MIKAILALSYS
Journal of Multidisciplinary Sciences

e-ISSN : 2987-2286
p-ISSN : 2987-3924
Index: Harvard, Boston, Sydney, Copernicus, Sinta 4, Scilit, Semantic, Google, etc

https://doi.org/10.58578/mikailalsys.v4i3.12631

Legal Problematics of Criminal Liability for Sexual Deepfakes as a Form of Digital Sexual Violence

Anisah Friti Anjelia, Yulia Tri Wahyuni, Wevy Efticha Sary
Universitas Bengkulu, Indonesia
anisacurup46@gmail.com

Submitted:	Revised:	Accepted:	Published:
Sep 29, 2026	Oct 28, 2026	Nov 8, 2026	Nov 13, 2026

Abstract

Artificial intelligence (AI) enables the creation of realistic synthetic sexual content using individuals' faces, bodies, voices, or identities without their consent. Sexual deepfakes raise significant legal concerns because individuals can become victims of digital sexual violence without having created or participated in the depicted content. This study analyzes the legal status of sexual deepfakes as a form of digital sexual violence and examines the criminal liability of their creators and disseminators under Indonesian criminal law. It employs a normative legal research method incorporating statutory, conceptual, case, and comparative approaches. The findings indicate that several Indonesian legal instruments partially address sexual deepfakes, including the Law on Sexual Violence Crimes (UU TPKS), the Electronic Information and Transactions Law (UU ITE), the Pornography Law, the Personal Data Protection Law, and the National Criminal Code (KUHP). However, these instruments do not establish a specific and comprehensive criminal offense encompassing the creation and dissemination of non-consensual synthetic sexual content. The principal legal challenge concerns liability at the creation stage because the content does not constitute an actual recording of the victim. These findings highlight the need for a criminal liability framework that distinguishes among the creation of sexual deepfakes, the use of victims' identities, and the dissemination of such content. This distinction provides a conceptual basis for addressing gaps in criminal liability while positioning the victim's lack of consent as the central consideration in legal protection.

Keywords: Sexual Deepfakes; Artificial Intelligence; Digital Sexual Violence; Criminal Liability; Consent

Mikailalsys is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

INTRODUCTION

The development of artificial intelligence (AI) technology has enabled the generation and manipulation of images and videos with increasingly realistic results (Bawole, 2026). One form of misuse of this technology is sexual deepfake, which refers to the creation of sexual representations of an individual using deepfake technology without the consent of the person depicted. In practice, this technology can be used to superimpose an individual's face or likeness onto sexual material depicting acts that the individual has never actually performed (Minegishi et al., 2026).

This phenomenon is part of non-consensual synthetic intimate imagery (NSII), which refers to synthetic intimate content created or used without the consent of the person depicted. A study involving more than 16,000 respondents across 10 countries found that 2.2% of respondents reported having experienced victimization related to deepfake pornography, while 1.8% reported having engaged in behaviors associated with deepfake pornography (Umbach et al., 2024). These findings indicate that sexual deepfake is no longer merely a hypothetical technological concern but has become a phenomenon that causes actual victimization. The problem of sexual deepfake has become increasingly serious because technological advancements enable individuals to produce sexual content without requiring original sexual recordings of the victim. Perpetrators only need to use photographs or videos of the victim available on the internet as source material to generate synthetic sexual content. Consequently, victims can be portrayed in sexual representations of acts that they have never performed or consented to. Research examining perceptions of AIG-NCII indicates that respondents generally consider the creation, and particularly the distribution, of non-consensual synthetic sexual content to be unacceptable (Tenaga & Di, 2026).

These characteristics demonstrate that sexual deepfake involves dimensions of harm that differ from those associated with ordinary information fabrication. The primary issue is not merely whether an image or video is authentic or fabricated, but rather the unauthorized use of an individual's identity to create a sexual representation without their consent. Citron explains that sexual privacy encompasses an individual's interest in controlling information concerning their body, sexuality, and intimate activities (April, 2025). Therefore, although AI-generated sexual content may depict events that never actually occurred, such representations can still violate victims' sexual privacy and autonomy. In recent developments, legal scholarship has also begun to address the creation of sexual deepfakes,

rather than focusing exclusively on their distribution. McGlynn and Toparlak argue that legal responses have so far tended to concentrate on the distribution of synthetic sexual material, while the acts of creating and commissioning such content have received relatively little attention. They propose that the creation of sexual digital forgeries should be understood as a new form of voyeurism because the act of creation itself already causes harm to victims, even before the content is distributed.

This issue is particularly significant in Indonesian criminal law because the criminal justice system must adhere to the principle of legality. An act may only be subject to criminal punishment if there is an existing legal provision establishing it as a criminal offense. The problem is that sexual deepfake represents a relatively new technological phenomenon, whereas Indonesian criminal law provisions were initially formulated to address forms of sexual violence and violations of decency with different characteristics. Nevertheless, Indonesia already has several legal instruments that may be relevant to this phenomenon. Law Number 12 of 2022 concerning Sexual Violence Crimes regulates electronic-based sexual violence under Article 14. This provision covers several intentional and unlawful acts, including the recording or taking of sexually explicit images against the will or without the consent of the person depicted, as well as the transmission of sexually explicit electronic information or documents (Nurahma et al., 2026).

In addition to the Sexual Violence Crimes Law, the Electronic Information and Transactions Law is also relevant to the distribution of content containing indecent material through electronic systems. Provisions concerning the distribution, transmission, and making accessible of electronic information or documents containing content that violates decency may serve as one of the legal grounds when sexual deepfake content has reached the stage of distribution through electronic media (Candra & Abrian, 2025). However, the legal issue does not end with distribution. There is a distinction between creating a sexual deepfake and distributing a sexual deepfake. A perpetrator may create synthetic sexual content involving a victim without ever distributing it to the public. Conversely, an individual may distribute such content without being the person who originally created it. These differences in the nature of each individual's involvement raise questions concerning the legal basis and forms of criminal liability applicable to each perpetrator.

Previous research by Fuadi Isnawan has examined criminal liability for deepfake pornography within the framework of Indonesian criminal law. The study analyzed the

possibility of applying several legal instruments, including the Electronic Information and Transactions Law, the Personal Data Protection Law, and the Pornography Law, to address deepfake pornography (Risky et al., 2026). The existence of this research demonstrates that the issue of deepfake pornography has begun to receive scholarly attention within the Indonesian legal framework. Nevertheless, research on sexual deepfake can still be further developed by focusing on the problems of criminal liability based on the stages of the conduct, particularly the creation and distribution of non-consensual synthetic sexual content. This focus is important because recent research on the criminalization of deepfake pornography indicates that there are distinct legal grounds for imposing liability for the act of creating synthetic sexual content, even before such content is disseminated (Indriawati, 2026).

Accordingly, the central issue addressed in this study is not merely whether sexual deepfake can be criminally prosecuted under Indonesian law, but rather the extent to which existing criminal law provisions provide a basis for establishing liability for each stage of sexual deepfake-related conduct, particularly when the victim has never created or possessed any original sexual content. Based on the foregoing discussion, this study addresses two research questions: first, how is sexual deepfake legally positioned as a form of digital-based sexual violence under Indonesian law? Second, how is criminal liability constructed for perpetrators who create and distribute sexual deepfake content without the victim's consent? This study aims to analyze the legal position of sexual deepfake as a form of digital-based sexual violence and to examine the criminal liability of individuals involved in creating and distributing such content under Indonesian criminal law.

METHODS

This study employs normative legal research, which focuses on examining legal norms, principles, doctrines, and statutory provisions relating to criminal liability for sexual deepfake as a form of digital-based sexual violence. This study aims to analyze legal certainty and the challenges associated with the application of criminal law provisions to acts involving the manipulation of images, videos, or digital content that portray individuals in a sexual context without their consent (non-consensual sexual deepfake). The research approaches employed in this study consist of the statutory approach, conceptual approach, and case approach. The statutory approach is conducted by examining the provisions of Law Number

12 of 2022 concerning Sexual Violence Crimes, the Electronic Information and Transactions Law and its amendments, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 44 of 2008 concerning Pornography, and Law Number 1 of 2023 concerning the Indonesian Criminal Code. Meanwhile, the conceptual approach is used to examine the concepts of sexual deepfake, sexual consent, sexual privacy, electronic-based sexual violence, as well as the principles of culpability and criminal liability. The case approach is employed to analyze relevant court decisions or legal cases in order to identify patterns in the application of legal norms and the potential existence of legal gaps or regulatory ambiguities concerning acts of sexual deepfake. The use of these multiple approaches is necessary because developments in artificial intelligence technology have introduced new forms of sexual violence that raise challenges in applying conventional criminal offense classifications (Chesney & Citron, 2019).

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include statutory regulations governing sexual violence crimes, electronic transactions and information, personal data protection, pornography, and the general provisions on criminal liability under the National Criminal Code. Secondary legal materials comprise criminal law textbooks, scientific journal articles, expert opinions, and research findings addressing deepfake, non-consensual intimate imagery (NCII), AI-generated non-consensual intimate imagery (AIG-NCII), digital-based sexual violence, and criminal liability for the misuse of artificial intelligence technology. Tertiary legal materials include legal dictionaries, encyclopedias, and other reference sources used to clarify relevant legal terms and concepts. Legal materials are collected through library research by inventorying, identifying, and classifying relevant materials according to their relationship with the research questions. Subsequently, all legal materials are analyzed qualitatively using a descriptive-prescriptive analytical method, which involves describing the applicable legal provisions, comparing their compatibility with the characteristics of sexual deepfake-related conduct, and subsequently formulating legal arguments concerning the forms of criminal liability, elements of culpability, parties who may be held liable, and obstacles to law enforcement against perpetrators. This analysis is also directed toward identifying the existence or absence of legal gaps (legal vacuum), vague legal norms (vague norms), and conflicting legal norms (conflict of norms) in providing legal protection for victims of sexual deepfake (Citron & Franks, 2014).

RESULTS

The findings of this study on the juridical problems of criminal liability for sexual deepfake as a form of digital-based sexual violence indicate that Indonesian positive law already provides several legal instruments that may be applied to address such conduct, namely Law Number 12 of 2022 concerning Sexual Violence Crimes (UU TPKS), the Electronic Information and Transactions Law (UU ITE), Law Number 44 of 2008 concerning Pornography, Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), and Law Number 1 of 2023 concerning the Indonesian Criminal Code (National Criminal Code). Nevertheless, the analysis reveals that there are no specific and comprehensive legal provisions governing the creation and distribution of synthetic sexual content using an individual's identity without their consent. This situation creates legal challenges in determining the applicable legal basis, establishing the elements of a criminal offense, proving criminal culpability, and identifying the parties who may be held criminally liable.

1. Characteristics of Sexual Deepfake as a Form of Digital-Based Sexual Violence

The findings indicate that sexual deepfake constitutes a form of digital-based sexual violence with characteristics that distinguish it from the distribution of conventional intimate content. This is because it employs artificial intelligence (AI) technology to create synthetic sexual images or videos by using an individual's face, identity, or physical characteristics without their consent. In such conduct, victims do not necessarily have to have performed or recorded the sexual activities depicted in the digital content. The use of a victim's identity to create false sexual representations can violate sexual privacy, honor, dignity, and individual autonomy. Furthermore, the distribution of such content has the potential to cause psychological, social, and reputational harm to victims. Accordingly, sexual deepfake is not merely associated with technological manipulation but also constitutes a form of identity abuse that involves the dimensions of digital-based sexual violence.

2. Relevance of the Sexual Violence Crimes Law (UU TPKS) to Sexual Deepfake

The findings indicate that Law Number 12 of 2022 concerning Sexual Violence Crimes is relevant to addressing sexual deepfake, particularly through Article 14, which regulates electronic-based sexual violence. This provision covers acts of recording, capturing images or screenshots containing sexual content, as well as transmitting sexually explicit electronic information or documents without consent under the circumstances specified by

law. However, its application to sexual deepfake still presents legal challenges because synthetic sexual content does not necessarily originate from recordings of actual sexual activities but may instead be generated through the manipulation of photographs or videos using AI technology. Consequently, interpretative issues arise concerning the elements of conduct under Article 14 of the UU TPKS, particularly in determining whether the process of creating synthetic sexual images or videos falls within the scope of this provision.

3. Relevance of the Electronic Information and Transactions Law (UU ITE) to the Distribution of Sexual Deepfake

The findings indicate that the UU ITE, particularly Article 27 paragraph (1), as amended by Law Number 1 of 2024, may be applied to analyze the distribution of sexual deepfake content containing material that violates decency. This provision prohibits broadcasting, displaying, distributing, transmitting, and/or making accessible electronic information or documents containing indecent material for public knowledge. Accordingly, uploading or distributing synthetic sexual videos through social media or other digital platforms may potentially fulfill the elements of this criminal offense if all the statutory elements are proven. However, this regulation primarily focuses on the distribution and provision of access to electronic content, meaning that it does not fully encompass the creation of sexual deepfake content carried out privately and without subsequent distribution.

4. Relevance of the Pornography Law to Synthetic Sexual Content

The findings indicate that Law Number 44 of 2008 concerning Pornography may serve as a legal instrument in addressing sexual deepfake when the resulting synthetic images or videos meet the legal definition of pornography as stipulated in Article 1 point 1 and Article 4. These provisions regulate the prohibition of producing, creating, reproducing, disseminating, and providing pornography that meets the characteristics specified by law. Accordingly, synthetic sexual content that substantively fulfills the elements of pornography may be examined under these provisions. Nevertheless, the Pornography Law does not specifically regulate the use of an individual's face or identity to generate sexual representations without their consent. This demonstrates that the regulation of pornography does not yet fully provide protection for the aspects of sexual privacy, identity, and the dignity of sexual deepfake victims.

5. Relevance of the Personal Data Protection Law (UU PDP) to the Protection of Victims' Identities

The findings indicate that Law Number 27 of 2022 concerning Personal Data Protection is relevant to protecting the digital identities of sexual deepfake victims. An individual's facial photographs, images, and visual information may constitute personal data if they can identify that individual, while biometric data and information concerning sexual life are classified as specific personal data under Article 4 of the UU PDP. Furthermore, Article 65 prohibits the unlawful acquisition, collection, disclosure, and use of personal data that does not belong to the individual concerned. Therefore, using a victim's identity to generate synthetic sexual content may give rise to legal issues under these provisions if the relevant elements are fulfilled. However, the UU PDP does not specifically regulate identity manipulation for the creation of synthetic sexual representations, resulting in limitations in providing specific protection for victims.

6. Relevance of the National Criminal Code to Criminal Liability

The findings indicate that Law Number 1 of 2023 concerning the National Criminal Code, through Article 407, provides a legal basis for addressing several acts related to pornography, including producing, creating, reproducing, and disseminating pornographic material. This provision may potentially be applied to the creation and distribution of sexual deepfake content if such conduct fulfills the definition and elements of pornography stipulated in the National Criminal Code. Nevertheless, the National Criminal Code does not yet specifically define sexual deepfake as a distinct form of digital-based sexual violence. The primary issue lies in the use of a victim's identity to generate false sexual representations, which involves not only pornography but also violations of sexual privacy, consent, and individual dignity.

7. Criminal Liability Based on the Stages of Sexual Deepfake-Related Conduct

The findings indicate that criminal liability for sexual deepfake needs to be distinguished according to the stages of conduct and the involvement of each party, namely content creation, requests for or facilitation of content creation, use of the victim's identity, and distribution of synthetic sexual content. Individuals who create such content may be held criminally liable under relevant legal provisions if the elements of a criminal offense are fulfilled. Meanwhile, individuals who commission or assist in the creation process may be held liable under the provisions concerning participation or aiding and abetting, provided

that the applicable legal requirements are satisfied. The use of a victim's identity may be examined under the UU PDP, whereas the distribution of content may fall within the scope of the UU TPKS, UU ITE, Pornography Law, or National Criminal Code, depending on the elements of each offense. Accordingly, the determination of criminal liability must consider the specific conduct, intent, unlawful nature of the act, and the contribution of each individual involved.

8. Lack of Consent as an Aspect of Victim Protection

The findings indicate that the lack of consent is an essential aspect in understanding violations of the rights of sexual deepfake victims. An individual's consent to upload or share photographs on social media cannot be interpreted as permission to use those photographs to create synthetic sexual images or videos. The unauthorized use of an individual's identity to create false sexual representations may violate sexual privacy, honor, dignity, and individual autonomy. Therefore, the handling of sexual deepfake cases needs to consider the context in which the identity is used, the purpose of content creation, the form of distribution, and the impact experienced by victims. Nevertheless, the absence of consent must still be examined alongside the elements of the criminal offense under the applicable legal provisions and does not automatically replace the requirement to prove the elements of the offense.

9. Legal Regulatory Gaps Concerning Sexual Deepfake

The findings indicate that the regulatory gaps concerning sexual deepfake lie in the absence of specific provisions governing the entire series of conduct involving the creation, use of identity, facilitation, and distribution of synthetic sexual content without consent. Although the UU TPKS, UU ITE, Pornography Law, UU PDP, and National Criminal Code may be used as legal instruments, each has a different scope and distinct criminal offense elements, potentially resulting in inconsistent interpretations in law enforcement. This situation demonstrates the need to strengthen regulations to provide legal certainty regarding prohibited conduct, parties who may be held criminally liable, evidentiary mechanisms, and victim protection and recovery. Such regulations must also take the principle of legality into account to ensure that the handling of sexual deepfake does not involve an extension of criminal liability that contradicts the fundamental principles of criminal law.

Table 1. Analysis of Legal Instruments Concerning Criminal Liability for Sexual Deepfake

No.	Legal Instrument	Relevant Provision	Relevance and Limitations
1.	UU TPKS	Article 14	Regulates electronic-based sexual violence but does not explicitly regulate the creation of AI-based synthetic content.
2.	UU ITE	Article 27 paragraph (1) of Law No. 1/2024	Covers the distribution of electronic content containing material that violates decency but does not specifically regulate the creation process.
3.	Pornography Law	Article 1 point 1 and Article 4	May cover the production and circulation of content that fulfills the elements of pornography but does not specifically regulate the manipulation of victims' identities.
4.	UU PDP	Articles 4 and 65	Provides protection against the misuse of personal data but does not specifically regulate the creation of synthetic sexual representations.
5.	National Criminal Code	Article 407	Regulates conduct related to pornography but does not establish sexual deepfake as a separate criminal offense.

Source: Researcher's analysis of statutory regulations, 2026.

Based on Table 1, it can be identified that each legal instrument has relevance in addressing sexual deepfake, but none provides a fully integrated regulatory framework. The UU TPKS and UU ITE are relevant to electronic-based sexual violence and content distribution, the Pornography Law and National Criminal Code concern the production and circulation of pornographic material, while the UU PDP provides protection against the misuse of personal data. The primary limitation lies in the absence of specific provisions that explicitly cover the creation of synthetic sexual representations using an individual's identity without their consent.

Table 2. Stages of Sexual Deepfake-Related Conduct and Potential Criminal Liability

No.	Stage of Conduct	Form of Action	Potential Legal Basis
1.	Creation	Generating synthetic sexual images or videos using the victim's identity.	Pornography Law, National Criminal Code, UU PDP, and UU TPKS, subject to the elements of each offense.
2.	Commissioning or Facilitation	Commissioning or assisting in the creation of the content.	Provisions concerning participation or aiding and abetting, provided that the relevant elements are fulfilled.

3.	Use of Identity	Obtaining and using the victim's photographs or personal data without a lawful basis.	UU PDP.
4.	Storage	Storing synthetic sexual content for a particular purpose.	Depends on the conduct involved and the fulfillment of the elements of the relevant criminal offense.
5.	Distribution	Uploading, sending, or distributing the content.	UU TPKS, UU ITE, Pornography Law, and National Criminal Code, subject to the elements of each offense.
6.	Threats or Extortion	Using the content to threaten or coerce the victim.	UU TPKS and other relevant criminal provisions.

Source: Researcher's analysis, 2026.

Based on Table 2, criminal liability for sexual deepfake must take into account all stages of conduct and the involvement of each party, rather than focusing solely on the individual who distributes the content. Individuals who create, commission, facilitate, use the victim's identity, or distribute the content may face different legal consequences. Nevertheless, the determination of criminal liability must remain based on the fulfillment of the elements of the criminal offense, culpability, the unlawful nature of the conduct, and the provisions concerning participation or aiding and abetting, where relevant.

Overall, the findings of this study reveal that the juridical problems of criminal liability for sexual deepfake lie in the limitations of existing legal norms in addressing all stages of the conduct, the ambiguity surrounding the application of certain criminal offense elements to synthetic sexual content, and the complexity of proving the offense and identifying the responsible parties. Therefore, it is necessary to strengthen criminal law regulations to ensure legal certainty while guaranteeing the protection of victims' identities, sexual privacy, honor, and dignity.

DISCUSSION

1. The Position of Sexual Deepfake as a Form of Digital-Based Sexual Violence

Sexual deepfake essentially constitutes a form of digital technology abuse that combines identity manipulation with sexual representation. This technology enables an individual's face or physical characteristics to be incorporated into sexual material, creating

the impression that the individual is engaging in certain sexual activities (Apriyani et al., 2026). Under such circumstances, victims do not need to have ever created, recorded, or transmitted the sexual material themselves. This characteristic distinguishes sexual deepfake from the distribution of non-consensual intimate content originating from authentic recordings. In conventional image-based sexual abuse, the sexual material may consist of photographs or videos that were actually created by the victim. In contrast, in sexual deepfake, the sexual content can be entirely synthetically generated. Accordingly, the issue of consent is not merely concerned with the distribution of previously created content but also involves an individual's right not to be depicted in sexual representations of acts that they have never performed.

This concept is closely related to the right to sexual privacy. Sexual privacy does not merely refer to the right to conceal one's sexual life from the public but also encompasses the right to determine how an individual's information, body, and sexual identity are represented (Citron, 2019). When AI technology is used to create sexual representations without consent, victims lose control over how they are represented. McGlynn and Toparlak further argue that the creation of sexual digital forgeries can be understood as a form of "new voyeurism." They explain that harm arises at the moment of creation because the act itself constitutes non-consensual sexual conduct that violates the victim's privacy, dignity, and sexual autonomy (McGlynn & Toparlak, 2025).

This approach is important for Indonesian criminal law because it broadens the understanding that harm to victims does not necessarily have to wait until the content is distributed. If the law focuses exclusively on the distribution stage, a protection gap may arise for victims who discover that they have been made the subject of sexual deepfake content even though the material has not yet been distributed. However, recognizing the creation of sexual deepfake as a form of harm against victims does not automatically mean that such conduct constitutes a criminal offense under Indonesian positive law. These two principles must be distinguished. Criminal law is governed by the principle of legality, meaning that an act must first fulfill the elements of a criminal offense as prescribed by legislation.

a. Regulation of Sexual Deepfake under the Sexual Violence Crimes Law (UU TPKS)

The UU TPKS is one of the legal instruments most closely related to the characteristics of sexual deepfake because it specifically regulates electronic-based sexual violence. Article 14 of the UU TPKS regulates acts of recording or taking sexually explicit

images or screenshots against the will or without the consent of the person who is the subject of the recording or image. The same provision also covers the transmission of sexually explicit electronic information or documents to another person without the will or consent of the individual depicted (Republik Indonesia, 2022). This regulation demonstrates that the victim's consent constitutes an essential element of electronic-based sexual violence. Accordingly, the law does not merely consider the sexual nature of the content but also takes into account whether the content was created or distributed without the consent of the person depicted.

Problems arise when this provision is applied to the creation stage of sexual deepfake. In creating sexual deepfake, perpetrators may use photographs of victims obtained from social media. They do not directly record sexual images of the victims. Instead, they use AI-based tools to generate new images or videos. Consequently, there is a distinction between "taking sexually explicit images," as formulated under Article 14 of the UU TPKS, and "creating sexually explicit images synthetically." This distinction cannot be disregarded because criminal law cannot employ analogy to establish a new criminal offense to the detriment of the accused (Isnawan, 2024). Therefore, Article 14 of the UU TPKS is particularly relevant when sexual deepfake has reached the transmission or distribution stage, whereas its application to the creation stage must be approached cautiously by considering the statutory elements of the offense.

b. Regulation under the Electronic Information and Transactions Law (UU ITE)

The UU ITE provides a legal basis for addressing the distribution of electronic information containing material that violates decency. Article 27 paragraph (1) of Law Number 1 of 2024 prohibits broadcasting, displaying, distributing, transmitting, and/or making accessible Electronic Information and/or Electronic Documents containing material that violates decency for public knowledge (Republik Indonesia, 2024). This provision may be applied when perpetrators of sexual deepfake distribute the content through social media, messaging applications, internet websites, or other electronic means. At this stage, the content has become electronic information or an electronic document that can be accessed by other parties.

Nevertheless, the UU ITE does not explicitly use the term deepfake or regulate AI technology as an element of a criminal offense. This creates a legal issue because sexual deepfake has characteristics that distinguish it from ordinary digital sexual content. Research

on criminal offenses involving deepfake pornography under the UU ITE indicates that Article 27 paragraph (1) may be used to prosecute the distribution of content containing material that violates decency, but it does not explicitly regulate content resulting from AI-based manipulation (Korengkeng et al., 2025). Accordingly, the UU ITE provides a basis for criminal liability primarily concerning distribution activities rather than establishing specific regulations on the creation of sexual deepfake.

c. Regulation under the Pornography Law

Law Number 44 of 2008 concerning Pornography is also relevant because it regulates prohibitions against producing, creating, reproducing, duplicating, disseminating, broadcasting, importing, exporting, offering, trading, renting, or providing pornography. If a sexual deepfake meets the characteristics of pornography as stipulated under the Pornography Law, these provisions may theoretically be used to hold the perpetrator criminally liable. However, problems arise concerning the relationship between synthetic content and the victim. In sexual deepfake, the victim is not the person performing the sexual activities depicted in the content. Instead, the victim's face or identity is merely incorporated into sexual material. Therefore, the application of the Pornography Law must consider whether the elements of "creating" or "producing" pornography have been fulfilled and how the victim's position is legally characterized in the conduct. This issue demonstrates that the Pornography Law was not specifically designed to protect victims whose identities are used in synthetic sexual material. Its primary orientation is to regulate pornography as a prohibited object, whereas sexual deepfake involves additional dimensions, including violations of the victim's identity, privacy, dignity, and sexual autonomy.

d. Regulation under the Personal Data Protection Law (UU PDP)

Law Number 27 of 2022 concerning Personal Data Protection is relevant because an individual's face may constitute part of their biometric data. Article 4 of the UU PDP classifies biometric data as specific personal data. In the context of sexual deepfake, a victim's facial photograph may be used as source material to generate synthetic content. If such use fulfills the elements of personal data processing as stipulated under the UU PDP, personal data protection provisions may serve as an additional legal instrument. However, the UU PDP cannot be regarded as the sole basis for criminal liability. Personal data protection focuses on the processing of personal data, whereas sexual deepfake also involves dimensions of sexual violence and violations of sexual privacy (Putra & Dewi, 2024).

Therefore, its application must be assessed based on the specific facts concerning how the data were obtained, used, and processed. Research on deepfake pornography in Indonesia also indicates that the UU PDP may serve as one of the applicable legal instruments, although its regulatory scope remains partial and has not yet established a specific criminal offense concerning sexual deepfake.

e. Regulation under the National Criminal Code

The National Criminal Code, through Law Number 1 of 2023, also contains provisions concerning pornography. Article 407 regulates several acts related to pornography, including producing, creating, reproducing, duplicating, disseminating, broadcasting, importing, exporting, offering, trading, renting, or providing pornography. The existence of these provisions provides a legal basis for addressing certain acts associated with sexual deepfake. However, similar to the Pornography Law, the National Criminal Code does not specifically mention the act of creating synthetic sexual representations of an individual without their consent. Recent research on deepfake pornography in Indonesia also indicates that the existence of several criminal provisions does not automatically eliminate problems associated with regulatory gaps. Multiple regulations may be applied to perpetrators, but there is still no single provision that specifically regulates the characteristics of deepfake pornography as a distinct criminal offense (Afif, 2025).

2. Construction of Criminal Liability for Perpetrators of Creating and Distributing Sexual Deepfake without Victims' Consent

a. Criminal Liability of Perpetrators Who Create Sexual Deepfake

The creation stage represents one of the most problematic aspects of criminal liability. Perpetrators may obtain photographs of victims from the internet, subsequently upload them into AI-based tools, and generate synthetic sexual content. Under these circumstances, the victims have never performed the sexual activities depicted in the content. According to McGlynn and Toparlak, such conduct still causes harm because victims lose control over their own sexual representations. They emphasize that laws that criminalize only distribution fail to address the root of the problem because the acts of creating and commissioning such content constitute the stages that enable the abuse to occur (Isnawan, 2024).

From the perspective of Indonesian criminal law, the issue concerns whether such conduct fulfills the elements of an existing criminal offense. If there is no statutory provision

that precisely covers the creation of such synthetic content, criminal punishment cannot be imposed merely on the assumption that the conduct is morally harmful to the victim. This condition demonstrates the distinction between conduct that causes harm and conduct that has been legally defined as a criminal offense. Not every socially harmful act can automatically be subjected to criminal punishment in the absence of a legal basis that satisfies the principle of legality. Therefore, when a sexual deepfake creator generates the content privately without distributing it, establishing criminal liability under Indonesian positive law becomes more difficult compared to cases involving perpetrators who have already distributed the content.

b. Criminal Liability of Perpetrators Who Distribute Sexual Deepfake

Criminal liability becomes more clearly established when sexual deepfake content has been distributed. Distribution may occur through social media, messaging applications, websites, forums, or other electronic systems. At this stage, Article 27 paragraph (1) of the UU ITE may serve as a legal basis if its elements are fulfilled. In addition, Article 14 of the UU TPKS may also be examined if the conduct fulfills the characteristics of electronic-based sexual violence. A further issue arises when the creator and distributor are two different individuals. The first individual may create the sexual deepfake, while the second obtains the content and subsequently distributes it (Isnawan, 2024).

Under such circumstances, criminal liability must be determined based on the conduct and culpability of each individual. The creator is responsible for the act of creation insofar as the elements of a criminal offense are fulfilled, whereas the distributor is responsible for the distribution or transmission they carry out. This distinction is important because not every individual involved in the circulation of content has the same role. The determination of criminal liability must consider intent, knowledge of the nature of the content, contribution to its distribution, and the applicable criminal provisions whose elements have been fulfilled.

c. Victims' Consent as a Basis for Legal Protection

Consent is one of the most important issues in sexual deepfake. An individual's consent to upload their photograph on social media cannot be equated with consent to use that photograph in sexual content. In other words, there is a distinction between consent to the use of an image and consent to the use of that image to create a sexual representation. This distinction demonstrates that the public availability of a victim's photograph does not

eliminate their right to control their own sexual representation. Victims retain a legal interest in determining how their identity and body are represented.

McGlynn and Toparlak recommend that the criminalization of creating sexual digital forgeries should be based on the absence of consent rather than solely on the perpetrator's motive (McGlynn & Toparlak, 2025). This approach is important because perpetrators may have various motives, ranging from financial gain, entertainment, harassment, revenge, coercion, to simply demonstrating their technological capabilities. If the law requires proof of a specific motive, there is a risk that certain victims will not receive legal protection because the perpetrator cannot be proven to have possessed a motive specifically prescribed by legislation.

d. An Ideal Construction of Criminal Liability

Based on the entire discussion, criminal liability for sexual deepfake can be constructed according to the stages of conduct. First, the creator is the individual who generates synthetic sexual content using the victim's identity or likeness. Second, the individual who commissions or facilitates the creation is the person who knowingly requests another party to produce synthetic sexual content involving the victim. Third, the individual who uses the victim's identity is the person who utilizes the victim's face, voice, body, or personal data as source material to generate synthetic sexual content. Fourth, the distributor is the individual who disseminates, transmits, or makes the content accessible to other parties. These distinctions are important because each action involves a different degree of contribution. Criminal liability must be imposed based on the conduct and culpability of each perpetrator.

On the other hand, artificial intelligence cannot be regarded as a party that bears criminal responsibility within the framework of Indonesian criminal law. AI is merely a tool used by human beings (Putra & Dewi, 2024). Therefore, criminal liability remains directed toward individuals who use, control, instruct, or exploit the technology to commit criminal offenses. This construction is also consistent with research on criminal liability for the misuse of AI, which states that responsibility is not imposed on AI technology itself but rather on the individuals who use such technology. Accordingly, the development of AI does not eliminate the fundamental principles of criminal liability. Technology merely changes the means through which an act is committed, while the subject responsible for the conduct remains human.

CONCLUSION

Based on the research findings and discussion, it can be concluded that sexual deepfake constitutes a form of digital-based sexual violence that raises legal issues in the application of criminal law in Indonesia. This practice involves the use of an individual's identity, face, or physical characteristics to produce synthetic sexual content without the victim's consent through artificial intelligence (AI) technology. Indonesian positive law, through the Sexual Violence Crimes Law (UU TPKS), the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), the Pornography Law, and the National Criminal Code, provides several legal instruments that may be used to address certain acts related to sexual deepfake. However, these provisions do not yet specifically and comprehensively regulate all stages of the conduct, particularly the creation of synthetic sexual content that does not involve the direct recording or capturing of sexual images. Criminal liability must be determined based on the perpetrator's role, form of involvement, intent, and fulfillment of the elements of a criminal offense at each stage of the conduct, ranging from the use of the victim's identity and content creation to facilitation and distribution. In this regard, the provisions of the UU ITE and the Pornography Law are relatively more applicable to acts of distributing or producing content that fulfills the elements of the relevant offenses, whereas the application of the UU TPKS and the UU PDP must be adjusted to the characteristics of the conduct and the respective legal elements. Accordingly, the current construction of Indonesian criminal law remains limited in specifically addressing the creation of sexual deepfake. Therefore, criminal law reform is necessary to establish legal certainty regarding the prohibition of creating and distributing synthetic sexual content without consent, while adhering to the principle of legality and taking into account the protection of victims' sexual privacy, identity, honor, and dignity.

This research contributes to the development of criminal law scholarship, particularly regarding criminal liability for sexual deepfake as a form of digital-based sexual violence arising from advances in artificial intelligence technology. Theoretically, this research broadens the discussion of the relationship between the principle of legality, victim consent, sexual privacy, and criminal liability in addressing forms of sexual violence that do not necessarily involve actual sexual activity or the creation of genuine intimate recordings. Practically, this research maps the relevance and limitations of the UU TPKS, UU ITE, UU PDP, Pornography Law, and National Criminal Code as legal bases for enforcing the law

against perpetrators of sexual deepfake. The findings may also serve as a consideration for legislators and law enforcement officials in developing a legal framework that is more responsive to the misuse of AI technology and in strengthening protection for victims of digital-based sexual violence.

Future research is recommended to examine more deeply the regulatory framework for the criminal offense of sexual deepfake through a comparative legal approach, particularly by examining countries that have enacted specific regulations concerning the creation and distribution of non-consensual synthetic intimate content. Such studies should focus on formulating the elements of the criminal offense, the legal significance of the absence of victim consent, the element of intent, the criminal liability of parties who create or facilitate such content, and the potential liability of digital platform providers. In addition, empirical research is needed to assess the preparedness of law enforcement officials in handling sexual deepfake cases, particularly with regard to digital evidence, perpetrator identification, tracing the source of content, and victim protection. Future research is expected to produce recommendations for a clearer and more comprehensive formulation of criminal law that is oriented toward legal certainty and the restoration of victims' rights, without disregarding the principle of legality and the development of digital technology.

REFERENCES

Afif, M. (2025). Tindak Pidana Deepfake Pornography di Indonesia: Analisis Yuridis terhadap Kekosongan Norma dalam KUHP dan UU ITE. *MERDEKA: Jurnal Ilmiah Multidisiplin*, *3*(2), 27–35. https://doi.org/10.62017/merdeka.v3i2.6133

Apriyani, R., Gegana, R. P., & Puspitasari, N. A. (2026). Perlindungan Hukum terhadap Korban Kejahatan Pornografi Berbasis Teknologi Artificial Intelligence. *Jurnal Hukum, Politik dan Ilmu Sosial*, *5*(3), 86–99. https://doi.org/10.55606/jhpis.v5i3.6677

Candra, M., & Abrian, R. (2025). Penerapan Asas Ultimum Remedium dalam Pengaturan Kekerasan Seksual: Analisis Overlapping Crime antara UU TPKS dan KUHP Nasional. *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, *28*(1), 86–102. https://doi.org/10.15642/alqanun.2025.28.1.86-102

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, *107*(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J

Citron, D. K. (2019). Sexual privacy. *The Yale Law Journal*, *128*(7), 1870–1960. https://yalelawjournal.org/article/sexual-privacy

Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest Law Review*, *49*(2), 345–392. https://www.wakeforestlawreview.com/2026/02/criminalizing-revenge-porn/

Indriawati, S. E. (2026). Konstruksi Pertanggungjawaban Pidana atas Pemanfaatan Kecerdasan Buatan dalam Tindak Pidana Berbasis Deepfake. *Judge: Jurnal Hukum*, *6*(10), 1933–1943. https://doi.org/10.54209/judge.v6i10.2295

Isnawan, F. (2024). Deepfake pornography: How criminal liability of perpetrators in the Indonesian criminal law framework. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *13*(3), 745–771. https://doi.org/10.24843/JMHU.2024.v13.i03.p15

Ivannoel, J., & Putra, M. R. S. (2026). Penyalahgunaan Deepfake sebagai Perbuatan Melawan Hukum dalam Perspektif Kitab Undang-Undang Hukum Perdata. *Al-IHKAM Jurnal Hukum Keluarga Jurusan Ahwal al-Syakhshiyyah Fakultas Syariah IAIN Mataram*, *18*(1), 316–333. https://doi.org/10.20414/alihkam.v18i1.15602

Korengkeng, M. L., Lembong, R. R., & Mewengkang, F. S. (2025). Analisis Tindak Pidana Deepfake Pornografi dalam Perspektif Undang-Undang Informasi dan Transaksi Elektronik. *Lex Administratum*, *13*(3), 1–12. https://ejournal.unsrat.ac.id/v3/index.php/administratum/article/view/62928

Logor, S. C., Bawole, H. Y. A., & Tuwaidan, H. F. D. (2026). Tindak Pidana Pemalsuan Wajah yang Menggunakan Teknologi Artificial Intelligence (AI) Menurut Peraturan Perundang-Undangan. *Lex Crimen*, *15*(3), 135–146. https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/68103

McGlynn, C., & Toparlak, R. T. (2025). The 'new voyeurism': Criminalizing the creation of 'deepfake porn'. *Journal of Law and Society*, *52*(2), 204–228. https://doi.org/10.1111/jols.12527

Minegishi, G. G., Hartono, M. S., & Suastika, I. N. (2026). Analisis Yuridis Hukum Pidana terhadap Penyalahgunaan Artificial Intelligence (AI) Berkenaan dengan Konten Deepfake Pornografi. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(3), 7136–7149. https://doi.org/10.61104/alz.v4i3.6358

Nurahma, N. A., Suharti, T., & Kartoningrat, R. B. (2026). Harmonisasi Regulasi Perlindungan Anak Korban Kekerasan Seksual dalam UU Perlindungan Anak UU Tindak Pidana Kekerasan Seksual dan KUHP Baru. *UNES Law Review*, *8*(4), 1218–1230. https://doi.org/10.31933/vc27e293

Putra, K. B. W., & Dewi, G. A. A. P. (2024). Urgensi Pengaturan Tindak Pidana Deepfake Pornografi di Indonesia. *Kertha Wicara: Journal Ilmu Hukum*, *13*(10), 530–541. https://doi.org/10.24843/KW.2024.v13.i10.p5

Putri, N. A., & Apriyani, M. N. (2025). Pertanggungjawaban Pidana Pelaku Kekerasan Seksual Berbasis Elektronik Artificial Intelegence (Deep Fake Porn). *Wajah Hukum*, *9*(1), 348–358. https://doi.org/10.33087/wjh.v9i1.1725

Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual*. https://peraturan.bpk.go.id/Details/207944/uu-no-12-tahun-2022

Republik Indonesia. (2024). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Pasal 27 ayat (1). https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

Tenaga, D. A. N., & Di, P. (2026). *Jurnal Dinamika Hukum*, *27*(1), 184–209. https://doi.org/10.55397/cps.v3i2.57.2

Umbach, R., Henry, N., Beard, G. F., & Berryessa, C. M. (2024). Non-consensual synthetic intimate imagery: Prevalence, attitudes, and knowledge in 10 countries. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Article 779, pp. 1–20). Association for Computing Machinery. https://doi.org/10.1145/3613904.3642382