authority. The third layer consists of restitution, identity protection, assistance, and victim recovery through the Sexual Violence Crimes Law regime and competent institutions. The fourth layer comprises digital-evidence and forensic standards that must operate through procedural law, investigative standard operating procedures, and expert examination. This division of authority prevents every solution from being treated as a new form of criminalization.

Within this framework, the phrase intentional sexual appropriation of identity is used only as a theoretical shorthand, not as an independent element of the offence. Every application must always be reduced to four measurable elements: the representation is sexual in nature; the victim can reasonably be identified; specific consent is absent; and the perpetrator possesses the required mens rea. Threat, coercion, distribution, monetization, and repeat dissemination are then assessed as additional conduct or aggravating factors. In this way, the theoretical concept does not become an elastic umbrella extending beyond the principle of legality.

To provide legal certainty, the *de lege ferenda* model can be formulated through layered elements. Objective elements: the perpetrator creates, manipulates, or commissions the creation of a visual, audiovisual, or voice representation of a sexual nature; the representation reasonably identifies or is intended to identify a particular person; and no valid specific consent exists. Subjective elements: the perpetrator knows that the target is a particular person and knows that such consent is absent. The formulation need not use the elastic phrase "serious humiliation" as an independent element; sexual purpose, coercion or intimidation, or commercial exploitation can serve as more measurable indicators or aggravating factors. Actual harm, distribution, monetization, abuse of power, child victims, and

repetition are placed at the aggravation stage rather than replacing the elements of the core offence.

The responsibility of AI service providers should be distinguished from the responsibility of content creators or distributors. Platforms or model providers are not criminally liable merely because their technology can be misused in general. Corporate criminal liability becomes relevant only when the Criminal Code's requirements for corporate attribution are satisfied, for example where the conduct occurs within corporate activities, provides an unlawful benefit, stems from policy, or reflects a culpable failure or omission. Recent Indonesian scholarship on deepfake platforms likewise emphasizes the need for clear boundaries between digital intermediaries and principal perpetrators. Reporting duties, preservation, risk controls, and other safeguards should first be placed within the regulatory regime for electronic-system operators; breach of a regulatory duty does not automatically become a criminal offence without a clear statutory basis.²⁷

For children in particular, protection should cover synthetic sexualization even where no child's body was actually recorded. The focus is the use of a child's identity in a sexual representation and the accompanying risk of exploitation. The relationship with the child-protection regime, however, must be tested element by element: whether the content is sexual, whether the child is identifiable, who created or circulated it, and whether there is additional conduct such as grooming, blackmail, or trafficking. Evidence should be handled through restricted access, hashing, and prohibitions on unnecessary reproduction so that enforcement itself does not create new circulation.

The reconstruction should also be accompanied by a rule of evidence that prevents the fetishization of forensic technology. Expert detection can assist, but the probability that a file was generated by AI is not the only question. Contextual evidence such as conversations, prompts, source images, accounts, transactions, and conduct after creation may be more powerful in linking the defendant to the act. Sandoval and colleagues show that deepfakes create serious challenges for evidentiary integrity and trust in the criminal justice system. The appropriate response is not to treat all digital media as suspicious, but to build chain of custody, authentication, disclosure of forensic methods, and an opportunity for the opposing party to test the reliability of the analysis.²⁸

CONCLUSION

Non-consensual sexual deepfakes reveal a partial gap in Indonesian criminal law, not an absence of all legal instruments. Current positive law can reach several forms of conduct: the ITE Law in relation to certain forms of electronic distribution or access; the Pornography Law in relation to the production or provision of material satisfying its elements; the PDP Law in relation to unlawful data processing; and the Sexual Violence Crimes Law in relation to forms of electronic-

²⁷Habil Huda Alghiffary, Mohamad Rapik, and Dheny Wahyudhi, "Dalam Pusaran Deepfake Pornografi: Menakar Pertanggungjawaban Pidana Platform Digital," *PAMPAS: Journal of Criminal Law* 7, no. 1 (2026), <https://doi.org/10.22437/pampas.v7i1.53737>.

²⁸ Maria-Paz Sandoval, Maria de Almeida Vau, John Solaas, and Luano Rodrigues, "Threat of Deepfakes to the Criminal Justice System: A Systematic Review," *Crime Science* 13 (2024): 41, <https://doi.org/10.1186/s40163-024-00239-1>.

based sexual violence consistent with the verbs used in Article 14. Initial synthetic creation of a sexual representation of an identifiable person, however, has not been expressly formulated and should not be covered through an analogy that expands the offence. Indonesian scholarship itself increasingly identifies this gap as a regulatory problem requiring measured reform.

De lege ferenda, the more coherent option is to expressly extend the Sexual Violence Crimes Law regime or create a specific offence centered on sexual autonomy. The core offence should require sexual character, identifiability, intent, and the absence of specific consent; threat/coercion, distribution, monetization, repeat dissemination, abuse of power, child victims, and actual harm should be treated as additional conduct or aggravating factors. Public-interest exceptions should not be based on professional or genre labels, but on necessity and proportionality. This tiered structure preserves *lex certa* while avoiding overcriminalization.

The effectiveness of the response also depends on a clear division among criminal law, victim recovery, platform governance, and digital evidence. Rapid removal should operate alongside preservation; anti-reupload and trusted reporting may be built as systemic duties that are not automatically criminal in nature; and evidentiary practice should distinguish preservation, authentication, attribution, and identifiability. This study has limitations: it does not examine the number of sexual-deepfake cases in Indonesia, enforcement practice under Article 14 of the Sexual Violence Crimes Law, forensic-laboratory capacity, platform responses, or empirical effects on victims. The proposed model is therefore a normative construction that still requires empirical research, consultation with victims, law-enforcement authorities, platforms, forensic experts, and regulatory-impact assessment before being adopted as policy.

REFERENCES

- Alghiffary, Habil Huda, Mohamad Rapik, and Dheny Wahyudhi. "Dalam Pusaran Deepfake Pornografi: Menakar Pertanggungjawaban Pidana Platform Digital." *PAMPAS: Journal of Criminal Law* 7, no. 1 (2026). <https://doi.org/10.22437/pampas.v7i1.53737>.
- Flynn, Asher, Anastasia Powell, Adrian J. Scott, and Elena Cama. "Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging Form of Image-Based Sexual Abuse." *The British Journal of Criminology* 62, no. 6 (2022): 1341–1358. <https://doi.org/10.1093/bjc/azab111>.
- Faturrachman SY., Muhammad. "Deepfake Pornografi: Studi Konstitusi dan Penegakannya di Indonesia." *Legislatif* 8, no. 2 (2025): 113–128. <https://doi.org/10.20956/jl.v8i2.44186>.
- Gotora, Ngonidzaishe T. "Unmasking Deception: Deepfake Regulation in the Context of South African Law, Could a Rethinking of Performers' Protection Rights Be the Answer?" *International Journal of Law and Information Technology* 32 (2024): eaae026. <https://doi.org/10.1093/ijlit/eaae026>.
- Hidayah, Siti Nur, and Gunawan Hadi Purwanto. "Legal Protection of Victims of AI-Driven Deepfake Pornography: An Analysis within Indonesian Law." *Al-Risalah*

- Jurnal Ilmu Syariah dan Hukum 26, no. 1 (2026): 917–935. <https://doi.org/10.24252/al-risalah.vi.63687>.
- Hörnle, Julia. “Fighting the Beast of Image-Based Sexual Abuse. Part 1—the Criminal Law and Platform Regulation.” *International Journal of Law and Information Technology* 34 (2026): eaag006. <https://doi.org/10.1093/ijlit/eaag006>.
- Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Indonesia. Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi.
- Indonesia. Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual.
- Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Indonesia. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
- Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Indonesia. Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana.
- Isnawan, Fuadi. “Deepfake Pornography: How Criminal Liability of Perpetrators in the Indonesian Criminal Law Framework.” *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 13, no. 3 (2024): 745–771. <https://doi.org/10.24843/JMHU.2024.v13.i03.p15>.
- Kuźnicka-Błaszowska, Dominika, and Nadiya Kostyuk. “Emerging Need to Regulate Deepfakes in International Law: The Russo–Ukrainian War as an Example.” *Journal of Cybersecurity* 11, no. 1 (2025): tyaf008. <https://doi.org/10.1093/cybsec/tyaf008>.
- Maskun, Nur Azisa, Muhammad Mutawalli Mukhlis, M. Aris Munandar, and Arnita Pratiwi Arifin. “Additional Criminal Revocation of Access to Online Communication Devices for Perpetrators of Electronic-Based Sexual Violence.” *Indonesian Journal of Criminal Law Studies* 10, no. 2 (2025): 451–486. <https://doi.org/10.15294/ijcls.v10i2.23100>.
- McGlynn, Clare, and Carlotta Rigotti. “From Virtual Rape to Meta-rape: Sexual Violence, Criminal Law and the Metaverse.” *Oxford Journal of Legal Studies* 45, no. 3 (2025): 554–582. <https://doi.org/10.1093/ojls/gqaf009>.
- Nitha, Fitha Ayun Lutvia, Ali Masyhar, Achmad Cholidin, M. Ridho Ilahi, and Amalina Zukhrufatul Bahriyah. “Optimalisasi Implementasi UU TPKS: Tantangan dan Solusi dalam Upaya Penghapusan Kekerasan Seksual di Indonesia.” *Masalah-Masalah Hukum* 53, no. 1 (2024): 90–100. <https://doi.org/10.14710/mmh.53.1.2024.90-100>.
- Putra, Komang Bagus Wicaksana, and Gusti Ayu Arya Prima Dewi. “Urgensi Pengaturan Tindak Pidana Deepfake Pornografi di Indonesia.” *Kertha Wicara*:

- Journal Ilmu Hukum 13, no. 10 (2024): 530–541. <https://doi.org/10.24843/KW.2024.v13.i10.p5>.
- Ramiyanto. “Bukti Elektronik sebagai Alat Bukti yang Sah dalam Hukum Acara Pidana.” *Jurnal Hukum dan Peradilan* 6, no. 3 (2017): 463–484. <https://doi.org/10.25216/jhp.6.3.2017.463-484>.
- Rigotti, Carlotta, Clare McGlynn, and Franziska Benning. “Image-Based Sexual Abuse and EU Law: A Critical Analysis.” *German Law Journal* 25, no. 9 (2024): 1472–1493. <https://doi.org/10.1017/glj.2024.49>.
- Sandoval, Maria-Paz, Maria de Almeida Vau, John Solaas, and Luano Rodrigues. “Threat of Deepfakes to the Criminal Justice System: A Systematic Review.” *Crime Science* 13 (2024): 41. <https://doi.org/10.1186/s40163-024-00239-1>.
- Sirait, Kevin David, Arman Saut Rivando, Cecilia Angel, Zico Ricardo Aritonang, and Lenny Maria Aritonang. “Pertanggungjawaban Pidana atas Deepfake AI dalam Produksi dan Distribusi Pornografi Digital di Indonesia.” *Jurnal Hukum Lex Generalis* 7, no. 7 (2026). <https://doi.org/10.56370/jhlg.v7i7.3458>.
- Mahkamah Konstitusi Republik Indonesia. Putusan Nomor 20/PUU-XIV/2016.
- Zakariya, Rizki, Yogi Prastia, and Siti Ismaya. “Revitalisasi Pengaturan Penanganan Bukti Elektronik dalam Proses Perkara Pidana di Indonesia.” *Legislatif* 3, no. 1 (2020): 134–150. <https://doi.org/10.20956/jl.v3i1.10211>.