

A Juridical Analysis of Non-Consensual Sexual Deepfakes From the Perspective of Cyber-Enabled Sexual Violence

Azzahra Sifa Anarki¹, Joko Setiyono²

¹Student Master of Law Program, Diponegoro University, Semarang

²Lecturer Master of Law Program, Diponegoro University, Semarang

ABSTRACT: Generative artificial intelligence has enabled the creation of realistic synthetic sexual content that places an identifiable person in a sexual setting without consent. This article examines non-consensual sexual deepfakes under Article 14(1)(a) and (b) of Law No. 12 of 2022 on Sexual Violence Crimes and Article 27(1) in conjunction with Article 45(1) of Law No. 1 of 2024 on Electronic Information and Transactions. It also assesses whether the conduct may qualify as cyber-enabled sexual violence under Article 7(1)(g) of the Rome Statute. The study applies normative legal research through statutory, conceptual, and limited comparative approaches. Indonesian criminal law can address transmission, distribution, and public accessibility, but it does not expressly criminalize the production of non-consensual synthetic sexual content as an autonomous offense. Article 7(1)(g) may encompass such conduct only when its sexual character, absence of consent or coercive circumstances, comparable gravity, mental element, and nexus to a widespread or systematic attack against a civilian population are established. A precise statutory response is required to protect sexual autonomy and digital identity without displacing the principle of legality.

KEYWORDS: sexual deepfakes; synthetic sexual content; electronic-based sexual violence; cyber-enabled sexual violence; Rome Statute.

INTRODUCTION

Generative artificial intelligence has transformed electronic-based sexual violence from the recording or circulation of intimate material into the fabrication of synthetic sexual representations. Deepfake systems can combine an identifiable face, body, or voice with a sexual image or video that never occurred. The resulting harm exceeds the circulation of indecent material because the technology appropriates the victim's identity, assigns a fictitious sexual act to that person, and deprives the victim of control over a digitally embodied representation. Non-consensual sexual deepfakes therefore shift the protected legal interest from the secrecy of an authentic intimate recording to sexual autonomy, dignity, psychological integrity, and digital identity.

Indonesian criminal law contains two principal statutory routes. Article 14(1)(a) and (b) of Law No. 12 of 2022 on Sexual Violence Crimes (the TPKS Law) regulates non-consensual recording, image capture, and transmission of sexual content. Article 27(1) in conjunction with Article 45(1) of Law No. 1 of 2024 amending the Electronic Information and Transactions Law (the ITE Law) prohibits broadcasting, displaying, distributing, transmitting, or otherwise making electronic information with content violating public decency accessible. Both regimes recognize digital sexual harm, yet their operative verbs primarily address capture and circulation rather than the fabrication of sexual content from non-sexual source data.

Existing Indonesian scholarship has examined deepfake misuse through privacy, personal data protectio, defamation, pornography, victimology, and the perceived absence of a specific offense (Kusnadi dan Putri, 2025; Oktallia dan Ariana, 2022; Sijabat dan Lukitasari, 2024; Aurelita dan Lewoleba, 2024). Those studies commonly distinguish the distribution-oriented character of the ITE Law from the victim-protection orientation of the TPKS Law (Padmasari dan Subekti, 2024). The unresolved doctrinal issue concerns the legal meaning of production itself: whether the deliberate construction of a false sexual representation should be treated merely as indecent electronic content or as technology-facilitated sexual violence that directly violates consent and sexual autonomy before any dissemination occurs.

International criminal law provides a limited analytical perspective because crimes within the Rome Statute may be committed, facilitated, or aggravated through cyber means (Cherif, 2013). Article 7(1)(g) includes rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization, and any other form of sexual violence of comparable gravity (International Criminal Court, 1998). The open-ended final category permits an assessment of emerging conduct without removing the threshold of seriousness or the contextual requirements of crimes against humanity (Gerhard dan Florian, 2020). Sexual deepfakes must

A Juridical Analysis of Non-Consensual Sexual Deepfakes From the Perspective of Cyber-Enabled Sexual Violence

consequently be tested as a possible mode of sexual violence rather than assumed to constitute an international crime because they use artificial intelligence.

Indonesia is not a State Party to the Rome Statute, and the Statute does not operate as directly applicable domestic criminal law. The concept of cyber-enabled sexual violence is used here as a doctrinal and limited comparative lens for evaluating the adequacy of national law. The analysis addresses two questions: the extent to which the TPKS Law and the ITE Law cover the production and circulation of non-consensual sexual deepfakes, and the conditions under which such conduct could fall within the residual category of sexual violence in Article 7(1)(g).

RESEARCH METHODOLOGY

This study employs normative legal research using statutory, conceptual, and limited comparative approaches (Marzuki, 2017). The statutory analysis focuses on Article 14(1)(a) and (b) of the TPKS Law and Article 27(1) in conjunction with Article 45(1) of the ITE Law. The conceptual approach examines consent, sexual autonomy, dignity, psychological integrity, digital identity, and the distinction between authentic intimate material and synthetic sexual representation. The limited comparative approach uses Article 7(1)(g), Article 7(2)(a), Article 22, and the relevant Elements of Crimes, together with the ICC Office of the Prosecutor's policy on cyber-enabled crimes. Primary, secondary, and tertiary legal materials are analyzed qualitatively and prescriptively through grammatical, systematic, and teleological interpretation, subject to the prohibition of analogy to the detriment of the accused (Moeljatno, 2008).

RESULTS AND DISCUSSION

Regulation of the Production of Non-Consensual Deepfake Synthetic Sexual Content under Indonesian Criminal Law

Indonesian criminal law addresses non-consensual sexual deepfakes through the TPKS Law and the ITE Law. Neither statute expressly refers to deepfakes, synthetic media, or generative artificial intelligence. Their relevance depends on whether the factual conduct falls within existing verbs such as recording, capturing, transmitting, distributing, broadcasting, displaying, or making content accessible. The legal inquiry must therefore separate production, direct transmission, and public dissemination because each stage engages a different statutory element and a different protected interest.

Article 14(1) of the TPKS Law defines forms of electronic-based sexual violence. Letter (a) concerns the recording, capture, or screenshot of sexually charged material without the knowledge or consent of the person who is the object of that material. Letter (b) concerns the transmission of electronic information or documents containing sexual material against the recipient's wishes. The placement of these acts within a sexual-violence statute directs interpretation toward consent, dignity, and sexual autonomy rather than public morality alone. The offense is generally complaint-based, subject to statutory exceptions involving children and persons with disabilities.

Article 14(1)(a) is relevant because a sexual deepfake uses an identifiable person as the object of a sexual representation without authorization. The textual difficulty lies in the terms recording, image capture, and screenshot. Those terms ordinarily presuppose the visual capture of an existing object or event, while a deepfake may begin with an ordinary photograph and generate sexual content through computational manipulation. The sexual element is created during synthesis rather than captured from an actual sexual occurrence.

A strict reading of Article 14(1)(a) does not readily equate the capture of an image with the production of a new synthetic image. Criminal liability cannot be created by extending the statutory verb through an analogy unfavorable to the accused (Moeljatno, 2008). A teleological reading may show that the conduct contradicts the protective purpose of the TPKS Law, but legislative purpose cannot replace a missing *actus reus*. The provision can therefore support the characterization of harm while remaining an uncertain basis for punishing production alone.

Article 14(1)(b) more clearly applies after a sexual deepfake has been transmitted. The provision does not require an authentic sexual recording; it requires electronic information or a document containing sexual material that is transmitted contrary to the recipient's wishes. Sending a deepfake to the depicted person, an employer, relatives, or another targeted recipient for humiliation, intimidation, extortion, or sexual control may satisfy this structure. Production without transmission remains outside the provision even though the appropriation of identity and the risk of future circulation already affect the victim.

Article 27(1) of the ITE Law covers a wider range of dissemination conduct by prohibiting the intentional and unauthorized broadcasting, displaying, distributing, transmitting, or making accessible of electronic information or documents that violate public decency. Article 45(1) supplies the criminal sanction (Wahid dan Labib, 2005). A sexual deepfake uploaded to a social-media account, website, group, forum, or file-sharing service can fall within these verbs when it becomes available to the public or a relevant audience. The provision is operationally stronger at the distribution stage than at the stage of private creation.

The ITE Law centers the unlawfulness inquiry on indecent electronic content and its circulation. That structure does not expressly require proof that the depicted person withheld consent to the sexual representation (Noerman dan Ibrahim, 2024). A prosecution framed only through public decency may obscure the principal injury: the attribution of a fictitious sexual act to an identifiable person and the resulting loss of control over that person's digital embodiment. The content may be harmful even when

the audience understands that it is fabricated because the forced sexualization itself can produce stigma, fear, and exclusion (Noviantama dan Rahman, 2025).

The two statutory regimes operate cumulatively at different stages. The TPKS Law more directly captures the consent-based and victim-centered character of the harm, especially when content is transmitted against a person's wishes. The ITE Law provides broader verbs for public circulation and accessibility. The applicable provision must be selected according to the proven act rather than treating the statutes as interchangeable labels for the same conduct.

The production stage remains the central normative gap. Article 14(1)(a) refers to obtaining or capturing sexual material, Article 14(1)(b) concerns transmission, and Article 27(1) concerns circulation or accessibility. None expressly prohibits the deliberate generation of synthetic sexual content through the unauthorized use of another person's identifiable image, voice, or biometric characteristics (Sompotan et al, 2026). The gap is material because the victim's identity is sexually appropriated at the moment of fabrication, independently of any later publication.

The distinction between consent and public decency also affects the object of legal protection. The TPKS Law treats the absence of consent as a defining feature of sexual violence, while the ITE Law evaluates the nature and dissemination of the content (Kusnadi dan Putri, 2025). Sexual deepfakes expose the limits of a morality-centered model because the core wrong is not merely that the material is explicit. The wrong lies in constructing a sexual persona for a real person who never performed, authorized, or controlled the represented act.

The current framework reaches non-consensual sexual deepfakes only in part. Transmission to a victim or another recipient can be addressed under Article 14(1)(b), and public circulation can be addressed under Article 27(1) in conjunction with Article 45(1). Article 14(1)(a) may apply only where the proven conduct genuinely falls within recording, image capture, or screenshot, not where liability depends on redefining those terms as synthetic production. An express offense directed at intentional non-consensual sexual synthesis would provide greater certainty while preserving the legality principle.

Qualification of Non-Consensual Deepfake Synthetic Sexual Content as Cyber-Enabled Sexual Violence under Article 7(1)(g) of the Rome Statute

Article 7(1)(g) must be applied within the legal framework of crimes against humanity. Sexual harm does not become an international crime solely because it is severe, digitally mediated, or directed at an identifiable victim. The conduct must form part of a widespread or systematic attack directed against a civilian population, and the accused must know that the conduct is connected to that attack (Cassese,2008). An isolated revenge act or personal harassment ordinarily remains within domestic criminal law.

The provision lists several specific sexual crimes and ends with any other form of sexual violence of comparable gravity (Ambos, 2013). The residual category can accommodate conduct that differs in method from the enumerated offenses, but it cannot dispense with sexual character and comparable seriousness. The relevant question is whether forcing an identifiable person into a fabricated sexual representation can constitute a sexual act against that person in the legal sense, not whether a deepfake is factually identical to rape or another listed offense.

The Elements of Crimes describes other sexual violence through conduct of a sexual nature committed against one or more persons, or conduct that causes such persons to engage in an act of a sexual nature, through force, threat, coercion, detention, psychological oppression, abuse of power, a coercive environment, or an inability to give genuine consent (International Criminal Court, 2011). The formulation does not make physical contact the sole determinant. Sexual nature, coercive circumstances, the victim's inability or lack of genuine consent, and gravity remain decisive.

The concept of cyber-enabled sexual violence identifies the digital means by which a recognized offense may be committed, facilitated, scaled, concealed, or aggravated. It does not create an autonomous crime under the Rome Statute (Office of the Prosecutor, 2025). Generative artificial intelligence, automated image manipulation, anonymous accounts, and networked distribution may serve as instruments of sexual violence when the underlying material and contextual elements are independently established.

A structured normative test distinguishes serious domestic cyber abuse from an underlying act of a crime against humanity by examining attack context, sexual character, consent or coercion, comparable gravity, cyber means, mens rea, and the protected legal interest.

Normative Layer	Normative Basis	Element	Deepfake Relevance	Indicators	Limit
Attack threshold	Arts. 7(1), 7(2)(a)	Widespread or systematic attack on civilians; knowledge	Only as part of a wider attack on civilians	Pattern; targeted group; intimidation; State or group policy	Isolated acts remain domestic
Sexual act	Art. 7(1)(g)	Other sexual violence of comparable gravity	Forced sexual depiction of a real person	Known identity; sexual scene; false sexual attribution	Non-sexual edits are excluded

A Juridical Analysis of Non-Consensual Sexual Deepfakes From the Perspective of Cyber-Enabled Sexual Violence

Normative Layer	Normative Basis	Element	Deepfake Relevance	Indicators	Limit
Consent or coercion	Elements, Art. 7(1)(g)-6	Force, threat, coercion, power abuse, coercive setting, or incapacity	Sexual use of identity without permission	No consent; threats; extortion; control; power gap	Non-consent must be proved
Gravity	Art. 7(1)(g); Elements	Seriousness comparable to listed sexual crimes	Serious harm to dignity, mind, safety, or sexual autonomy	Scale; persistence; trauma; stigma; threats; exclusion	Minor harm is insufficient
Cyber means	ICC Cyber Policy	Cyber means commit, aid, scale, hide, or worsen a Statute crime	AI is a means, not a new offense	AI; automation; anonymity; broad reach; mass copying	No liability beyond the Statute
Mental element	Arts. 7(1), 30	Intent and knowledge of the conduct and attack	Knowledge of creation alone is insufficient	Intent; victim awareness; knowledge of the wider attack	Attack knowledge is required
Protected interests	Art. 7(1)(g)	Dignity; sexual autonomy; bodily integrity; security	Digital harm causes real mental and social injury	Loss of control; forced sexual image; trauma; stigma; exclusion	Morality or falsity alone is insufficient

Source: Compiled by the Author (2026)

The matrix establishes that sexual content and digital technology are necessary but insufficient conditions. International qualification requires a cumulative analysis of the conduct's sexual nature, the victim's lack of genuine consent or the existence of coercive circumstances, the seriousness of the injury, the accused's mental element, and the nexus with a widespread or systematic attack against a civilian population (Bassiouni, 2013). The term cyber-enabled describes the means of commission and does not enlarge the Court's subject-matter jurisdiction.

The sexual nature of a deepfake arises from the deliberate placement of an identifiable person within a fabricated sexual scene or act. The victim is made to appear sexually exposed, participating, or available despite never performing or authorizing the represented conduct. The false character of the image does not neutralize the sexual attribution. The relevant injury is the compelled association between the victim's identity and a sexual act imposed by the perpetrator.

The absence of consent begins at production because the perpetrator uses the victim's face, body, voice, or other identifying features to construct a sexual persona without authorization. Consent to an ordinary photograph, public appearance, or online profile does not amount to consent to synthetic sexualization. Coercive circumstances become especially visible when the material is used for blackmail, threats, silencing, forced compliance, reputational destruction, or the exploitation of an existing power imbalance (Noviantama dan Rahman, 2025).

Comparable gravity requires more than offensiveness or embarrassment. Relevant factors include the scale and duration of circulation, the explicitness and degrading character of the representation, the victim's psychological injury, exposure to threats or physical danger, social stigma, economic loss, forced withdrawal from public life, and the practical permanence created by repeated copying. A limited private fabrication may constitute a serious domestic offense without reaching the gravity required by Article 7(1)(g).

The contextual element separates domestic criminality from crimes against humanity. A deepfake campaign may acquire international relevance when it targets a civilian group, forms part of a repeated or organized course of conduct, and serves intimidation, persecution, collective humiliation, displacement, or political silencing (Office of the Prosecutor, 2022). Women, journalists, activists, human-rights defenders, and members of minority groups may be targeted through sexual stigma, but membership in a vulnerable group alone does not prove the required attack or organizational policy.

The cyber-enabled character can intensify the underlying harm through speed, automation, anonymity, cross-platform dissemination, global reach, and persistent reproduction. Removal of an initial upload does not end the injury when copies remain searchable or are repeatedly recirculated. Those technological features may support the assessment of gravity and contribution to an attack, yet they cannot substitute for proof of sexual violence or the contextual elements of Article 7.

Article 22 of the Rome Statute requires strict construction and prohibits extending criminal definitions by analogy (International Criminal Court, 1998). Non-consensual sexual deepfakes cannot be inserted automatically into Article 7(1)(g) merely because the residual phrase is open-ended. The prosecution would need to establish that the proven conduct itself constitutes another form of sexual violence of comparable gravity and that every contextual and mental element is satisfied. The accused must also know the factual circumstances linking the conduct to the broader attack.

The cumulative assessment permits a limited and conditional qualification. Sexual deepfakes may function as cyber-enabled sexual violence when they impose a sexual representation without genuine consent, operate through coercion or an equivalent circumstance recognized by the Elements of Crimes, cause harm of comparable gravity, and contribute to a widespread or systematic attack against civilians with the required knowledge. Failure to establish any of those elements leaves the conduct outside crimes against humanity even though it may remain punishable and gravely harmful under national law.

A Juridical Analysis of Non-Consensual Sexual Deepfakes From the Perspective of Cyber-Enabled Sexual Violence

Article 7(1)(g) supplies a doctrinal framework for recognizing that sexual violence need not be confined to physical penetration or direct bodily contact. Digital fabrication can attack sexual autonomy and human dignity by appropriating an identifiable person's embodied identity and imposing a fictitious sexual act. The framework remains bounded by comparable gravity, attack context, mens rea, and legality, ensuring that technological novelty does not produce an uncontrolled expansion of international criminal liability.

CONCLUSION

Indonesian criminal law regulates non-consensual sexual deepfakes only partially. Article 14(1)(b) of the TPKS Law can address transmission against a recipient's wishes, while Article 27(1) in conjunction with Article 45(1) of the ITE Law can address broadcasting, distribution, transmission, display, and public accessibility of indecent electronic content. Article 14(1)(a) should not be extended by analogy from recording or image capture to synthetic production. The deliberate fabrication of sexual content from another person's identifiable features therefore remains insufficiently defined as an autonomous offense. Article 7(1)(g) of the Rome Statute may characterize such conduct as cyber-enabled sexual violence only when sexual nature, lack of genuine consent or coercive circumstances, comparable gravity, the required mental element, and a nexus to a widespread or systematic attack against a civilian population are cumulatively established. A specific domestic prohibition on intentional non-consensual sexual synthesis would better protect sexual autonomy and digital identity while maintaining legal certainty and the principle of legality (Noerman dan Ibrahim, 2024).

REFERENCES

- 1) Abdul Wahid, & Mohammad Labib. (2005). *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama.
- 2) Antonio Cassese. (2008). *International Criminal Law* (2nd ed.). Oxford: Oxford University Press.
- 3) Aurelita, M., & Lewoleba, K. K. (2024). Perempuan sebagai Korban Deepfake Pornografi dalam Perspektif Viktimologi. *Kertha Semaya: Journal Ilmu Hukum*, 12(12).
- 4) Gerhard Werle, & Florian Jessberger. (2020). *Principles of International Criminal Law* (4th ed.). Oxford, United Kingdom: Oxford University Press
- 5) International Criminal Court. (1998, July 17). *Rome Statute of the International Criminal Court*. Rome, Italy: United Nations Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court.
- 6) International Criminal Court. (2011). *Elements of Crimes*. The Hague: International Criminal Court.
- 7) Kai Ambos. (2013). *Treatise on International Criminal Law. Volume I: Foundations and General Part*. Oxford: Oxford University Press.
- 8) Kusnadi, S. A., & Putri, D. W. S. (2025). *Perlindungan Hak Privasi dalam Penyalahgunaan Teknologi Deepfake di Indonesia*. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 14(2).
- 9) M. Cherif Bassiouni. (2013). *Introduction to International Criminal Law* (2nd ed.). Leiden, The Netherlands: Martinus Nijhoff Publishers.
- 10) Moeljatno. (2008). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.
- 11) Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi Deepfake di Indonesia sebagai Bentuk Pelindungan Negara. *Jurnal USM Law Review*, 7(2).
- 12) Noviantama, D., & Rahman, A. A. (2025). Deepfake: A Review from the Victimology Perspective. *Contemporary Issues in Criminal Law*, 1(2).
- 13) Office of the Prosecutor. (2022). *Policy on the Crime of Gender Persecution*. The Hague: International Criminal Court.
- 14) Office of the Prosecutor. (2025). *Policy on Cyber-Enabled Crimes under the Rome Statute*. The Hague: International Criminal Court.
- 15) Oktallia, V., & Ariana, I. G. P. (2022). *Perlindungan terhadap Korban Penyalahgunaan Teknik Deepfake terhadap Data Pribadi*. *Kertha Desa*, 10(11).
- 16) Padmasari, A. Q., & Subekti. (2024). Peran LBH APIK Jakarta dalam Perlindungan Hukum terhadap Korban Kekerasan Seksual Berbasis Elektronik. *Qistina: Jurnal Multidisiplin Indonesia*, 3(1).
- 17) Peter Mahmud Marzuki. (2017). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.
- 18) Sijabat, S. A. U., & Lukitasari, D. (2024). Konten Gambar dan Video Pornografi Deepfake sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik. *Recidive*, 13(2).
- 19) Sompotan, S. A., Sondakh, J., & Muaja, H. S. (2026). Kekosongan Hukum (Rechtsvacuum) dalam Penjeratan Tindak Pidana Pembuatan dan Penyebaran Deepfake Pornografi Menggunakan Kecerdasan Buatan di Indonesia. *Lex Crimen*, 15(3).