Journal of International Trade, Logistics and Law, Vol. 12, Num. 1, 2026, 159-173

IMAGINING FUTURE PROTECTION FROM THE PIT: THE FATE OF VICTIMS OF DEEPFAKE PORN IN INDONESIA- CESSANTE RATIONE LEGIS, CESSAT IPSA LEX

Apriza PUTRI
Universitas Pelita Harapan, Tangerang Indonesia

Fajar SUGIANTO
Universitas Pelita Harapan, Tangerang Indonesia

Velliana TANAYA
Universitas Pelita Harapan, Tangerang Indonesia

Edy GUNAWAN
Universitas Pelita Harapan, Tangerang Indonesia

Received: Feb 04, 2026 Accepted: May 02, 2026 Published: June 01, 2026

Abstract:
The research aims to analyze, identify, and elaborate on the concept of legal liability and legal protection for victims of deepfake pornography generated by Artificial Intelligence (AI) in Indonesia. It also conducts a comparative analysis with the European Union's regulation through the AI Act. Employing a normative methodology with a systematic and comparative legal approach, the research highlights the significant impact of AI development on digital crimes, particularly deepfake pornography, which manipulates victims' images or voices to produce false content without consent. In Indonesia, legal liability for creators and distributors is only partially addressed through laws such as the Electronic Information and Transactions Law (ITE Law), the Pornography Law, the Personal Data Protection Law (PDP Law), and the Sexual Violence Law. However, legal protections for victims are generally broad and lack preventive measures, especially against AI-generated manipulative content. Conversely, the European Union's AI Act provides comprehensive regulation of AI systems, including prohibitions on manipulation, risk assessment, content transparency, and a clear definition of deepfake. Consequently, there is a need for a systematic update of national laws to incorporate both repressive and preventive measures, thereby enhancing legal protections for victims of AI-related crimes such as deepfake pornography.

Keywords:
Deepfakeporn, Artificial Intelligence, Legal Protection

1. Introduction
Technological advancement is progressing at an accelerated pace. Society is experiencing significant transformations, including substantial technological innovations and developments. These changes influence cultural dynamics, presenting both beneficial and adverse effects. This digital age has facilitated the development of technology-driven Artificial Intelligence ("AI"). AI is a specialized field within computer science focused on designing systems capable of executing tasks that typically require human intelligence, including knowledge representation and comprehension. AI systems can encode knowledge in formats understandable to computers, such as logical rules or artificial neural networks (Buffett Institute for Global Affairs, 2023). Additionally, AI functions as an information processor, necessitating rapid and efficient data handling. This encompasses decision-making and problem-solving capabilities essential for advanced applications.

As society's reliance on technology continues to grow, the prevalence of cybercrime has correspondingly increased. Cybercrime encompasses activities conducted by individuals, groups, or organizations that utilize computers, digital technology, or electronic media as instruments or targets of illegal actions. These offenses violate legal statutes both substantively and procedurally, reflecting their serious implications for digital security and legal compliance.

One instance of AI misuse currently is AI-driven cybercrime, specifically Deepfake technology. Deepfake represents a widespread form of cybercrime today and is among the most technologically advanced offenses with a global reach in cyberspace (Edwards, 2023).

The impact of certain actions may not be physically observable but can be equally harmful as other criminal activities. Deepfakes are AI-generated media that manipulate images or video clips to produce realistic-looking fake videos. These videos can convincingly depict individuals performing actions or saying things they did not actually do (Alanazi & Asif, 2024). Such content may range from humorous clips to explicit material or political statements, often created without the consent of the individuals depicted or whose voices are used.

Microsoft President Brad Smith has expressed concerns regarding the development of deepfake AI technology. He emphasizes that, among various AI-related risks, deepfake technology poses significant threats due to its potential for misuse. If exploited by malicious actors, it could facilitate the dissemination of misinformation and disinformation, compromise personal data security, and contribute to widespread misinformation (Edwards, 2023). These issues underscore the importance of implementing robust safeguards to mitigate associated risks.

The adverse effects of deepfake AI pose significant threats to individual privacy rights. These concerns are grounded in the principles outlined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which affirms the right to privacy and protection against arbitrary interference. It states:

“No one shall arbitrarily interfere with his privacy, family, home or correspondence, or attack his honor and reputation. Everyone has the right tolegal protection against such interference or attacks.” This right guarantees that everyone has the right to, in essence, “hide” or close parts of his life from the public eye as one of the most fundamental Human Rights”.

The legal basis for privacy rights in Indonesia is grounded in Article 28G, paragraph 1, of the 1945 Constitution of the Republic of Indonesia, which states:

"Every individual shall have the right to the protection of their person, family, honor, dignity, and property under their control, as well as the right to security and protection from threats of fear, whether to act or refrain from acting. This constitutes a fundamental human right."

While traditionally associated with physical security, the right to personal protection also encompasses digital environments, emphasizing the importance of safeguarding individual privacy in cyberspace. Violations occur when entities such as individuals, corporations, or AI systems access and utilize personal data without proper consent, potentially resulting in the dissemination of misinformation or disinformation through advanced technologies like deepfake (de Vries, 2020).

Contemporary society expresses concern regarding the proliferation of deepfake technology, particularly in the context of pornography. Deepfake pornography involves the use of AI to manipulate video content, creating realistic but fabricated depictions that are challenging to distinguish from authentic footage (Ranjan & Gulati, 2024). This process typically entails altering the facial features of individuals to resemble the original subjects. For instance, a notable case in Indonesia involved actress Nagita Slavina, who was depicted in a 61-second video containing explicit content. Investigations by law enforcement confirmed that the video was artificially fabricated (Agung et al., 2022). Deepfake-related incidents are not unprecedented; numerous public figures, including Gal Gadot, Emma Watson, K-pop idols, and TikTok personalities, have been targeted by such technology (Ji, 2025).

The use of deepfake technology to manipulate images and videos has raised significant concerns regarding privacy and security. An incident in South Jakarta involved the alteration of a minor's photograph to depict nudity, which was reported by the child's mother, RMD. Despite reporting the case to local authorities, the Women and Children's Services Unit indicated that existing sexual harassment laws did not apply. This situation exemplifies the potential for deepfake technology to be misused for malicious purposes.

The proliferation of deepfakes within the adult entertainment industry underscores their increasing influence on consumer behavior. Such technology can cause societal discomfort and breach norms of decency, contributing to social unrest. According to the National Commission on Violence Against Women, reports of gender-based violence, including the dissemination of pornographic content via deepfakes, rose from 876 cases in 2022 to 1,801 in 2023,

highlighting the growing impact of this issue on public safety and societal well-being (CATAHU Komnas Perempuan, 2023).

In the context of legal accountability for AI-related consequences, liability cannot be directly attributed to the technology itself. It is essential to first assess whether AI can be recognized as a legal entity capable of bearing responsibility for its actions. Currently, AI is regarded as a product developed and managed by human operators. Although AI systems can operate autonomously, they remain heavily reliant on human oversight. As technological advancements continue, AI may increasingly make complex decisions and execute actions that are challenging to predict without human intervention.

In addressing these issues, it is imperative that legal frameworks proactively promote a responsible technological environment. Establishing clear regulations will guide stakeholders in defining standards for AI's legal status and accountability. Consequently, regulatory authorities play a vital role in safeguarding societal rights while supporting the progression of AI technology (Isnawan, 2024).

The misuse of AI has led to the alteration of original photographs and videos, resulting in the creation of inappropriate content. Existing legal frameworks, such as Law Number 44 of 2008 on Pornography ("Pornography Law"), Law Number 12 of 2022 on Crime of Sexual Violence ("Sexual Violance Law"), and Law Number 27 of 2022 on Personal Data Protection ("PDP Law") provide some regulation over these issues. These laws regulate the production and distribution of pornographic material, especially when involving objects or models containing such content, and address the unauthorized use of personal data like facial images, voices, or videos to generate fake pornography. While these regulations implicitly cover aspects of deepfake technology, significant legal gaps remain, making enforcement challenging. The Indonesian Information and Electronic Transactions Law ("ITE Law") does not explicitly regulate AI-generated pornography, complicating prosecution efforts due to difficulties in gathering sufficient evidence. The sophisticated nature of digital technology can obscure digital footprints, hindering law enforcement's ability to identify and apprehend offenders. Furthermore, applying existing laws to deepfake cases requires a careful balance between safeguarding individual privacy rights and protecting public interests. Addressing these challenges necessitates the development of more specific legal provisions tailored to emerging AI technologies and their potential misuse.

Additionally, in the context of applying the ITE Law to deepfake incidents, it is essential to maintain a balance between safeguarding individual privacy rights and upholding freedom of expression. Protecting victims' rights should not infringe upon the public's right to privacy and free speech. These legal provisions primarily target the perpetrators or creators involved in the production of inappropriate content. Currently, there are no specific regulations addressing the use of AI to generate or distribute such content, highlighting a gap in existing legal frameworks.

Several nations have implemented measures to regulate AI. The European Union has enacted the EU Artificial Intelligence Act ("AIA"), establishing comprehensive guidelines for AI deployment in sensitive sectors. Indonesia is in the process of developing legislation specifically addressing the transmission and reception of electronic messages via AI technology. Such legislation should delineate appropriate and responsible use of AI, particularly amid ongoing technological advancements (Cancela-Outeda, 2024). Furthermore, establishing legal accountability for AI applications is essential to safeguard societal interests and promote sustainability, thereby mitigating risks associated with irresponsible or unethical AI practices.

Effective oversight mechanisms and advanced deepfake detection tools are critical for ensuring the responsible and ethical application of AI technologies. Establishing clear regulations and guidelines is essential to regulate and limit the use of such technologies. The government should implement comprehensive legal frameworks with defined consequences for violations. Individuals involved in the creation or dissemination of deepfake content must be held legally accountable. Furthermore, developers facilitating the creation and distribution of deepfakes should be liable, especially if their platforms lack sufficient safeguards to prevent misuse. Addressing deepfake-related crimes, such as non-consensual pornography, presents significant challenges for law enforcement due to the technological complexity and difficulties in identifying perpetrators.

Having this said, this research addresses pertinent legal issue: what legal measures are in place to protect victims of AI-generated deepfake pornography under the Indonesian Laws and European Union AI Act? The objective is to establish a comprehensive regulatory framework and enforce appropriate sanctions to ensure the responsible deployment of AI technology, with particular attention to privacy, security, and ethical considerations. Furthermore, advanced detection and tracking capabilities are necessary to identify and mitigate remaining deepfake content. The proliferation of

deepfake pornography poses significant societal risks, including the potential to distort public perception of victims and exacerbate instances of abuse.

2. Method

This research conducts a comparative analysis with the European Union's regulation through the AI Act. Employing a normative methodology with a systematic and comparative legal approach, the research highlights the significant impact of AI development on digital crimes, particularly deepfake pornography, which manipulates victims' images or voices to produce false content without consent.

3. Legal Protection for Victims of Deepfake Porn: a Comparative Analysis between Indonesia and the European Union

3.1 Indonesia's Regulatory Framework

3.1.1 Law No. 11 of 2008 concerning Information and Electronic Transactions

Article 26, paragraph (1), stipulates that the use of information through electronic media involving an individual's personal data without their consent is prohibited. This provision is relevant to issues such as deepfake pornography, where an individual's image or face is digitally manipulated and disseminated via electronic media without authorization. Victims of such violations have the right to pursue legal action against perpetrators, as their personal data rights are infringed upon, resulting in harm. This is further supported by Article 26, paragraph (2), which encompasses elements such as the violation of privacy rights, incurred damages, and the right to file a lawsuit. Additionally, Articles 27, paragraphs (1) and (2), address acts committed intentionally and without legal rights, including the distribution, transmission, or accessibility of content that violates decency or constitutes defamation.

The articles outlined establish regulations for the protection of personal data and privacy. They provide a legal basis for prosecuting individuals involved in the creation and dissemination of deepfake pornography without the consent of the affected parties. Furthermore, these regulations prohibit the intentional distribution, transmission, or accessibility of electronic content that contains obscenity or defamation. Deepfake pornography constitutes a violation of these provisions as it infringes upon an individual's rights, privacy, and reputation.

3.1.2 Law Number 44 of 2008 on Pornography.

Article 4, paragraph (1), explicitly prohibits individuals from producing, reproducing, disseminating, or trading objects that constitute pornography, including explicit images of sexual acts, violence, nudity, genitals, and child pornography. This prohibition extends to digital representations, such as deepfake pornography, which can be considered a form of visual pornography regardless of the content's authenticity.

Furthermore, Articles 6 and 9 restrict individuals from listening to, displaying, possessing, or storing pornographic material, unless authorized. They also prohibit the creation of digital models or representations of individuals for pornographic purposes without consent. Consequently, creating or storing deepfake pornographic videos on personal devices without proper authorization may constitute a legal violation, even in the absence of distribution. Using individuals as digital models without their permission also constitutes an infringement under these provisions.

Violations of this legislation may lead to imprisonment and penalties as specified in Articles 29 and 35. Any individual who breaches the provisions outlined in Article 4, Paragraph 1; Article 6; or Article 9 faces imprisonment ranging from six months to twelve years and a fine between 250 million and 6 billion Rupiah, particularly if they produce or distribute deepfake pornography. Specifically, individuals involved in creating deepfake pornographic content are subject to imprisonment of one to twelve years and a fine ranging from 500 million to 6 billion Rupiah if they violate Article 9, which pertains to the misrepresentation of individuals as appearing in pornographic material. Deepfake pornography inherently encompasses such content.

3.1.3 The Indonesian Criminal Code

Article 407, paragraph (1), addresses the entire distribution and commercialization chain of both physical and digital pornographic content. Violations may result in imprisonment ranging from a minimum of six months to a maximum of ten years, along with fines categorized as category IV and category VI.

This legislation governs various activities that facilitate the dissemination of pornographic material through traditional media, such as films and photographs, as well as digital and electronic platforms. In the contemporary context, it is

particularly pertinent to issues like deepfake pornography, which involves the illegal production and distribution of pornographic content using digital technology.

3.1.4 Law No. 12 of 2022 on Sexual Violence Crimes

The legal framework outlined in the specified articles delineates the scope and classification of sexual violence offenses. Article 4, paragraph (1), defines sexual violence comprehensively, encompassing both non-physical and physical acts, including sexual harassment, exploitation, sexual slavery, and cyber-based sexual violence. This provision underscores the recognition of acts that compromise an individual's dignity and sexual integrity, including those perpetrated through digital media platforms.

Additionally, Article 5 highlights non-physical sexual acts aimed at degrading a person's dignity, targeting their body, sexual desires, or reproductive organs. The emphasis on non-physical acts broadens the scope of criminal liability to include verbal, symbolic, or digital harassment that does not involve physical contact. Such offenses are punishable by imprisonment for up to nine months and a fine of up to 10 million Rupiah. Furthermore, Article 14, paragraph 1, explicitly addresses sexual violence committed via electronic media, reinforcing the legal recognition of digital forms of abuse.

The article analyzes the elements constituting sexual violence offenses, including unauthorized recording, photographing, or capturing of sexually explicit material involving a victim; non-consensual transmission of such content; and electronic stalking or tracking for sexual purposes. This analysis emphasizes that sexual violence encompasses not only physical acts but also technology-facilitated misconduct, involving the misuse of personal images or data for sexual objectives. The provisions explicitly address various forms of sexual acts that cause harm to victims, either directly or indirectly. This includes, by implication, deepfake pornography, which can constitute non-physical harassment and electronic-based sexual violence.

Detecting and prosecuting deepfake pornography presents significant challenges due to the sophisticated visual manipulation technology involved. Such content involves superimposing a person's face or body onto pornographic material without their consent. Consequently, the violence is not physically or verbally directed at the victim but circulates within cyberspace through digital manipulation (Kasita, 2022).

The law primarily targets "person-to-person" sexual violence, where the perpetrator and victim share an identifiable physical, emotional, or communicative relationship. Conversely, deepfake pornography often involves an anonymous third party, making it difficult to identify the perpetrator. This anonymity complicates law enforcement efforts and may hinder timely legal action.

The provisions outlined in Article 14 concerning electronic-based sexual violence primarily address actions such as recording, transmitting sexual content, or directly monitoring the victim. However, in cases of deepfake pornography, the content is often not directly documented; it may be generated using publicly available images or videos, which are subsequently manipulated without the victim's knowledge. The lack of direct interaction between the perpetrator and the victim complicates the classification of deepfake-based activities within the framework of this law.

3.1.5 Law No. 27 of 2022 on Personal Data Protection

Article 65, paragraphs (1), (2), and (3), explicitly prohibit any individual from unlawfully acquiring, disclosing, or utilizing another person's personal data, particularly when such actions confer benefits upon the perpetrator or others and cause harm to the data subject. A significant aspect of this provision concerns unauthorized access to and use of data, including digital photographs or videos, without the requisite consent. This regulation is particularly pertinent in the context of deepfake pornography, where such unauthorized data manipulation constitutes a primary method of content creation.

Additionally, Article 66 explicitly forbids the creation or falsification of personal data for the advantage of specific parties. This prohibition underpins the criminal sanctions outlined in Article 68. The term "profit" within this context extends beyond monetary gains to encompass non-monetary benefits, such as personal satisfaction, increased popularity, humiliation of the victim, or motives rooted in revenge.

In the realm of deepfake pornography, perpetrators may derive non-monetary benefits, such as psychological gratification or enhancement of social reputation, despite not generating direct financial gain. The legal provisions outlined in the relevant statutes address acts of falsifying personal data that could harm the data subject. Specifically, manipulating an individual's face, voice, or body into sexual content without consent constitutes a clear violation of

personal data integrity within the context of deepfake pornography. Although Articles 65, 66, and 68 of the Personal Data Protection Law explicitly prohibit unlawful collection, use, and falsification of personal data, these regulations have proven insufficient in safeguarding victims of technology-facilitated crimes like deepfake pornography. This inadequacy stems from various normative and technical limitations.

The PDP Law emphasizes administrative procedures and data protection broadly, including safeguarding consumer information, demographic data, and digital transactions. However, it lacks specific provisions addressing deepfake pornography, where personal data is compromised through sophisticated visual and auditory manipulations. Establishing a direct link between these manipulations and the perpetrator's intent to profit, as outlined in Articles 66 and 68, remains challenging. Additionally, the law does not explicitly establish a liability framework for the misuse of personal data in the context of fabricated sexual content. Such misuse causes not only material harm but also significant psychological and reputational damage to victims. Non-material damages, including embarrassment, trauma, and social dignity loss, are insufficiently protected under current legislation.

Furthermore, identifying perpetrators of deepfake pornography presents considerable difficulties. The PDP Law lacks technical guidelines for law enforcement to trace and act against individuals involved in producing or distributing manipulated content derived from personal data. Perpetrators often conceal their identities through international cyber networks, complicating enforcement efforts. Although the PDP Law establishes a legal framework for addressing violations related to personal data misuse; however, it does not fully encompass protections for victims of deepfake pornography.

3.1.6 Law No. 28 of 2014 on Copyright

The development of AI models often involves utilizing large-scale datasets comprising text, images, audio, or video sourced from online platforms. Such data is frequently collected without explicit consent from the copyright holders, including literary works, journalistic articles, digital images, music, and videos, many of which are protected by copyright law. This practice may constitute a violation of Article 9 which grants creators exclusive rights to reproduce and distribute their works, as well as Article 113, which establishes legal sanctions for infringement. Using copyrighted materials as training data without proper authorization or licensing can undermine the economic interests and moral rights of creators, regardless of whether the use is direct or involves data transformation.

AI as computer programes is protected under Article 40 which included in the types of protected works. Furthermore, according to Article 31, there are 4 instances to attribute an individual as a "creator" of a work, unless proven otherwise. The individual considered the creator of a work is the person whose name appears in the creation, is declared as the creator of the creation, is listed in the creation's registration certificate, or is included in the public register of creations as the creator.

The Indonesian Copyright Law adopts the declarative principle, meaning that recordation is not a requirement under the law as protection is automatically afforded when a work is first published and manifested in a tangible form. However, it is advisable to file a recordation with the Directorate General of Intellectual Property to formally validate the copyright protection and enhance the commercial value of the work. In application, potential purchasers or licensees of copyrighted works typically request an official statement confirming ownership of the copyright from the seller or licensor, through a recordation certification. This certification serve as preliminary proof of ownership, subject to further verification (Aurelia et al., 2025).

A party may seek legal remedy for copyright infringement by filing a police report and pursuing settlement through alternative dispute resolution, arbitration, or a commercial court. The criminal provisions and penalties are outlined in Chapter 17, Articles 112-120 of the Indonesian Copyright Law. For copyright infringement, depending on the severity and context, the law provides for imprisonment ranging from one year to a maximum of 10 years and/or fines from IDR 100,000,000 (one hundred million Rupiah) to a maximum of IDR 40,000,000,000 (forty billion Rupiah). The criminal offenses specified in this law are classified as complaints-based offenses.

3.2 the Legal Implications of Ai-Generated Deepfake Pornography

3.2.1 Indonesia's Regulatory Landscape

The ongoing challenges in addressing deepfake pornography primarily involve regulatory and investigative hurdles. Key issues include:

a. Identification of Perpetrators: The anonymity provided by deepfake technology complicates efforts to identify and prosecute offenders, especially when identity-disguise tools are employed.
b. Legal Framework Limitations: Existing laws, such as the ITE Law and the Pornography Law, may not comprehensively address all aspects of deepfake pornography, and their enforcement can be constrained.
c. Evidence Collection and Investigation: The sophisticated nature of deepfake creation poses significant challenges for evidence gathering. Effective investigations demand substantial resources and advanced technical expertise.
d. Public Awareness: Limited awareness among the public regarding the risks and consequences of deepfake pornography can hinder victims from reporting incidents and seeking assistance.
e. Limited Resources and Capabilities: Law enforcement agencies often face constraints due to limited resources and capabilities when addressing cases involving deepfake pornography. Insufficient training and infrastructure for digital crimes further complicate these efforts.
f. Lack of Inter-Agency Cooperation: Effective response requires robust inter-agency cooperation among law enforcement, internet service providers, and relevant stakeholders. A lack of coordination can impede efforts to protect victims and enforce legal measures.
Given these challenges, it is evident that Indonesia's existing legal framework primarily addresses regulatory aspects of specific AI applications. Liability for damages is generally assigned to legal entities, including individuals and organizations with recognized rights and obligations. This approach may be inadequate when AI systems exhibiting human-like intelligence and capabilities cause harm. The legal status of AI as a potential legal subject remains a pertinent consideration in determining liability for criminal acts and damages (Rezon et al., 2025).
The advancement of AI technology is an inevitable development across all societal levels and nations. This progression necessitates the formulation of specialized legal frameworks to regulate AI. Consequently, regulations such as ITE Law have been enacted. However, it lacks a precise definition of AI. As AI technology evolves rapidly, diverse interpretations have emerged from various sectors, aligning with the provisions of the ITE Law.
Under the ITE Law, AI is interpreted as electronic systems and electronic agents. Article 1, Number 5 defines an electronic system as:
"A series of electronic devices and procedures designed to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate electronic information."
Furthermore, Article 1, Number 8 describes an electronic agent as:
"A device within an electronic system created to perform actions on specific electronic information organized by a human operator."
AI refers to an electronic system operated under human oversight to execute specific tasks. While AI is capable of addressing problems similarly to human cognition, it does not act autonomously; human intervention is required to direct its actions.
The operation of AI systems is managed by designated electronic system administrators responsible for compliance with Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions. Consequently, AI is not recognized as a legal entity and cannot bear criminal liability, as its actions are governed and directed by human operators who are the sole legal subjects under Indonesian criminal law.
The current legal framework presents challenges in addressing the use of AI technology to produce synthetic pornographic content. Existing laws, such as the ITE Law, regulate the distribution of illegal content and privacy violations but do not explicitly address deepfake pornography. The lack of specific legislation targeting this form of digital manipulation hampers law enforcement efforts to identify and prosecute offenders effectively. Although the Sexual Violance Law Law recognizes electronic and non-physical sexual violence, it does not explicitly mention deepfake pornography, further complicating legal enforcement (Chairani et al., 2022). Legal provisions within the Criminal Code could potentially be applied to cases involving deepfake pornography; however, these are broad and do not account for the unique aspects of AI-generated content, creating legal gaps that offenders may exploit (Judijanto et al., 2025). The PDP Law aims to safeguard personal data but does not specifically regulate the misuse of personal information through digital manipulation techniques such as deepfakes, leaving this area left unregulated.
The absence of comprehensive and targeted regulations impedes effective legal recourse for victims of deepfake pornography, thereby complicating law enforcement efforts to prosecute offenders fairly and proportionately. Current legal frameworks are insufficiently adapted to address the specific challenges presented by AI technologies, especially

deepfakes. The lack of a precise legal definition for deepfakes results in regulatory gaps, which can be exploited for malicious purposes and hinder enforcement and sanctions against such activities.

3.2.2 the European Union's Regulatory Landscape

The advancement of AI technology has introduced significant legal challenges, notably the emergence of deepfake pornography, which jeopardizes individual privacy and dignity. In response, the European Union has drafted the AIA, a comprehensive legal framework designed to regulate high-risk AI applications that may infringe on human rights.

Public awareness regarding the widespread adoption of AI and machine learning technologies has increased markedly in recent years. This heightened awareness contributed to the development of the AIA, which is the culmination of ongoing efforts to establish ethical and safe AI regulations. The legislative process commenced in February 2020 with the publication of the White Paper on AI: A European Approach to Excellence and Trust by the European Commission. This document underscores the importance of a risk-based approach to AI regulation. The proposed legislation aims to establish a robust legal framework for AI in Europe, ensuring safety, transparency, and accountability in AI deployment (Nizza, 2024).

The European Union announced in December 2023 that it had reached a provisional agreement on the fundamental aspects of the upcoming AIA. The draft legislation delineates the classification of AI-related risks, establishes obligations for AI system providers and users, and introduces new supervisory entities, including the European Artificial Intelligence Board and the Artificial Intelligence Office, to oversee effective implementation and enforcement. The law is anticipated to become effective between May and July 2024, providing stakeholders with an early understanding of the AIA's framework. Following an extensive legislative process, the European Parliament formally approved the AIA on March 13, 2024, and the Council of the European Union endorsed it on May 21, 2024. The legislation entered into force on August 1, 2024 (Aboy et al., 2024).

The AIA seeks to establish a comprehensive legal framework for AI on a global scale, promoting trustworthy AI practices within Europe and internationally. This framework aims to ensure that AI systems uphold fundamental rights, safety standards, and ethical principles, while effectively managing the risks associated with highly advanced and impactful AI models. The newly created EU AI Office will be responsible for overseeing the implementation and enforcement of the AIA. Noncompliance may result in significant penalties, including fines of €35 million or 7 percent of global revenue, or €7.5 million or 1.5 percent of revenue, depending on the severity of the violation and the company's size. Consequently, AI providers, developers, and implementers must familiarize themselves with the provisions of the AIA and understand its implications for their operations (European Parliament, 2023).

The AIA provides a formal definition of "deepfake" in Article 3(60), describing it as " deep fake' means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful". This regulation addresses manipulated content generated by AI that impersonates individuals or objects in videos or images without their consent. Specific provisions in Article 5, including clauses (a), (b), (e), and (g), prohibit activities that involve the manipulation or distortion of individuals' or groups' behavior through AI systems, particularly when such actions could lead to harmful decisions (Kusche, 2024).

Furthermore, Article 5 restricts the exploitation of vulnerabilities based on factors such as age, disability, or socioeconomic status. It also bans the use of AI to create or expand facial recognition databases by capturing images from the internet or CCTV footage. Additionally, the regulation prohibits biometric categorization systems that classify individuals based on biometric data to infer sensitive personal attributes, including sexual orientation or sexual activity.

Article 6 delineates a classification framework for AI systems, emphasizing the regulation of high-risk AI applications. Deepfake pornography is identified as a high-risk category under this regulation. According to this article, AI systems that automatically profile individuals by analyzing personal data to evaluate various aspects such as performance, health, or preferences are considered high-risk. Specifically, Article 6 of the AIA states that any system performing automated analysis of personal data to assess factors like employment performance, economic status, or health qualifies as a high-risk system. While deepfake technology primarily involves generating synthetic visual and audio content, it can also be regarded as a profiling system that potentially infringes on individuals' reputation, privacy, and safety.

Article 50 of the AIA delineates transparency requirements concerning the deployment of synthetic and deepfake content. It mandates that AI systems responsible for generating manipulated or entirely AI-produced media—such as images, videos, or audio—must clearly disclose to the public that the content is not authentic or has been altered through AI technology. This requirement applies not only to high-risk AI systems, which are subject to rigorous conformity assessments, but also to general-purpose AI used for creating synthetic or deepfake content (Umbach et

al., 2024). Consequently, even AI technologies not classified as high-risk must adhere to transparency obligations when used to produce content that could mislead or influence public perception. The primary objective of this regulation is to safeguard individual rights and enable the public to distinguish authentic content from manipulated media. Furthermore, Articles 71–73 specify the administrative penalties for violations of the AIA, with fines potentially reaching €35 million or 7% of the company's annual revenue, depending on the severity of the violation (Momeni, 2024).

This regulation provides a precise definition of a "deepfake" and explicitly prohibits the use of AI systems that facilitate behavioral manipulation, exploit vulnerabilities, misuse biometric data, or violate individual privacy and dignity. Through provisions outlined in Articles 5, 6, and 50, as well as administrative sanctions specified in Articles 71-73, the AI Act underscores that employing AI technology to produce non-consensual fake pornographic content constitutes a serious violation of human rights. The legal framework of the AI Act primarily targets the creators, developers, and providers of such technology, indicating that legal liability extends beyond the end-users to include those responsible for the development and distribution of AI systems enabling such content creation. Developers are mandated to ensure their systems are not exploited to harm individuals, especially concerning sexual privacy breaches and defamation, which can cause significant damage. Overall, the AI Act is designed as a preventive regulation addressing the core issue: the AI systems themselves and the entities involved in their creation.

The AIA uses a layered assessment approach to evaluate the potential risks posed by AI technology. Each level of this structure reflects a different level of regulation; the higher the risk level, the more stringent the regulation. Generally, AI risks are categorized into four main tiers and visualized in the form of a pyramid.

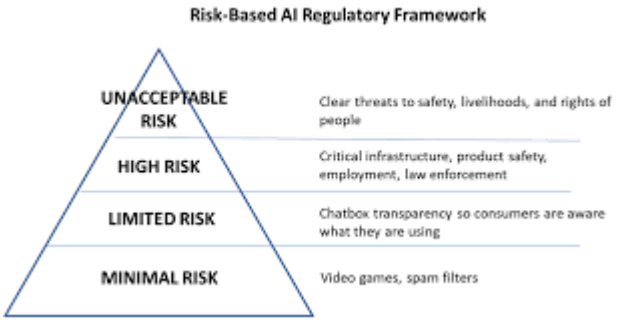

Figure 1. Risk-Based AI Regulatory Framework
Source: https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/

High-risk AI systems are those employed in contexts or applications that could significantly affect fundamental human rights, health, or safety. These systems are characterized by their integration into safety-critical components or products regulated under EU law, specifically in Annex I, and are subject to third-party conformity assessments as mandated by the relevant legislation. This regulation is detailed in Articles 6 and 8-17 of AIA.

Furthermore, AI systems may be classified as high risk if they satisfy specific criteria outlined in Annex III. The categories of high-risk AI systems include:

a. Systems involved in automated decision-making processes concerning personal attributes such as employment, economic status, health, or needs, particularly when utilizing sensitive personal data.

b. Biometric identification or categorization systems, such as facial recognition or emotion analysis technologies, which are considered to pose high risks.

c. Critical infrastructure systems encompass the management and operation of essential digital frameworks, including road traffic management and water supply systems.

d. Vocational education and training systems involve establishing criteria for student access, evaluation, supervision, and the overall learning process.

e. Systems utilized in public and private services include the assessment of social benefit eligibility and credit allocation mechanisms.

f. Law enforcement systems are employed to evaluate individual risk levels related to criminal activity and to analyze evidence during investigations.
g. Migration and border management systems are responsible for verifying identities, assessing criminal risks, and determining eligibility for asylum and visa applications.
h. Systems within the administration of justice and democratic processes support the research and application of legal facts, influencing election outcomes and results

Providers of High-Risk AI Systems are required to adhere to comprehensive compliance measures, including risk management throughout the AI lifecycle, relevant and accurate data management, thorough technical documentation, automated traceability with human oversight, and ensuring system accuracy, robustness, cybersecurity, and quality management to meet regulatory standards.

Deepfake pornography is classified as a high-risk activity. It was previously designated as limited risk; however, considering its substantial impact on individuals—particularly concerning privacy breaches, defamation, and the misuse of personal data—the European Commission approved the reclassification to high risk. Consequently, the European Commission has authorized the modification or addition of risk categories following comprehensive risk assessments (Jacobsen & Simpson, 2024).

The AIA establishes provisions for legal sanctions to ensure compliance with regulations aimed at protecting victims. Administrative sanctions, as outlined in Articles 71-73 of the AIA, may include fines of up to €35 million or 7% of the company's total annual global revenue, whichever is greater. These sanctions target AI system providers, distributors, and entities that violate regulations concerning risk classification, transparency, or the use of AI for prohibited purposes. The sanctions embody the precautionary principle within the European Union legal framework, emphasizing that technology entities are accountable not only for the technical outcomes of AI systems but also for their social and ethical implications, including potential harm caused by deepfake content.

As previously explained, the AIA focuses more on imposing sanctions on creators, developers, and technology providers. Not to the perpetrators who create deepfakes, because this is aimed at protecting victims from the root (preventive) and not just the perpetrators, but, developers can also be held accountable. Individual perpetrators of deepfake porn can be subject to criminal sanctions based on the applicable national laws of European Union member states, particularly under legal frameworks that protect privacy, defamation, gender-based violence, and digital sexual exploitation.

Italy, as a member of the European Union, has adopted a comprehensive legal framework to address deepfake pornography and related issues. The country leverages general criminal provisions outlined in the Criminal Code and incorporates principles from the General Data Protection Regulation ("GDPR") to enhance data protection measures. A key legislative development is Article 612-ter of the Italian Penal Code, introduced through the "Red Code" reform on July 17, 2019. This legislation aims to strengthen protections for victims of gender-based and domestic violence, explicitly criminalizing revenge porn—the dissemination of intimate images or videos without consent. The reform addresses previous legal gaps, providing robust safeguards for victims' rights to self-determination, honor, reputation, privacy, and sexual dignity. Penalties for violations include imprisonment ranging from one to six years and fines between €5,000 and €15,000, applicable to content creators, distributors, and third parties who knowingly spread illegal material. Enhanced sanctions are imposed if the offender is a partner, uses digital media, or if the victim is vulnerable, such as being pregnant or mentally or physically incapacitated. Additionally, provisions from Article 595, paragraph (3), concerning defamation via mass media, including online platforms, can be applied analogously, with penalties extending to imprisonment for up to three years and higher fines, depending on the severity of the offense.

The AI assesses risk levels, particularly in the context of pornography, where AI-driven misleading manipulation is classified as a prohibited practice. The AIA mandates transparency, feasibility testing, and internal controls by developers and providers of AI systems. It also assigns legal responsibility not only to those who distribute deepfake pornography but also to all entities involved in the development and deployment of AI technologies used for such purposes. This approach emphasizes oversight and ethical considerations throughout the entire lifecycle of AI systems, from design to societal application (Vecchietti et al., 2025). Developers are required to evaluate the social impact and potential risks, including violations of privacy, reputation, and human dignity. AIA enforces labelling requirements for digitally manipulated content to ensure public awareness of AI-synthesized media, thereby preventing deception and protecting victims of manipulative content. These regulations are complemented by other legal frameworks, such as the Digital Services Act (DSA), which obligates digital platforms to promptly and responsibly remove illegal content (European Commission, 2022).

Italy exemplifies the implementation of these principles through its legislative actions. In April 2024, Italy proposed Draft Law No. 78 on AI, aiming to incorporate the AI Act's principles into national law. The draft includes specific provisions addressing AI-related crimes, notably a proposed Article 612-quarter to the Italian Penal Code, criminalizing the dissemination of artificially generated or manipulated content, including deepfake pornography. These measures seek to strengthen legal protections, targeting both perpetrators and the developers and users of relevant technologies (Vecchietti et al., 2025). Italy's initiative reflects the European Union's broader commitment to aligning national legislation with the AI Act, fostering a legal environment responsive to the challenges of the digital and AI era. Collectively, these regulations demonstrate the EU's dedication to safeguarding citizens' fundamental rights by ensuring safety, accountability, and public trust in AI-based products and services.
The comparison result can be summarized as follows:

Table 1.

Element	**Regulating Law(s) in Indonesia**	**Regulating Law(s) in the European Union**	**Legal Protection**
AI (deepfake)	Unregulated	Article 3 (60) of AIA: definition of deepfake	Indonesia: AI is not a legal person
		Article 5 of AIA: Prohibition of manipulation and exploitation	AIA: does not consider AI as a legal subject, but protects society from the risks of AI through strict regulations (preventing misuse of AI before harm occurs/preventive)
		Article 6 of AIA: high-risk classification	
Developer	Article 9 Copyright Law: exclusive rights of the creator	Article 5 of AIA: Prohibition of manipulation and exploitation	Indonesia: The Copyright Law only protects creations, only to the extent that developers create AI as computer programs, do not control distribution, and provide unlimited access to third parties to tools that could harm others.
	Article 40 (1): protected as computer programe	Article 50 of AIA: Transparancy	AIA: can be held liable to developers if they fail to prevent misuse and are subject to a maximum administrative penalty of up to €35 million or 7% of the company's total global annual revenue, whichever is greater
Content Creator	Article 27 (1), Article 45 (1) of ITE Law	Article 3 (6), Article 5, Article 6 of AIA	Indonesia: enforcement is difficult (anonymity & digital evidence), no regulations regarding engineered/manipulated digital porn content
	Article 4 (1), Article 29, Article 35 of	EU GDPR: protection of the victim's personal data if the	

	Pornography Law	face/identity aspect is used without permission	(deepfake), more regulation of "person-to-person" sexual activity
	Article 407 (1) of the Indonesian Criminal Code	Article 612-ter, Article 595 (3) of Italia Penal Code	EU: prohibited if used for sexual manipulation without consent, individual perpetrators are subject to the national laws of each member state, such as Italy
	Article 4 (1), Article 5 (1), Article 14 (1) of Sexual Violence Law		
	Article 65, Article 66, Article 68 of PDP Law		
Content Disseminator	Article 27 (1), (3), Article 45 (1) of ITE Law	Article 50 of AIA	Indonesia: can be prosecuted if proven to have distributed it, there are no regulations regarding engineered/manipulated digital porn content, victims have difficulty accessing platforms to request removal
	Article 4 (1), Article 29 of Pornography Law	Article 60 of DSA	EU: distributors can be held liable in the form of sanctions and fines (returning to the national laws of each country), DSA forces digital platforms to quickly remove illegal content (within 24 hours) distribution is charged to digital service providers.
	Article 407 (1) of Indonesian Criminal Code		
Victims	Article 4 (1), Article 5, Article 14 (1), Article 67, Article 68 of Sexual Violence Law	Article 16 of DSA	Indonesia: protection is still general and not yet comprehensive, especially for psychological and reputational losses due to manipulative content, a difficult complaint system for victims, protection is still partial and repressive rather than preventive

	Article 65 of PDP Law	EUGDPR: Victim's right to data deletion, right to privacy, redress for losses	EU: There is a right to redress, the right to erasure of content, and the protection of personal data (referring to each country's national laws). Italy is expanding protection through AI Bill No. 78 of 2024 and the proposed Article 612-quarter, which explicitly criminalizes manipulative AI-generated content. There is preventive and repressive protection

4. Conclusion

Legal accountability for victims of AI-driven deepfake pornography within Indonesia's current legal framework is insufficient. Existing regulations, such as the ITE Law, Pornography Law, Sexual Violence Law, PDP Law, and the Criminal Code, do not explicitly address the phenomenon of AI-generated digital manipulation, including deepfake pornography. The sophisticated nature of deepfake content, which employs advanced technologies like Generative Adversarial Networks (GANs) and deep learning, complicates the process of distinguishing authentic from manipulated content. This complexity hampers law enforcement efforts in establishing elements of wrongdoing, causal relationships, and identifying perpetrators. The lack of a precise legal definition of deepfake and the absence of specific regulations concerning legal accountability for AI systems or technology entities constitute significant barriers to providing comprehensive legal protection for victims and limit legal recourse against operators of AI platforms involved in content creation. Their role is integral to the production chain of deepfake content.

Comparative analysis with European Union regulations reveals a regulatory imbalance. The AIA and Digital Service Act (DSA) offer a comprehensive, preventive, and adaptive legal framework. The AIA defines deepfake as misleading synthetic content, classifies AI system risks, prohibits AI applications that threaten human rights, and assigns legal responsibility to developers and technology providers, including transparency and ethical oversight obligations. The DSA mandates digital platforms to swiftly and responsibly remove illegal content. In contrast, Indonesia lacks comparable legal instruments to anticipate AI-related risks. The country has yet to establish a legal framework for classifying AI risks, transparency obligations for developers, or mechanisms for victim recovery. This deficiency indicates that Indonesia's legal system is inadequately equipped to address the complexities and threats posed by deepfake technology, which infringe on privacy, reputation, and human dignity. An effective legal system should encompass both preventive and repressive measures; however, Indonesia's current laws fall short in providing comprehensive protection. The regulatory gaps weaken preventive efforts and diminish access to justice for victims, thereby undermining repressive measures. Consequently, victims of deepfake pornography in Indonesia do not receive optimal legal protection. This situation underscores the urgent need for Indonesia to develop legal policies aligned with technological advancements and grounded in respect for human rights in the digital age.

References

Aboy, M., Minssen, T., & Vayena, E. (2024). Navigating the EU AI Act: implications for regulated digital medical products. Npj Digital Medicine, 7(1), 237. https://doi.org/10.1038/s41746-024-01232-3

Agung, A., Hafrida, H., & Erwin, E. (2022). Pencegahan Kejahatan Terhadap Cybercrime. PAMPAS: Journal of Criminal Law, 3(2 SE-Articles), 212–222. https://doi.org/10.22437/pampas.v3i2.23367

Alanazi, S., & Asif, S. (2024). Exploring deepfake technology: creation, consequences and countermeasures. Human-Intelligent Systems Integration, 6(1), 49–60. https://doi.org/10.1007/s42454-024-00054-8

Aurelia, C. N., Tanaya, V., Sugianto, F., & Yamamoto, A. (2025). Enhancing Fair Use in Protecting Appropriated Artworks: A Comparative Analysis of Safeguarding Indonesian Copyright Law. Lex Scientia Law Review, 9(1 SE-Research Articles), 1181–1222. https://doi.org/10.15294/lslr.v9i1.20570

Buffett Institute for Global Affairs. (2023). The Rise of Artificial Intelligence and Deepfakes. https://buffett.northwestern.edu/documents/buffett-brief_the-rise-of-ai-and-deepfake-technology.pdf

Cancela-Outeda, C. (2024). The EU's AI act: A framework for collaborative governance. Internet of Things, 27, 101291. https://doi.org/10.1016/j.iot.2024.101291

CATAHU Komnas Perempuan. (2023). CATAHU 2020 Komnas Perempuan: Lembar Fakta dan Poin Kunci (5 Maret 2021). https://komnasperempuan.go.id/siaran-pers-detail/catahu-2020-komnas-perempuan-lembar-fakta-dan-poin-kunci-5-maret-2021

Chairani, M. A., Pradhana, A. P., & Purnama, T. Y. (2022). The Urgency Of Developing Law As A Legal Basis For The Implementation Of Artificial Intelligence In Indonesia. Law and Justice, 7(1), 35–45. https://doi.org/10.23917/laj.v7i1.760

de Vries, K. (2020). You never fake alone. Creative AI in action. Information, Communication & Society, 23(14), 2110–2127. https://doi.org/10.1080/1369118X.2020.1754877

Edwards, B. (2023). Among AI dangers, deepfakes worry Microsoft president most - Ars Technica. https://arstechnica.com/information-technology/2023/05/microsoft-president-declares-deepfakes-biggest-ai-concern/

European Commission. (2022). The EU's Digital Services Act. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

European Parliament. (2023). EU AI Act: Final Text.

Isnawan, F. (2024). Deepfake Pornography: How Criminal Liability of Perpetrators in the Indonesian Criminal Law Framework. Jurnal Magister Hukum Udayana, 13, 745–771. https://doi.org/10.24843/JMHU.2024.v13.i03.p15

Jacobsen, B. N., & Simpson, J. (2024). The tensions of deepfakes. Information, Communication & Society, 27(6), 1095–1109. https://doi.org/10.1080/1369118X.2023.2234980

Ji, S. (2025). #MeToo in an AI-generated deepfake sexual violence era in South Korea. Women's Studies International Forum, 112, 103146. https://doi.org/10.1016/j.wsif.2025.103146

Judijanto, L., Utama, A. S., & Setiyawan, H. (2025). Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia. The Easta Journal Law and Human Rights, 3(02 SE-Articles), 101–109. https://doi.org/10.58812/eslhr.v3i02.470

Kasita, I. D. (2022). Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19. Jurnal Wanita Dan Keluarga, 3(1 SE-Articles). https://doi.org/10.22146/jwk.5202

Kusche, I. (2024). Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk. Journal of Risk Research, 1–14. https://doi.org/10.1080/13669877.2024.2350720

Momeni, M. (2024). Artificial Intelligence and Political Deepfakes: Shaping Citizen Perceptions Through Misinformation. Journal of Creative Communications, 20(1), 41–56. https://doi.org/10.1177/09732586241277335

Nizza, U. (2024). Assessing the Impact of the European AI Act on Innovation Dynamics: Insights from Artificial Intelligences. Fourth Annual Empirical Research Conference on Standardization. https://www.nytimes.com/2023/05/30/technology/ai-threat-warning.html

Ranjan, R., & Gulati, J. (2024). Deep Fake Porn : Duplicity And Dystopia. In Law In The Age Of Disruption-Understanding The Impact Of Technology (pp. 110–116). Lex Asisto Media and Publication.

Rezon, A., Montolalu, Y., Kenuwiarja, H., & Sugianto, F. (2025). Studi Komparasi Hak Cipta Atas Proses Data Scrapping AI di Indonesia, Uni Eropa, dan Amerika. Anthology: Inside Intellectual Property Rights, 3(1 SE-Articles), 243–265. https://ojs.uph.edu/index.php/Anthology/article/view/9815

Umbach, R., Henry, N., Beard, G. F., & Berryessa, C. M. (2024). Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries. Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3613904.3642382

Vecchietti, G., Liyanaarachchi, G., & Viglia, G. (2025). Managing deepfakes with artificial intelligence: Introducing the business privacy calculus. Journal of Business Research, 186, 115010. https://doi.org/10.1016/j.jbusres.2024.115010