

Deepfake Porn And Victim Protection: Legal Challenges In The Era Of Technological Disruption Within The Framework Of The SDGs

Evi Yanti¹, Heni Susanti², Yusra Mizaa Md Isa³.

¹² Faculty Of Law, Universitas Islam Riau
email: eviyanti1996@law.uir.ac.id, heni@law.uir.ac.id.

³ University Utama Malaysia

Abstract

The development of generative artificial intelligence technology has given birth to the phenomenon of deepfake porn that allows the creation of synthetic sexual content with a high resemblance to identity without the consent of the represented subject. This phenomenon creates a crisis of authenticity to the identity and self-representation of victims and presents new challenges for the legal protection system. This study aims to analyze deepfake porn as a form of technological disruption that has an epistemic and ontological impact, evaluate the form of legal protection for victims within the framework of Indonesian laws and regulations, and formulate the need for norm reformulation based on the principles of the Sustainable Development Goals (SDGs). The research method used is normative legal research with conceptual, legislative, and philosophical approaches to knowledge, through an analysis of the Sexual Violence Crime Law and regulations related to the digital space. The results of the study show that deepfake porn is not only a violation of digital law, but also a visual truth crisis that undermines the integrity of the victim's identity. The existing legal framework has provided a basis for protection, but it still contains normative gaps related to the synthetic character of content and the responsibilities of the technology ecosystem. The reformulation of norms is necessary through explicit recognition of digital sexual manipulation, rapid removal mechanisms, victim recovery, and expanded platform liability. In the discussion, the protection of victims of deepfake porn is placed within the framework of the SDGs, especially the goals of gender equality and strengthening justice and effective institutions, so that legal protection is positioned as part of the development of digital justice that is oriented towards human dignity.

Keywords: *Deepfake pornography; victim protection; digital gender-based violence; regulatory reform; SDGs framework;*

BACKGROUND

Information and communication technology has changed the behavior of society and civilization globally. In addition, the development of information technology has caused the world to be *borderless* and caused social changes that are significantly taking place so quickly.¹ Information technology is currently a double-edged sword, because in addition to

contributing to the improvement of human welfare, progress and civilization, it is also an effective means of unlawful acts, such as defamation, decency, gambling, threats, destruction and terror which are all known as *cyber crime*.²

In the midst of the increasing reach of the internet, the sophistication of the development and spread of information technology, and the popularity of the use of

¹ Ahmad M. Ramli, *Cyberlaw and IPR in the Indonesian Legal System*, Third Edition (Bandung: Refika Aditama, 2010).

² Abdul Wahid & Mohammad Labib, *Cybercrime* (Bandung: Refika Aditama, 2005).

social media, have presented new forms of criminal acts.³ Sexual violence can happen anytime and anywhere, including on the internet. Online gender-based violence (KBGO) is a form of violence that is carried out and facilitated by the internet medium. *The Association of Progressive Communication* (APC) defines GBV as a form of gender-based violence that is partially or entirely exacerbated by information and communication technologies such as mobile phones, the internet, social media platforms, and email.⁴ SAFENet then also formulated KBGO as an act of violence that intends to harass gender and sexuality facilitated by technology.⁵

KBGO is a form of violence that is basically very close to people's lives, especially during the COVID-19 pandemic which forces everyone to meet and meet face-to-face virtually. Women are more vulnerable to becoming victims of KBGO

than men. A study by the *United Nations Entity for Gender Equality and The Empowerment of Women* (UN Women) stated that during the COVID-19 pandemic in France there were 15% of women who experienced sexual harassment cyberly, in Pakistan it was stated that 40% of women had received some form of harassment when using the internet.⁶ In Indonesia itself, it is mentioned in the 2020 Komnas Perempuan Year-End Notes (Catahu) which explains the increase in reported KBGO acts.⁷ From 2018, reports of KBGO actions increased to reach 510 cases of KBGO in 2020. Then in 2021 the data recorded related to KBGO amounted to 1721 cases, in 2022 it rose to 1697 cases, and in 2023 it amounted to 1272 cases.⁸ It is undeniable that there are still many cases that are not reported to the authorities related to KBGO, both female and male victims, which are based on the concern of victims to report this because of fear of the possibility of criminalization using the Criminal Code

³ Ellen Kusuma and Nenden Sekar Arum, 'Understanding and Responding to Online Gender-Based Violence - Safa Net (Awas KBGO)', Safenet, 2020 <<https://awaskbgo.id/wp-content/uploads/2020/11/panduan-kbgo-v3.pdf>>.

⁴ Association for Progressive Communications (APC), "Online Gender-Based Violence: A Submission from the Association for Progressive Communications to the United Nations Special Rapporteur on Violence against Women, Its Causes and Consequences", Article, 2017, 3.

⁵ Fadillah Adkiras, Fatma Reza Zubarita, and Zihan Tasha Maharani Fauzi, 'The Construction of Online Gender-Based Violence Arrangements in Indonesia', *Jurnal Lex Renaissance*, 6.4 (2021), 781–98 <<https://doi.org/10.20885/jlr.vol6.iss4.art10>>.

⁶ UN Women, "UN Women, 'Online and ICT Facilitated Violence Against Women and Girls During COVID-19', <https://www.unwomen.org/-/Media/Headquarters/Attachments/Sections/Library/Publications/2020/Briefonline-and-ict-facilitated-violence-against-women-and-girls-during-co-19>, n.d.

⁷ <https://www.kemnpppa.go.id/page/view/NTQzMw==>. Accessed on March 2, 2025, at 11.45 WIB.

⁸ <https://www.tempo.co/hukum/jumlah-kasus-kekerasan-berbasis-gender-online-naik--52168>. It will be accessed on March 2, 2025, at 11.45 WIB.

and the ITE Law. Especially if the victim is involved in creating intimate content digitally. KBGO acts in the scope of online games are known to occur when live broadcasts or live streams are carried out by pro players or content creators gamers on various *live streaming platforms* such as NimoTV, Tweak, Youtube, and so on.⁹

KBGO is regulated in the Sexual Violence Crime Law (TPKS Law) which is regulated in Article 14 paragraph (1) of Law Number 12 of 2022 concerning the Crime of Sexual Violence which reads:

"(1) Every person who is without the right to:

- a. making recordings and/or taking sexually charged photographs or screenshots against the will or without the consent of the person to whom the recording is the object of the recording or the images or screenshots;
- b. transmitting electronic information and/or electronic documents of sexual content beyond the will of the recipient aimed at sexual desire; and/or

- c. stalking and/or tracking using an electronic system against a person who is the object of information/electronic documents for sexual purposes, convicted of committing electronic-based sexual violence, with a maximum prison sentence of 4 (four) years and/or a maximum fine of Rp200,000,000.00 (two hundred million rupiah)".

Prior to the existence of the TPKS Law, the regulation to ensnare KBGO perpetrators using the Information and Electronic Transactions Law No. 19 of 2016 as amended to Law No. 1 of 2024 in Article 27 paragraph (1) of Law Number on Information and Electronic Transactions reads:

"Every Person deliberately and without the right to broadcast, perform, distribute, transmit, and/or make accessible Electronic Information and/or Electronic Documents that have content that violates morality to be known to the public".

Furthermore, related to the enforcement of the law regarding KBGO after the enactment of the Sexual Violence

⁹ Nursyafia, Muhamad Amirulloh, and Helitha Novianty Muchtar, 'Online Gender-Based Violence (KBGO) in Online Games According to Law in

Indonesia and Comparison with Other Countries', *Tambusai Education Journal*, 7 (2023), 2046.

Crime Law in 2022 and now in 2025, it has been running for about 3 years, it is still very ineffective. Based on data obtained from LBH in Jakarta throughout 2023, there are 1141 complaints of cases against women in Greater Jakarta, of these cases related to KBGO dominating up to 250 cases out of 497 complaints about sexual violence. In terms of threatening the dissemination of sexual images/photos, 111 cases and the dissemination of intimate content without consensuality were 77 cases. The rise of KBGO cases that continue to occur and are not handled properly is due to the fact that in the criminal law on sexual violence regarding KBGO, there are only 3 (three) forms, namely the first recording, the second transmission and the last stalking, then many other KBGO cases, which are not regulated in the information and electronic transaction law and are also not accommodated in the sexual violence crime law.¹⁰ There are several types of KBGO that have not been regulated in various laws and regulations in Indonesia, one of which is related to *deepfakes* (photo manipulation), threats of rape and the dissemination of information through online loans, the dissemination of personal information (including photos, or the

creation of fake accounts by making slander in the form of an "open BO" narrative, a term that refers to sex workers who offer their services through the internet.

In the landscape of Online Gender-Based Violence (KBGO), various forms of digital attacks such as the dissemination of intimate content without consent, hacking, manipulation of personal data, and online-based harassment have become part of the social reality that increasingly threatens human dignity. However, the advent of generative artificial intelligence technology gave birth to a new form of violence that was much more problematic and shook the very foundation of the concept of identity, namely *deepfake porn*. Unlike other forms of KBGO that rely on original content, *deepfake porn* works through algorithmic engineering that blurs the line between fact and fabrication, between the victim's body and the digital representations imposed on it. The presence of the victim's face in a body that does not belong to him not only takes away the right to privacy and honor, but also creates a *crisis of authenticity*, because the victim is forced to live in a double reality, his own reality and the artificial reality created by technology. This is what makes deepfake porn not just a variation of KBGO, but a new epistemic

¹⁰ Ida Rachmawati and others, 'Education for Children in Efforts to Prevent Sexual Crimes with Child Grooming Mode', RESWARA: Journal of

Community Service, 4.1 (2023), 332–39 <<https://doi.org/10.46576/rjpkkm.v4i1.2399>>.

and ontological phenomenon that demands a more in-depth analytical approach. Therefore, this discussion focuses specifically on *deepfake porn* as a form of digital violence that requires adaptive legal protection as well as a philosophical understanding that is able to explain how technology can confuse the definition of reality, identity, and truth in the digital age.¹¹

In this article, the author focuses on discussing *Deepfake porn* which is a form of KBGO which from year to year the number of victims continues to increase. *Deepfake porn* is AI-generated pornographic content that inserts a person's face into video pornography without their consent. This technique uses deep learning technology to produce visuals that appear very realistic, often targeting victims without notice or consent, and especially affecting women.¹² In addition, SAFEnet (*Southeast Asia Freedom of Expression Network*) reported that throughout 2024, there were 40 cases specifically related to the use of morphing and *deepfake technology* to create pornographic content without the victim's consent. This number is a significant increase from the dozens of

cases recorded in previous years. This fact reflects that although the phenomenon of *deepfake porn* is still relatively new in Indonesia, the potential threat and escalation continue to grow as access and use of artificial intelligence technology increases freely in the digital space.

The following author presents related to *Deepfake porn* data as follows:

Table 1 Data related to the increase in *Deepfake cases* at the international level

Year	Location	Number of Cases	Remarks
2021-2023	South Korea	523 Cases	60.% of adolescent fatalities; 3.4× increase (koreaboo.com)
2023-2022	Global	+464 % video	98% pornography, 99% female victims
March	World	Approximately 4000 celebrities	100 Million

¹¹ Substantive Justice and International Journal, "Deepfakes and Victimology : Exploring the Impact of Digital Manipulation on Victims" 8, no. 1 (2025): 1–12, <https://doi.org/10.56087/substantivejustice.v8i1.306>.

¹² Dr. Rituparna Bhattacharjee and Ms. Muskan Sharma, "Deepfake & Pornography: The Coming Crisis of Privacy and Consent," *South Eastern European Journal of Public Health*, February 21, 2025, 1196–1213, <https://doi.org/10.70135/seejph.vi.4885>.

2024			viewers/3 months
------	--	--	------------------

In the last three years, cases of *deepfake* pornography have increased significantly globally. In South Korea, there were 523 reports of *deepfake porn* crimes received by the police from 2021 to 2023. Of these, 59.8% or 315 victims were teenagers, showing a tendency that young age groups are the main targets of this crime. The number of cases increased sharply from 53 cases in 2021 to 181 cases in 2023, an increase of almost 3.4 times. Globally, a report from The Guardian in March 2024 noted that around 4,000 celebrities have been victims of deepfake pornography by five major websites, with total views reaching more than 100 million times in just three months. Meanwhile, another report shows that in 2023 there was a 464% spike in the number of deepfake porn videos compared to the previous year, where 98% of all *deepfake* content was pornographic and 99% of the victims were women. These findings show that deepfake porn is now an increasingly massive, systemic, and gender-biased form of digital crime in the global realm. Furthermore, for data on Deepfake cases that occurred in Indonesia. **Table 2** Data related to the increase in *Deepfake cases* in Indonesia

Year	Source	Recorded Cases
2022	Komnas Perempuan (KBGO pornography)	281 reports of cyber pornography cases (300% & increase since 2018)
2023		(kumparan.com)
2024	SAFEnet (KBGO morphing/deepfake porn)	40 cases, a significant increase from the dozen cases the previous year

In Indonesia, cases of *deepfake* pornography have begun to show a significant increase in the last three years, although not as much as in other countries. Based on the Komnas Perempuan report from 2022 to 2023, there were at least 281 complaints related to digital pornography content in the category of online gender-based violence (KBGO). This number increased by 300% compared to 2018 data, showing that digital sexual crimes including the use of technology such as *deepfakes* are increasingly alarming. Many people fall victim to deepfake porn, where their faces are used in porn videos without their permission. This can damage the

reputation and personal life of the victim, and can cause serious psychological repercussions. In addition, deepfake porn can also be used to create fake porn videos of famous figures or celebrities, which can damage their reputation and cause unexpected damage. This can also trigger legal and security issues, as such fake porn videos can be widely spread on the internet and are difficult to remove.¹³

In recent years, *the deepfake* phenomenon has created a significant wave of excitement and concern, reaching a wide range of audiences, from prominent figures to global political figures. In Indonesia, the famous actress Nagita Slavina is suspected of being a victim of a deepfake video that tarnished her good name. A short video features a woman with a face that looks very similar to her in an inappropriate scene. The case is similar to a series of incidents involving prominent figures former US Presidents Donald Trump and Barack Obama, as well as Meta founder Mark Zuckerberg, who have been the subject of outrageous deepfake videos, with voice and facial manipulation that confused viewers as to the authenticity of the videos. In fact, world leaders such as Russian

President Vladimir Putin and North Korean President Kim Jong-un have not escaped the reach of this phenomenon, being targeted by deep-fake content that creates false narratives and images about them. In April 2018, a disturbing video quickly spread on WhatsApp, an instant messaging platform prevalent around the world. Captured as if through a CCTV lens, the video depicts a group of children engaged in a game of street cricket. Suddenly, the scene turned alarming when two men on motorcycles appeared, snatched one of the smaller children, and then quickly left. This footage of the alleged "kidnapping" sparked immense confusion and fear, triggering a period of mob violence that tragically lasted eight weeks and resulted in the deaths of at least nine innocent people. This incident highlights the dangerous potential of viral misinformation to incite violence and chaos in the real world.¹⁴ This phenomenon confirms that deepfakes have become a powerful tool in the spread of disinformation and digital manipulation, which can have a major and detrimental impact on individuals and society at large.

The birth of Law No. 12 of 2022 concerning the Crime of Sexual Violence

¹³ Mahfudz Ikhsan Mahardika, 'Journal of the Faculty of Law Unsrat Lex Privatum Vol.14 N0 5 Jan 2025', Journal of the Faculty of Law Unsrat Lex Privatum, 14.5 (2025), 1–8.

¹⁴ Cristian Vaccari and Andrew Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News," 2020, <https://doi.org/10.1177/2056305120903408>.

provides a breath of fresh air for women's protection. The state finally came forward and showed its partiality to victims of sexual violence. The TPKS Law is a law that regulates the Crime of Sexual Violence. Sexual Violence is a form of violence and treatment that degrades the degree of human dignity that is contrary to divine and human values, and that disturbs the security and peace of society. Regulations related to Electronic-Based Sexual Violence Crimes, namely *Deepfake* crimes, are not specifically regulated in Law Number 12 of 2022 concerning Sexual Violence.¹⁵ The regulation has not optimally regulated the protection and enforcement of the law that is preventive and representative to the maximum, especially for women who are victims. Therefore, the author is interested in discussing how to protect women victims of violence and law enforcement in the *Artificial intelligence* (AI) Deepfake crime based on Law Number 12 of 2022 concerning the Crime of Sexual Violence.

It is at this point that the approach based on the Sustainable Development Goals (SDGs) framework becomes relevant

as an evaluative and normative foundation.¹⁶ Using the principles of protection of human dignity, equality, and access to justice as parameters, the analysis can be directed to assess whether existing legal arrangements have been adequate in responding to the risk of digital identity manipulation and victim harm in the technology space.¹⁷ The SDGs framework, in particular the goals of gender equality and the strengthening of effective justice and institutions, provide substantive measures to assess the adequacy of norms, the effectiveness of victim protection, and the responsibilities of actors in the digital ecosystem. Through this approach, the reformulation of legal articles or policies is not only driven by regulatory technical needs, but also by a commitment to human protection and sustainable digital justice. Thus, the law does not stop at the caustic response to technological phenomena, but rather develops systematically, victim-oriented, and in line with the principles of sustainable development. Based on the facts described above, the author is interested in discussing **"DEEPFAKE**

¹⁵ Memei Apriana and Any Nugroho, "Legal Protection for Women Victims of the Crime of Artificial Intelligence (Ai) Deepfake Based on Law Number 12 of 2022 Concerning Criminal Actions of Sexual Violence," *Journal of Social and Economics Research* 7, no. 1 (2025): 57–75, <https://idm.or.id/JSER/index.php/JSER>.

¹⁶ Alfian Ma et al., "Social Sciences & Humanities Open Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital

Platforms : A Systematic Literature Review," *Social Sciences & Humanities Open* 12, no. January (2025): 101882, <https://doi.org/10.1016/j.ssaho.2025.101882>.

¹⁷ Andrea Gracia-zomeño et al., "Preventing Harassment and Gender-Based Violence in Online Videogames Through Education," *Social Sciences* 14, no. 297 (2025): 1–18, <https://doi.org/https://doi.org/10.3390/socsci14050297>.

PORN AND VICTIM PROTECTION: LEGAL CHALLENGES IN THE ERA OF TECHNOLOGICAL DISRUPTION WITHIN THE FRAMEWORK OF THE SDGS".

FORMULATION OF THE PROBLEM

The main problems in this study are as follows:

1. How does the phenomenon of deepfake porn as a form of technological disruption create a crisis of authenticity to the identity and self-representation of the victim, as well as its implications for the purpose of protecting human dignity within the framework of the SDGs?
2. What is the form of legal protection for *victims of deepfake porn* within the framework of Indonesian laws and regulations, especially Law No. 12 of 2022 concerning the Crime of Sexual Violence, as well as what are the normative gaps that arise and require reformulation?

METHODE

This study uses a normative legal research method with a legislative approach,¹⁸ a conceptual approach, and a Sustainable Development Goals (SDGs) framework approach as evaluative parameters for victim protection.¹⁹ The legislative approach is used to analyze relevant positive legal provisions, specifically Law Number 12 of 2022 concerning Criminal Acts of Sexual Violence and regulations related to digital space and victim protection.²⁰ While the conceptual approach is used to examine the concepts of deepfake porn, technological disruption, online gender-based violence, and legal protection for victims. The SDGs framework, particularly the goals of gender equality and strengthening justice and effective institutions, is used as a normative benchmark to assess the adequacy of regulations and formulate the need for norm reformulation. The type of data used is secondary data in the form of primary, secondary, and tertiary legal materials obtained through literature studies. Then, it is analyzed qualitatively using systematic interpretation and evaluative techniques to produce arguments regarding a legal protection model for deepfake porn victims

¹⁸ Peter Mahmud Marzuki, *Penelitian Hukum*, Cetakan ke (Jakarta: Divisi Kencana Prenada Media Group, 2021).

¹⁹ M. Zainuddin, *Pemahaman Metode Penelitian Hukum (Pengertian, Paradigma, Dan Susunan Pembentukan)*. (Yogyakarta: CV.Istana Agency, 2019).

²⁰ Sidi Ahyar Wiraguna, "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia," *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (2024), <https://doi.org/10.59818/jps.v3i3.1390>.

that is more adaptive to technological disruption.

RESULT AND DISCUSSION

1. The phenomenon of *deepfake porn* as a form of technological disruption creates a crisis of authenticity to the identity and self-representation of victims

Advances in information technology have a positive impact on making various aspects of human life easier. However, on the other hand, this development also poses new risks that are detrimental, one of which is through *Artificial Intelligence (AI) technology*, especially *deepfakes*. According to Marissa Koopman, Andrea Macarulla Rodriguez, and Zeno Geradts, *deepfake* algorithms allow users to realistically replace someone's face in a video with someone else's. This technology is used to falsify visual identities in photos or videos, so that the real actors in the media seem to be replaced by someone else. As the sophistication of this technology increases, the results of manipulation become increasingly difficult to distinguish from the original content. One of the negative impacts of *deepfakes* is the

emergence of *deepfake pornography*, which is categorized as a form of online gender-based violence, where the majority of victims are women.²¹ This phenomenon is often male-produced and targets women's bodies without consent. From a legal perspective, *deepfake pornography* includes forms of invasion of sexual privacy, non-consensual pornography, and visual-based sexual violence. The perpetrator takes control of the victim's body image, creating sexual representations without the victim's permission or knowledge. These actions not only violate ethical norms, but are also classified as criminal acts that include sexual harassment, theft of personal data, dissemination of false information, and digital manipulation.²²

The term technological disruption refers to a radical change that disrupts the old way of doing things and replaces it with a completely different new way. In the context of *deepfakes*, disruption occurs because generative AI technology is changing the paradigm of visual representation: what was originally thought to be a recording of reality can now be produced without reality itself. This

²¹ Asmak U I Hosnah Silvia Maharani Iskandar Putri, Nashwa Salsabila, 'Criminalization of the Use of Deepfakes in Fraud and Defamation: Legal Challenges and Solutions 6, No. 2 (2024): 83–90', "Journal of Legal Legalita, 6.2 (2024), 83–90 <<https://doi.org/doi:10.47637/legalita.v6i2.1453>>.

²² Rituparna Bhattacharjee & Muskan Sharma, "'Deepfake & Pornography: The Coming Crisis of Privacy and Consent,'" *South Eastern European Journal of Public Health* XXVI (2025), <https://doi.org/10.70135/seejph.vi.488>.

technology removes the prerequisite for the existence of the physical body in producing a real-looking image or video. Thus, deepfakes are no longer just an innovation, but an epistemic disorder that makes humans no longer able to rely on their visual senses to judge the truth.²³

This disruption has serious consequences for the victims. In the digital world, visual representations are often more powerful than reality. Authenticity is no longer a requirement to be trusted; The important thing is *visual consistency* which seems natural. Therefore, deepfake porn takes away one's control over one's self-image (*self-image*) and forced him to face a new reality he never chose. This is the root of the authenticity crisis: humans are no longer the sole owners of their bodies and faces in the digital space. Epistemology as a branch of philosophy of science discusses how humans acquire and validate knowledge. In the classical tradition, the visual media of photos and videos is seen as empirical evidence that approaches objective truth because it is considered to capture reality as it is. However, the emergence of deepfakes shifted this position.

Deepfake porn suggests that visuals can no longer be used as a trustworthy

epistemic basis. Videos that appear to be real can be completely fake, created without the victim's involvement, and produced by algorithms with no moral boundaries. In the tradition of the philosophy of science, especially epistemology, visual evidence has always been positioned as one of the *independen evidences* Powerful, images and videos are considered the most authentic representations of reality. Since the era of positivism, empirical observation has been believed to be the basis for the validity of knowledge. However, the emergence of technology *deepfake* disrupts these fundamental assumptions. With AI's ability to mimic faces, voices, body movements, and expressions almost perfectly, visual evidence can no longer be relied upon as a "mirror of reality". This technology not only blurs the line between fact and engineering, but also gives birth to what media philosophers call *epistemic collapse*: the collapse of the human ability to distinguish empirical reality from digital constructions.

This collapse is clearly visible in context *deepfake porn*, a form of Online Gender-Based Violence that manipulates a person's facial image to be attached to the body in pornographic videos. In Indonesia,

²³ Bobby Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy ,

Democracy , and National Security," 2019, 1753–1820.

a number of cases prove how fragile visual evidence can be when it is reproduced as a tool of violence. The case of the "SMAN 11 Semarang Scandal" in 2025, for example, is a real example of how a female student becomes a victim of making pornographic photos and videos that are completely fake, but seem very convincing. The perpetrator uses the victim's face and combines it with the body in an explicit sexual pose, so that the general public has difficulty distinguishing between real content and fake content. The epistemic impact is very serious: even if the victim objectively never engages in the act, false visual evidence creates a public perception that seems to be true, resulting in reputational damage and profound psychological trauma.

This epistemic shift can only be understood in its entirety when viewed from an ontological perspective. Jean Baudrillard explained that in the digital era, representation has entered a phase *hyperreality*, that is, when the simulation appears more real than reality itself. *Deepfake porn* is the most extreme form of *simulacrum*: a fake entity that replaces reality. Deepfake videos not only falsify the victim's face, but create another "identity" that the victim never does, but circulates and is treated as if it is true. These false

identities live as new ontological entities that have a real impact on the social life of the victim, suggesting that deepfakes create a dual reality of biological reality and digital reality that both affect a person's existence.²⁴

Within this framework, *deepfake porn* Collapse the autonomy of the digital body (*digital bodily autonomy*). If a person's physical body is protected by law, then their digital body is actually vulnerable to exploitation without limits. When the victim's face is attached to another body in a sexual context, what is lost is not only reputation, but also ontological sovereignty over the body and its identity. This phenomenon is in line with Donna Haraway's analysis of the body and identity as a commoditable construct in technological culture. This crisis of representation puts the victim in an unequal ontological state: he must coexist with a false digital identity that spreads uncontrollably

On a global scale, attacks *deepfake porn* even more massive. A number of world celebrities such as Taylor Swift, Scarlett Johansson, Emma Watson, and Billie Eilish have become victims of AI-based pornography manipulation. In 2024, Taylor Swift became the victim of the

²⁴ Seongcheol. Wang, Soyoung & Kim, "Users' Emotional and Behavioral Responses to Deepfake Videos of K-Pop Idols.," *Computers in Human*

Behavior, 2024, <https://doi.org/10.1016/j.chb.2022.107305>.

spread of thousands of sexual deepfake images on X (Twitter) that went viral around the world in a matter of hours. Although the entire image is fake, its reputational and emotional impact is enormous, showing that even public figures with legal and financial power cannot fully protect their authenticity in the digital age. Scarlett Johansson even stated publicly that "everyone is now living with a digital identity that can be stolen at any time," asserting the authenticity crisis as a universal issue, not just a technical incident.

Deepfake Porn specifically shows how generative technology is used to create a sexual representation of a person without consent and without the victim's participation. The victim's digital body is used as an object of exploitation, while his personal identity remains attached to the content by public perception. This is where the crisis of authenticity occurs: representation no longer comes from reality, but from simulations that are then treated as if they were real. Victims face multiple reputational, psychological, social, and even professional losses even though the events represented never actually occurred. This shows that in the

digital ecosystem, social impact is no longer dependent entirely on empirical reality, but rather on the credibility of the representations that circulate.²⁵

Within the framework of global development, the Sustainable Development Goals (SDGs) place the protection of human dignity, equality, and justice as the main foundations of modern social governance and law. Among these goals, SDGs 5 focuses on the realization of gender equality and the elimination of all forms of violence, exploitation, and discrimination against women and vulnerable groups, both in the physical and digital spaces.²⁶ This goal is not only oriented towards increasing participation, but also on ensuring safety, bodily autonomy, and personal integrity from various forms of gender-based violence. Meanwhile, SDGs 16 focuses on building a peaceful and inclusive society, providing access to justice for all, and strengthening effective, accountable, and adaptive institutions. In this context, the legal and institutional systems are required to be able to respond to new forms of risks and violations that arise due to technological developments, including crimes and abuses based on digital

²⁵ Olatz Lopez-fernandez, A Jess Williams, and Daria J Kuss, "Measuring Female Gaming : Gamer Profile , Predictors , Prevalence , and Characteristics From Psychological and Gender Perspectives" 10, no. April (2019), <https://doi.org/10.3389/fpsyg.2019.00898>.

²⁶ Dini Rakhmawati et al., "824 Digital Footprint of Violence: Bibliometric Analysis of Online Gender-Based Violence with Vosviewer and Scopus" 10, no. 01 (2026): 824–33, <https://doi.org/10.31316/g-couns.v10i01.8737>.

manipulation. Both objectives provide a relevant normative framework for assessing the extent to which a technological phenomenon impacts victim protection, justice, and human dignity

When associated with the Sustainable Development Goals (SDGs) framework, this phenomenon has direct relevance to the goals of gender equality and the strengthening of justice and effective institutions. The goal of gender equality in the SDGs emphasizes the elimination of all forms of violence and exploitation against women and girls, including technology-based violence. Deepfake porn in global practice has been proven to dominantly target women, female public figures, journalists, activists, and individuals in socially vulnerable positions. Sexual manipulation based on digital imagery without consent is a form of digital gender-based violence because it uses women's bodies as sexual objects without autonomy. Thus, the practice of deepfake porn is directly contrary to the principles of protecting bodily integrity, dignity, and personal autonomy that are at the core of the goal of gender equality.

Furthermore, the goal of gender equality in the framework of sustainable

development speaks not only about access and participation, but also about security and freedom from violence. An unsafe digital environment due to the abuse of manipulative technology creates a silencing effect, where victims or potential victims withdraw from digital public spaces for fear of being attacked through visual sexual engineering. This impact reduces women's participation in information spaces, public discourse, and digital-based professional activities. Therefore, the protection of victims of deepfake porn is not only an individual issue, but also related to the creation of a safe and equal digital space, as demanded in the principles of global gender equality.²⁷

On the other hand, the sustainable development goals also emphasize the importance of access to justice and institutions that are effective, accountable, and adaptive. In this context, the spread of deepfake porn tests the capacity of the legal and institutional systems to respond to new forms of harm that do not fully fit into the category of conventional crimes. Issues of proof, cross-jurisdictional identification of perpetrators, digital platform engagement, and the speed of content dissemination create structural challenges for law

²⁷ Anupama Gupta Ved Dilip Beloskar, Arunima Halder, "Gender Equality and Women's Empowerment: A Bibliometric Review of the Literature on SDG 5 through the Management

Lens," *Journal of Business Research*, 172 (2024), <https://doi.org/https://doi.org/10.1016/j.jbusres.2023.114442>.

enforcement. If legal institutions are unable to adapt to forms of technological disruption, then there is a gap in victim protection. This is contrary to the principle of building responsive and effective institutions, which demand the ability of the legal system to adapt to the risks of new technologies.

Justice in the digital context is no longer enough to be interpreted as punishing perpetrators, but also includes victim recovery, content removal, spread control, and prevention of repeat losses. This approach is in line with the orientation of institutional development that is not only repressive, but also protective and preventive. Thus, the response to deepfake porn needs to be placed within the framework of strengthening digital governance, platform accountability, and rapid and effective victim protection mechanisms. This shows that the problem of deepfake porn is at the intersection of technological ethics, human rights protection, and the development of justice institutions.

In addition, the sustainable development goals in the fields of innovation and infrastructure also emphasize that technological progress must

be in harmony with human values. Innovation is not seen as neutral, but must be managed so as not to produce systemic social disadvantages. Deepfake porn is an example of how technological innovations without normative safeguards can turn into an instrument of exploitation. Therefore, the development and utilization of artificial intelligence technology needs to be accompanied by an ethical, regulatory, and social responsibility framework. In this perspective, victim protection is not an obstacle to innovation, but rather a condition for sustainable innovation.²⁸

Based on the overall analysis, deepfake porn as a product of technological disruption must be understood as an authenticity crisis that has a direct impact on identity, dignity, and the structure of social knowledge. This phenomenon demands an expansion of legal approaches towards epistemic, ontological, and ethical analysis, while placing victim protection as part of a commitment to sustainable human development. By linking it to the principles of gender equality, justice, and adaptive institutions, the discussion of deepfake porn has moved from just an issue of digital crime to a question of digital justice and the

²⁸ Syarifuddin. Suardi*, Yumriani, Herdianty Ramlan, Indah Ainun Mutiara, Firdaus, Rahmat Nur, Hasruddin Nur, Syahban Nur, Nur Riswandy Marsuki, Fitri Yanty Muchtar, 'Gender Equality in

Higher Education: Access, Participation, and Academic Leadership', *Journal Of Education Sciences*, 9.4 (2025), 2038–48.

protection of human dignity in the global technological order.

2. What are the forms of legal protection for victims of deepfake porn in Indonesian laws and regulations, especially Law Number 12 of 2022 concerning the Crime of Sexual Violence, as well as normative gaps that require reformulation in the perspective of victim protection and the principles of the SDGs?

In Indonesia, although there is no specific regulation that explicitly states *deepfake* As a criminal offense, several articles in existing laws and regulations can be used to ensnare the perpetrators of spreading deepfake content. However, with the rapid development of technology, there are major challenges in law enforcement of cases *deepfake*, both in the aspects of proof and punishment. In the context of Indonesian criminal law, the dissemination of deepfake content can be categorized as a criminal act of information and electronic transactions (ITE), which is regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). Article 27 paragraph (3) of the ITE Law states that:

"Everyone deliberately and without rights distributes and/or transmits

and/or makes accessible electronic information and/or electronic documents that have insulting and/or defamatory content".

In addition, *deepfake porn* which contains pornographic elements can be sanctioned under Law Number 44 of 2008 concerning Pornography. Article 29 of the Pornography Law states that:

"Every person who produces, makes, reproduces, reproduces, disseminates, broadcasts, imports, exports, offers, sells, rents, or provides pornography as referred to in Article 4 paragraph (1) shall be sentenced to imprisonment for a minimum of 6 months and a maximum of 12 years and/or a fine of at least Rp250 million and a maximum of Rp6 billion".

In context *deepfake porn*, this regulation can be applied if someone creates and distributes deepfake-based pornographic content by manipulating the victim's face into videos or images that are explicit. Cases like this have begun to occur in various countries, including Indonesia, and are often used as a tool for extortion or revenge against victims. In addition to the ITE Law and the Pornography Law, the dissemination of *deepfake porn* It can also be associated with the criminal acts of forgery and defamation in the Criminal

Code (KUHP). Article 263 of the Criminal Code states that:

"Whoever forges or forges a letter that may give rise to a right, obligation, or release of a debt, or that is intended as evidence of a thing with the intention of using or instructing another person to use the letter as if its contents were true and not forged, shall be punished with imprisonment for a maximum of six years".

Although this article focuses more on forgery of written documents, the concept of forgery in criminal law can be extended to include digital manipulation, including *deepfake porn*. Therefore, if someone creates and uses *deepfake porn* With the intention of deceiving or harming others, this article can be used as a legal basis in ensnaring the perpetrator. However, the application of the law to the case *deepfake porn* in Indonesia still faces various obstacles.²⁹ Furthermore, Deepfake Porn is also regulated in Article 14 of Law Number 12 of 2022 concerning the Crime of Sexual Violence (TPKS Law):

Article 14

- (1) Any Person who without the right: a. makes a recording and/or takes a sexually charged photograph or screenshot against the will or without

the consent of the person who is the object of the recording or the image or screenshot; b. transmit electronic information and/or electronic documents with sexual content beyond the will of the recipient aimed at sexual desire; and/or c. stalking and/or tracking using an electronic system against a person who is the object of information/electronic documents for sexual purposes, convicted of committing electronic-based sexual violence, with a maximum prison sentence of 4 (four) years and/or a maximum fine of Rp200,000,000.00 (two hundred million rupiah).

- (2) In the event that the act as intended in paragraph (1) is committed with the intention of: a. to extort or threaten, coerce; or b. misleading and/or deceiving, a person to do, allow to be done, or not to do something, shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp300.000.000,00 (three hundred million rupiah).
- (3) Electronic-based sexual violence as intended in paragraph (1) is a complaint offense, unless the victim is a child or a person with a disability.
- (4) In the event that the act as intended in paragraph (1) letters a and b is done in the public interest or for the defense of oneself from the Crime of Sexual Violence, it shall not be punishable.
- (5) In the event that the victim of electronic-based sexual violence as intended in paragraph (1) letters a and

²⁹ King Tuasikal. Hendra Prayoga, 'The Spread of Deepfake Content as a Criminal Offense: A Critical Analysis of Law Enforcement and Public Protection

in Indonesia', Abdurrauf Law and Sharia, 1.2 (2024), 22–38.

b is a Child or Person with a Disability, the existence of the Victim's will or consent does not abolish the criminal charge.

After seeing how the Indonesian legal framework regulates the act of *Deepfake Porn* in various regulations such as the TPKS Law, ITE Law, and others provide a normative basis for ensnaring perpetrators and provide initial protection to victims *deepfake porn*, The discussion needs to be expanded to a more basic dimension, namely the protection of affected human values. Deepfake porn content not only destroys one's reputation in the public sphere, but also damages the value of dignity (*Dignity*), personal autonomy, and moral integrity which are the essence of human existence. When a person's identity can be engineered, falsified, and disseminated without control through AI technology, the damage that occurs is not only a legal loss, but also an axiological wound, that is, a disruption of the basic values inherent in humans as meaningful subjects. It is in this context that *right to be forgotten* ³⁰ It acquires its philosophical relevance: this right is not merely a legal device for the erasure of digital data, but is a normative statement that the individual has the right to determine a correct self-representation, free

from manipulation, and in harmony with his will and dignity.

Legal protection for victims of deepfake porn in the current Indonesian legal system relies on several regulatory regimes, especially Law Number 12 of 2022 concerning the Crime of Sexual Violence (TPKS Law), provisions regarding electronic information and transactions, and personal data protection. The TPKS Law provides an important foundation because it recognizes non-physical and technology-based forms of sexual violence, including the dissemination of sexual content without consent that attacks the dignity and integrity of the victim. In an impact-based approach to victimization, deepfake sexual manipulation can be interpreted as digital sexual violence because it causes real psychological, social, and reputational harm, even though the sexual events depicted never actually occurred.

However, the application of existing norms to deepfake porn cases still faces conceptual and operational limitations. Many of the formulations are still oriented towards material that is assumed to come from real events or actual documentation, while deepfake porn is a synthetic representation generated through

³⁰ Faqi Rawni Arndarnijariah, 'THE RIGHT TO BE FORGOTTEN AS A LAW ON THE PROTECTION OF PERSONAL DATA OF REVENGE PORN

VICTIMS', 8 (2024), 69–82
<<https://doi.org/10.24246/alethea.vol8.no1>>.

algorithmic engineering. This inconsistency has the potential to cause a debate about the fulfillment of the elements of delicacy, especially related to the object, intention, and relationship with the identity of the victim. In addition, the construction of legal accountability still focuses on the direct perpetrators, whereas in deepfake practices there is a broader chain of roles, including model makers, application providers, and distribution platforms that accelerate the spread of content. This regulatory vacuum regarding the responsibility of the digital ecosystem shows the need for a reformulation of norms that are more adaptive to the character of technological disruption.

Through the framework of the Sustainable Development Goals, especially the principles of gender equality and protection from violence, adequate legal protection for victims of deepfake porn must be oriented towards the protection of bodily integrity, identity, and personal dignity. This principle requires the state to not only prohibit the act, but also ensure the safety of victims from technology-based sexual exploitation. Therefore, the reformulation of legal protection needs to explicitly recognize synthetic sexual manipulation without consent as a form of

digital gender-based violence. This normative recognition is important to avoid interpretive loopholes and ensure that victims obtain protected status without being burdened with proof that the sexual event actually occurred.³¹

On the other hand, the principles of strengthening justice and effective institutions in the framework of sustainable development require that the legal system be able to provide a fast, accessible, and effective response to digital losses. In this context, the form of legal protection is not enough in the form of criminal threats, but must include an operational mechanism for victim protection. The reformulation of norms needs to contain at least four main forms of protection. First, preventive protection, in the form of an obligation for platforms and technology service providers to implement a system of detection, labeling, and restriction of the distribution of sexual synthetic content. Second, fast responsive protection, in the form of an accelerated takedown mechanism based on victim reports, without convoluted procedures that prolong losses. Third, victim recovery protection, which includes psychological rehabilitation, digital reputation recovery, and legal assistance, as well as the spirit of victim recovery in the

³¹ Sara Hajikazemi and Ilaria Rimondi, "Gender Equality Interventions in Project-Based Organizations : What Works , What Doesn ' t , and

Why," 2025,
<https://doi.org/10.1177/87569728251335301>.

TPKS Law. Fourth, ecosystem responsibility-based protection, i.e. the extension of the subject of legal liability not only to content creators, but also to parties who knowingly facilitate the dissemination and monetization of manipulative content.

SDGs-based reformulation also requires a victim-centered and not just offender-centered approach to protection. In the case of deepfake porn, the victim's losses often last longer than the criminal proceedings against the perpetrator. Therefore, norms need to guarantee victims' rights to control their digital identities, the right to be forgotten against manipulative content, and the right to cross-platform remediation. This approach is in line with the principles of institutional development that are oriented towards human protection and access to substantive justice, not just procedural justice.³²

Thus, within the framework of sustainable development, forms of legal protection for victims of deepfake porn should be formulated in an explicit, adaptive, and victim-based manner, including normative recognition of digital sexual identity manipulation, expanded legal responsibilities of the technology ecosystem, rapid removal mechanisms, and comprehensive recovery guarantees. This kind of reformulation not only strengthens

the adequacy of national norms, but also places the protection of victims of deepfake porn as part of the commitment to equality, protection from violence, and the construction of an effective and human dignity-oriented digital justice system.

CONCLUSION

The phenomenon of deepfake porn as a product of technological disruption shows that artificial intelligence-based visual manipulation has caused a serious crisis of authenticity to the identity and self-representation of victims, so that it can no longer be understood solely as a conventional criminal offense, but as an epistemic, ontological, and ethical issue that has a real impact on human dignity. Within the framework of legal protection, Indonesian laws and regulations, especially the Sexual Violence Crime Law, have provided a starting basis for protecting victims of digital-based sexual violence, but there are still normative gaps related to the synthetic character of deepfakes and the responsibility of the technology ecosystem. Therefore, an explicit, adaptive, and victim-oriented reformulation of legal protection is needed, including the recognition of digital sexual manipulation as a form of violence, rapid removal mechanisms, comprehensive remediation, and the expansion of platform responsibilities, which are in line with the

³² Hajikazemi and Rimondi.

principles of gender equality, protection from violence, and the strengthening of justice and effective institutions as emphasized in the SDGs

REFERENCES

Abdul Wahid & Mohammad Labib.

Kejahatan Mayantara (Cybercrime).
Bandung: Refika Aditama, 2005.

Adkiras, Fadillah, Fatma Reza Zubarita,
and Zihan Tasha Maharani Fauzi.

“Konstruksi Pengaturan Kekerasan
Berbasis Gender Online Di
Indonesia.” *Jurnal Lex Renaissance*
6, no. 4 (2021): 781–98.
[https://doi.org/10.20885/jlr.vol6.iss4.
art10](https://doi.org/10.20885/jlr.vol6.iss4.art10).

Apriana, Memei, and Any Nugroho.

“Legal Protection for Women
Victims of the Crime of Artificial
Intelligence (Ai) Deepfake Based on
Law Number 12 of 2022 Concerning
Criminal Actions of Sexual
Violence.” *Journal of Social and
Economics Research* 7, no. 1 (2025):
57–75.
<https://idm.or.id/JSER/index.php/JSE>
R.

Arndarnijariah, Faqi Rawni. “THE RIGHT
TO BE FORGOTTEN SEBAGAI
HUKUM PERLINDUNGAN DATA
PRIBADI KORBAN REVENGE
PORN” 8 (2024): 69–82.

[https://doi.org/10.24246/alethea.vol8.
no1](https://doi.org/10.24246/alethea.vol8.no1).

Association for Progressive

Communications (APC). ““Online
Gender-Based Violence: A
Submission from the Association for
Progressive Communications to the
United Nations Special Rapporteur on
Violence against Women, Its Causes
and Consequences.”” *Artikel*, 2017, 3.

Bhattacharjee, Dr. Rituparna, and Ms.

Muskan Sharma. “Deepfake &
Pornography: The Coming Crisis of
Privacy and Consent.” *South Eastern
European Journal of Public Health*,
February 21, 2025, 1196–1213.
<https://doi.org/10.70135/seejph.vi.488>
5.

Chesney, Bobby, and Danielle Citron.

“Deep Fakes : A Looming Challenge
for Privacy , Democracy , and
National Security,” 2019, 1753–1820.

Gracia-zomeño, Andrea, Belinda

Domingo-gómez, Ramón García-
perales, and Eduardo García-
toledano. “Preventing Harassment
and Gender-Based Violence in Online
Videogames Through Education.”
Social Sciencs 14, no. 297 (2025): 1–
18.
[https://doi.org/https://doi.org/10.3390/
/socsci14050297](https://doi.org/https://doi.org/10.3390/socsci14050297).

- Hajikazemi, Sara, and Ilaria Rimondi. "Gender Equality Interventions in Project-Based Organizations : What Works , What Doesn ' t , and Why," 2025. <https://doi.org/10.1177/87569728251335301>.
- Hendra Prayoga, Hadi Tuasikal. "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia." *Abdurrauf Law and Sharia* 1, no. 2 (2024): 22–38.
- Justice, Substantive, and International Journal. "Deepfakes and Victimology : Exploring the Impact of Digital Manipulation on Victims" 8, no. 1 (2025): 1–12. <https://doi.org/10.56087/substantivejustice.v8i1.306>.
- Kusuma, Ellen, and Nenden Sekar Arum. "Memahami Dan Menyikapi Kekerasan Berbasis Gender Online - Safa Net (Awaskbgo)." *Safenet*, 2020. <https://awaskbgo.id/wp-content/uploads/2020/11/panduan-kbgo-v3.pdf>.
- Lopez-fernandez, Olatz, A Jess Williams, and Daria J Kuss. "Measuring Female Gaming : Gamer Profile , Predictors , Prevalence , and Characteristics From Psychological and Gender Perspectives" 10, no. April (2019). <https://doi.org/10.3389/fpsyg.2019.00898>.
- Ma, Alfian, Hari Maghfiroh, Iswanto Suwarno, and Denis Prayogi. "Social Sciences & Humanities Open Social , Legal , and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms : A Systematic Literature Review." *Social Sciences & Humanities Open* 12, no. January (2025): 101882. <https://doi.org/10.1016/j.ssaho.2025.101882>.
- Mahardika, Mahfudz Ikhsan. "Jurnal Fakultas Hukum Unsrat Lex Privatum Vol.14 N0 5 Jan 2025." *Jurnal Fakultas Hukum Unsrat Lex Privatum* 14, no. 5 (2025): 1–8.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Cetakan ke. Jakarta: Divisi Kencana Prenada Media Group, 2021.
- "No Title," n.d. <https://www.kemenpppa.go.id/page/view/NTQzMw==>.
- "No Title," n.d. <https://www.tempo.co/hukum/jumlah-kasus-kekerasan-berbasis-gender-online-naik--52168>.

- Nursyafia, Muhamad Amirulloh, and Helitha Novianty Muchtar. "Kekerasan Berbasis Gender Online (KBGO) Dalam Game Online Menurut Hukum Di Indonesia Serta Perbandingan Dengan Negara Lain." *Jurnal Pendidikan Tambusai* 7 (2023): 2046.
- Rachmawati, Ida, Indah Listyaningrum, Julia Magdalena Waysang, Dewi Suratiningsih, and Ade Risna Sari. "Edukasi Bagi Anak Dalam Upaya Preventif Tindak Kejahatan Seksual Dengan Modus Child Grooming." *RESWARA: Jurnal Pengabdian Kepada Masyarakat* 4, no. 1 (2023): 332–39. <https://doi.org/10.46576/rjpkm.v4i1.2399>.
- Rakhmawati, Dini, Heri Saptadi Ismanto, Bau Ratu, Basir Jarah Anilon, Counseling Study Program, Counseling Study Program, Counseling Study Program, Universitas Tadulako, and Counseling Study Program. "824 Digital Footprint of Violence: Bibliometric Analysis of Online Gender-Based Violence with Vosviewer and Scopus" 10, no. 01 (2026): 824–33. <https://doi.org/10.31316/g-couns.v10i01.8737>.
- Ramli, Ahmad M. *Cyberlaw Dan HAKI Dalam Sistem Hukum Indonesia, Cetakan Ketiga*. Bandung: Refika Aditama, 2010.
- Sharma, Rituparna Bhattacharjee & Muskan. "'Deepfake & Pornography: The Coming Crisis of Privacy and Consent,.'" *South Eastern European Journal of Public Health* XXVI (2025). <https://doi.org/10.70135/seejph.vi.488>.
- Silvia Maharani Iskandar Putri, Nashwa Salsabila, Asmak U I Hosnah. "Kriminalisasi Penggunaan Deepfake Dalam Tindak Pidana Penipuan Dan Pencemaran Nama Baik: Tantangan Dan Solusi Hukum 6, No. 2 (2024): 83–90," " *Jurnal Hukum Legalita* 6, no. 2 (2024): 83–90. <https://doi.org/doi:10.47637/legalita.v6i2.1453>.
- Suardi*, Yumriani, Herdianty Ramlan, Indah Ainun Mutiara, Firdaus, Rahmat Nur, Hasruddin Nur, Syahban Nur, Nur Riswandy Marsuki, Fitri Yanty Muchtar, Syarifuddin. "Gender Equality in Higher Education: Access, Participation, and Academic Leadership." *Journal Of Education Sciences* 9, no. 4 (2025): 2038–48.

- Vaccari, Cristian, and Andrew Chadwick. "Deepfakes and Disinformation : Exploring the Impact of Synthetic Political Video on Deception , Uncertainty , and Trust in News," 2020.
<https://doi.org/10.1177/2056305120903408>.
- Ved Dilip Beloskar, Arunima Haldar, Anupama Gupta. "Gender Equality and Women's Empowerment: A Bibliometric Review of the Literature on SDG 5 through the Management Lens,," *Journal of Business Research*, 172 (2024).
<https://doi.org/https://doi.org/10.1016/j.jbusres.2023.114442>.
- Wang, Soyoung & Kim, Seongcheol. "Users' Emotional and Behavioral Responses to Deepfake Videos of K-Pop Idols." *Computers in Human Behavior*, 2024.
<https://doi.org/10.1016/j.chb.2022.107305>.
- Wiraguna, Sidi Ahyar. "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia." *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (2024).
<https://doi.org/10.59818/jps.v3i3.1390>.
- Women, UN. "UN Women, 'Online and ICT Facilitated Violence Against Women and Girls During COVID-19', <https://www.unwomen.org/-/Media/Headquarters/Attachments/Sections/Library/Publications/2020/Briefonline-and-ict-facilitated-violence-against-women-and-girls-during-co>," n.d.
- Zainuddin, M. *Pemahaman Metode Penelitian Hukum (Pengertian, Paradigma, Dan Susunan Pembentukan)*. Yogyakarta: CV.Istana Agency, 2019.