JURNAL MAGISTER HUKUM UDAYANA
(UDAYANA MASTER LAW JOURNAL)
Vol. 13 No. 3 September 2024
E-ISSN: 2502-3101 P-ISSN: 2302-528x
http: //ojs.unud.ac.id/index.php/jmhu

Deepfake Pornography: How Criminal Liability of Perpetrators in the Indonesian Criminal Law Framework

Fuadi Isnawan[1]

[1]Faculty of Law, Universitas Islam indonesia, E-mail: fuadi.isnawan@uii.ac.id

Info Artikel

Received: 5th April 2024
Accepted: 29th September 2024
Published: 30th September 2024

Keywords:
Artificial Intelligence; Criminal Liability; Cybercrime; Deepfake Pornography

Kata kunci:
Artificial Intelligence; Cybercrime; Deepfake Pornography; Pertanggungjawaban Pidana

Abstract

This study explores the issue of criminal liability for the distribution of deepfake pornography in Indonesia, an emerging form of cybercrime that leverages artificial intelligence (AI) technologies, particularly Generative Adversarial Networks (GANs), to create nonconsensual hyper-realistic sexual content. The research highlights the legal, social, and ethical implications of deepfake pornography, which disproportionately targets women and perpetuates gender-based violence. Despite the growing prevalence of such content, Indonesian legal frameworks currently provide limited protection for victims of deepfake pornography. This normative legal research examines the applicability of two primary legislative tools: The Information and Electronic Transactions Act (ITE Law), Law Number 27 2022 (PDP Law) and the Pornography Law. The ITE Law, while not explicitly mentioning pornography, addresses content that violates decency, including deepfake pornography. In PDP Law which offer crucial legal protections against the unlawful processing of personal data, including the manipulation of individuals' likenesses in deepfake content. Article 66 outlines the legal recourse available for victims whose personal data, such as their image, has been altered or disseminated without consent. Meanwhile, Article 68 establishes penalties for violations of data processing, further strengthening criminal accountability in cases involving deepfake pornography. The Pornography Law specifically prohibits the creation and dissemination of nonconsensual pornographic material, covering digitally manipulated content. The findings underscore the importance of mens rea (intent) and actus reus (criminal actions) in establishing criminal liability for deepfake pornography perpetrators under Indonesian law. In conclusion, the research calls for more comprehensive legal reforms to better protect victims of this evolving cybercrime, emphasizing the need to adapt to technological advancements while upholding privacy and dignity.

Abstrak

Penelitian ini mengeksplorasi isu pertanggungjawaban pidana atas distribusi pornografi deepfake di Indonesia, sebuah bentuk kejahatan siber yang sedang berkembang yang memanfaatkan teknologi kecerdasan buatan (artificial intelligence/AI), khususnya Generative Adversarial Networks (GAN), untuk membuat konten seksual hiper-realistis yang tidak konsensual. Penelitian ini menyoroti implikasi hukum, sosial, dan etika dari pornografi deepfake, yang secara tidak proporsional menargetkan perempuan dan melanggengkan kekerasan berbasis gender. Terlepas dari meningkatnya prevalensi konten semacam itu,

Corresponding Author:
Fuadi Isnawan, E-mail: *fuadi.isnawan@uii.ac.id*

DOI:
10.24843/JMHU.2024.v13.i03.p15.

kerangka hukum Indonesia saat ini hanya memberikan perlindungan yang terbatas bagi para korban pornografi deepfake. Penelitian hukum normatif ini mengkaji penerapan dua perangkat legislatif utama: Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 (UU PDP), dan Undang-Undang Pornografi. UU ITE, meskipun tidak secara eksplisit menyebutkan pornografi, membahas konten yang melanggar kesusilaan, termasuk pornografi deepfake. Dalam UU PDP yang menawarkan perlindungan hukum yang penting terhadap pemrosesan data pribadi yang melanggar hukum, termasuk manipulasi kemiripan individu dalam konten deepfake. Pasal 66 menguraikan jalur hukum yang tersedia bagi para korban yang data pribadinya, seperti gambarnya, telah diubah atau disebarkan tanpa persetujuan. Sementara itu, Pasal 68 menetapkan hukuman untuk pelanggaran pengolahan data, yang semakin memperkuat akuntabilitas pidana dalam kasus-kasus yang melibatkan pornografi deepfake. UU Pornografi secara khusus melarang pembuatan dan penyebaran materi pornografi yang tidak sesuai dengan persetujuan, termasuk konten yang dimanipulasi secara digital. Temuan ini menggarisbawahi pentingnya mens rea (niat) dan actus reus (tindakan kriminal) dalam menetapkan pertanggungjawaban pidana bagi pelaku pornografi deepfake di bawah hukum Indonesia. Sebagai kesimpulan, penelitian ini menyerukan reformasi hukum yang lebih komprehensif untuk melindungi korban kejahatan siber yang terus berkembang ini, dengan menekankan perlunya beradaptasi dengan kemajuan teknologi dengan tetap menjunjung tinggi privasi dan martabat.

.

I. Introduction

In recent years, the rapid advancement of digital technology has significantly transformed various aspects of human life[1], including the legal field, where new challenges continue to emerge.[2] One of the most concerning technological innovations is deepfake, an artificial intelligence (AI)-based technology that allows for the manipulation of visual and audio content with a high degree of accuracy.[3] Through deepfake, a person's face can be superimposed onto another person's body in videos or images, creating content that appears authentic but is entirely fabricated.[4] While this technology has potential beneficial applications in industries such as entertainment and

[1] Martin Hilbert, "Digital Technology and Social Change: The Digital Transformation of Society from a Historical Perspective," *Dialogues in Clinical Neuroscience* 22, no. 2 (June 30, 2020): 189, https://doi.org/10.31887/DCNS.2020.22.2/mhilbert.

[2] Yuri Tikhomirov et al., "Law and Digital Transformation," *Legal Issues in the Digital Age*, 2 (2021): 3, https://doi.org/10.17323/2713-2749.2021.2.3.20.

[3] Mika Westerlund, "The Emergence of Deepfake Technology: A Review," *Technology Innovation Management Review* 9, no. 11 (2019): 40, https://doi.org/10.22215/timreview/1282.

[4] Andrei O. J. Kwok and Sharon G. M. Koh, "Deepfake: A Social Construction of Technology Perspective," *Current Issues in Tourism* 24, no. 13 (July 3, 2021): 2, https://doi.org/10.1080/13683500.2020.1738357.

education, its misuse has led to serious issues, particularly in the production and distribution of non-consensual pornographic content, known as deepfake pornography.[5]

Deepfake pornography has garnered global attention due to its destructive impact on individual privacy and dignity, especially for women.[6] This type of pornography allows perpetrators to combine a person's face with another body in explicit situations without the individual's knowledge or consent.[7] As a result, victims often experience profound psychological impacts, including shame, depression, and anxiety, all exacerbated by the persistent nature of the internet in spreading such content.[8] Furthermore, victims face significant social challenges, such as reputational damage, job loss, and social ostracism.[9][10] This phenomenon positions deepfake pornography as a new form of cybercrime that not only devastates individual lives but also challenges the integrity of legal systems.[11]

In Indonesia, cybercrime regulations have evolved, with various laws and regulations aimed at addressing these threats.[12] However, the complexity associated with deepfake pornography cases presents new challenges for law enforcement.[13][14] The realistic nature of deepfake content often makes the process of legal proof more difficult.[15] Additionally, the criminal liability of deepfake pornography perpetrators becomes a crucial issue that

[5] Lorenzo Di Silvestro and Cristina Iurissevich, "Pornografia Contemporanea: Il Deepfake Come Forma Di Abuso," *European Public & Social Innovation Review* 9 (July 24, 2024): 11, https://doi.org/10.31637/epsir-2024-370.

[6] Jacquelyn Burkell and Chandell Gosse, "Nothing New Here: Emphasizing the Social and Cultural Context of Deepfakes," *First Monday* 24, no. 12 (December 2, 2019), https://doi.org/10.5210/fm.v24i12.10287.

[7] Kate Kobriger et al., "Out of Our Depth with Deep Fakes: How the Law Fails Victims of Deep Fake Nonconsensual Pornography," *Richmond Journal of Law & Technology* XXVIII, no. 2 (n.d.): 207.

[8] Jeffrey T. Hancock and Jeremy N. Bailenson, "The Social Impact of Deepfakes," *Cyberpsychology, Behavior, and Social Networking* 24, no. 3 (March 1, 2021): 151, https://doi.org/10.1089/cyber.2021.29208.jth.

[9] Sami Alanazi, Seemal Asif, and Irene Moulitsas, "Examining the Societal Impact and Legislative Requirements of Deepfake Technology: A Comprehensive Study," *International Journal of Social Science and Humanity* 14, no. 2 (2024): 58, https://doi.org/10.18178/ijssh.2024.14.2.1194.

[10] Olivia Debroy and Bhargavi D Hemmige, "Psycho-Social Impact of Deepfake Content in Entertainment Media," *INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD* 10, no. 5 (2024): 234, https://doi.org/:10.2015/IJIRMF/202405032.

[11] Miha Šepec and Melanija Lango, "Virtual Revenge Pornography as a New Online Threat to Sexual Integrity," *Balkan Social Science Review* 15 (2020): 119.

[12] Isra Ruddin and Subhan Zein SGN, "Evolution of Cybercrime Law in Legal Development in the Digital World," *Jurnal Multidisiplin Madani* 4, no. 1 (January 29, 2024): 169, https://doi.org/10.55927/mudima.v4i1.7962.

[13] Matthew B. Kugler and Carly Pace, "Deepfake Privacy: Attitudes and Regulation," *Northwestern Public Law Research Paper* 116, no. 3 (2021): 615, https://dx.doi.org/10.2139/ssrn.3781968.

[14] Bart van der Sloot and Yvette Wagensveld, "Deepfakes: Regulatory Challenges for the Synthetic Society," *Computer Law & Security Review* 46 (September 1, 2022): 4, https://doi.org/10.1016/j.clsr.2022.105716.

[15] Riana Pfefferkorn, "'Deepfakes' in the Courtroom," *Boston University Public Interest Law Journal* 29, no. 2 (2020): 260, https://ssrn.com/abstract=4321140.

requires thorough analysis, considering the dynamic and ever-evolving nature of this crime.[16]

The primary objective of this research is to conduct an in-depth analysis of the Indonesian criminal law framework in addressing the phenomenon of deepfake pornography, with a particular focus on the criminal liability of the perpetrators. This study aims to identify potential legal gaps in the current regulations and evaluate the effectiveness of existing laws in facing the challenges posed by this technology. Consequently, this research seeks to provide concrete and practical recommendations for the development of legal policies that are more adaptive and responsive to the advances in digital technology.

The urgency of this research cannot be overstated, given the increasing prevalence of deepfake pornography cases not only globally but also in Indonesia. The lack of specific and effective regulations to address this crime may allow perpetrators to evade legal consequences, potentially leading to an increase in cases and victims. Moreover, this research is crucial in the context of protecting human rights, where every individual has the right to privacy and personal dignity. Without adequate legal intervention, deepfake pornography could pose a serious threat to the protection of these rights in the future.

This research is expected to make a significant contribution to strengthening the criminal law foundation in Indonesia, particularly in addressing the evolving threat of cybercrime. The findings of this study will not only benefit the development of law at the national level but also have important implications in the global discourse on how the international community can respond to the threats posed by deepfake technology. Thus, this research aims not only to contribute to the existing scientific literature but also to provide practical guidance for policymakers, law enforcement, and the general public in the collective effort to protect fundamental rights from technology-based crimes.

This research offers a novel contribution to the existing literature on deepfake pornography within the framework of Indonesian criminal law by specifically focusing on the criminal liability of individuals who distribute deepfake pornography, rather than examining the accountability of AI as the perpetrator. Unlike the 2024 study by Asri Gresmelian Eurike Hailtik and Wiwik Afifah, which centers on the regulation and criminal responsibility of AI in the commission of deepfake crimes in Indonesia, my research shifts the focus to human actors who exploit this technology to disseminate nonconsensual and fabricated sexual content. This approach addresses a critical gap in the literature by analyzing how existing criminal law can be applied or adapted to hold these individuals accountable, thereby emphasizing the role of human agency in the propagation of deepfake pornography.

Furthermore, while Sayid Muhammad Rifki Noval's 2023 research delves into Indonesia's readiness to face social engineering attacks facilitated by deepfake technology, my study specifically hones in on the legal implications and the need for robust legal frameworks to combat the spread of deepfake pornography. My research also distinguishes itself from the work of Adnasohn Aqilla Respati and colleagues in 2024, which broadly examines legal aspects related to the prevention of deepfake crimes

[16] Kareem Gibson, "Deepfakes and Involuntary Pornography: Can Our Current Legal Framework Address This Technology," *Wayne Law Review* 66 (2020): 269.

and legal protections, by narrowing down the focus to criminal responsibility in cases where deepfake pornography is disseminated without consent.

This research, conducted in 2024, fills an important gap by providing a detailed analysis of how Indonesian criminal law can address the challenges posed by deepfake pornography, particularly in holding distributors legally accountable. The study contributes to the ongoing discourse on cybercrime and digital privacy, offering new perspectives on legal responses to emerging technological threats in the Indonesian context.

2. Research Method

This study employs a normative legal research method, which is fundamentally characterized by its focus on library-based or secondary data analysis. Normative legal research, also known as library legal study, involves a systematic examination of legal materials, including statutory laws, regulations, and scholarly literature, to address specific legal issues. The normative approach is essential in this research as it facilitates a comprehensive understanding of the legal framework governing deepfake pornography within the context of Indonesian criminal law. [17]

The research adopts two primary approaches: the statutory approach and the conceptual approach. The statutory approach involves a thorough examination and analysis of all relevant legislation and regulations that pertain to the legal issues at hand, particularly the laws governing cybercrime and digital content, such as Indonesia's Information and Electronic Transactions Law (UU ITE). This approach ensures that the study is grounded in the existing legal framework, providing a solid basis for analyzing the criminal liability of deepfake pornography perpetrators.

In situations where, existing laws are insufficient or non-existent to address the complexities posed by deepfake technology, the conceptual approach is applied. This approach allows the researcher to explore and develop legal concepts that could be proposed as new regulations or amendments to existing laws. The conceptual approach is particularly relevant given the rapidly evolving nature of digital crimes, where legal systems often lag behind technological advancements.[18]

The research relies on two categories of legal materials: primary legal materials and secondary legal materials. Primary legal materials consist of binding legal documents, including statutes, regulations, and court decisions, with the UU ITE being the cornerstone of this study. These materials provide the authoritative basis for legal analysis. Secondary legal materials, on the other hand, include scholarly articles, books, and commentaries that offer interpretations and critiques of the primary legal materials.

[17] Nurul Qamar and Farah Syah Rezah, *Metode Penelitian Hukum: Doktrinal Dan Non-Doktrinal* (Makassar: CV. Social Politic Genius (SIGn), 2020), 47.

[18] Muhaimin Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Press, 2020), 54.

These secondary sources are invaluable in understanding the broader context of the law and in identifying potential gaps or ambiguities in the existing legal framework.[19]

The data analysis in this research is conducted using a qualitative descriptive technique. This method involves systematically describing and interpreting the collected legal materials to draw conclusions about the current state of the law and to propose recommendations for future legal developments. The qualitative approach is crucial in normative legal research as it allows for a deep and nuanced understanding of the legal issues being studied, facilitating the development of well-founded legal arguments and conclusions.

3. Result and Discussion

3.1. Analyze of Deepfake Pornography as Cybercrime

The term "deepfake porn" emerged from discussions on Reddit forums, marking the intersection of advanced artificial intelligence (AI) technologies with the realm of explicit content. Within scientific literature, deepfake technology is analyzed from two distinct perspectives: technological and content-based.[20] The technological aspect focuses on the implementation of machine learning and AI algorithms that enhance deepfake videos, enabling the realistic superimposition of one person’s face onto another's body. On the other hand, content-based analysis examines the nature of these videos, which frequently involve non-consensual pornography. Deepfake videos, particularly those of a pornographic nature, have become a significant concern due to their potential for harm. These videos often involve the unauthorized use of AI to create highly realistic fake content, where the victim's face is seamlessly merged onto the body of a pornographic actor. [21] The problem of deepfake pornography gained substantial attention in 2017, following a high-profile case in which the face of actress Gal Gadot was superimposed onto a pornographic video, sparking widespread media coverage and public discourse in the United States.[22] This incident highlighted the vulnerability of public figures to such violations and triggered a nationwide debate on the ethical and legal ramifications of deepfake technology.[23]

Deepfakes, a sophisticated form of cybercrime, are generated through a method known as Generative Adversarial Network (GAN), which falls under the sub-category of

[19] Muhammad Siddiq Armia, *Penentuan Metode & Pendekatan Penelitian Hukum* (Banda Aceh: Lembaga Kajian Konstitusi Indonesia, 2022), 12.

[20] Emily van der Nagel, “Verifying Images: Deepfakes, Control, and Consent,” *Porn Studies* 7, no. 4 (October 1, 2020): 425, https://doi.org/10.1080/23268743.2020.1741434.

[21] Karolina Mania, “Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study,” *Trauma, Violence, & Abuse* 25, no. 1 (January 1, 2024): 2, https://doi.org/10.1177/15248380221143772.

[22] Regina Rini and Leah Cohen, “Deepfakes, Deep Harms,” *Journal of Ethics and Social Philosophy (JESP)* XXII, no. 2 (2022): 145.

[23] Eric Kocsis, “Deepfakes, Shallowfakes, and the Need for a Private Right of Action,” *DICKINSON LAW REVIEW* 126, no. 2 (2022): 625.

pattern recognition in machine learning.[24] Introduced in 2014 by researchers at the University of Montreal, GANs employ two neural networks that work in opposition.[25] The first network, a generative model, creates data by learning the distribution of the original dataset, while the second, a discriminative model, aims to distinguish between genuine and fabricated data. These networks engage in an adversarial process, iterating through multiple cycles of generation and detection.[26] Over time, the generative model becomes so refined that the discriminative model, and eventually even human observers, can no longer differentiate between real and fake content. This ability to produce highly realistic yet entirely fabricated videos make deepfakes a particularly insidious tool for criminal activity, including the creation of deepfake pornography. Such developments underscore the pressing need for robust legal frameworks in Indonesia to address the criminal liability of individuals involved in producing and distributing deepfake pornography.[27]

Expanding on the analysis of deepfake pornography within the context of cybercrime, it is essential to explore the implications of categorizing such offenses under the three-factor spectrum proposed by Sarre, Lau, and Chang. Their framework introduces a nuanced approach to understanding cybercrimes by classifying them into three distinct types:[28]

1. Type I Cybercrimes involve crimes that are purely technical in nature, such as hacking, where the primary method of execution relies on exploiting technological vulnerabilities. These crimes are often carried out without direct human interaction beyond the initial setup.

2. Type II Cybercrimes involve crimes where technology facilitates human interaction, such as cyberbullying or online harassment. Here, technology serves as a medium through which individuals perpetrate crimes against one another, with human contact being a significant component of the offense.

3. Type III Cybercrimes, which are particularly relevant to the discussion of deepfake pornography, encompass crimes that are perpetrated by advanced technologies, including Artificial Intelligence, robots, or self-learning systems. These crimes represent a new frontier in cybercrime, where the technology itself plays an active role in the creation and dissemination of harmful content.

Deepfake porn, which employs AI technologies like Generative Adversarial Networks (GANs) to create realistic but fake pornographic videos, squarely fits within the Type III

[24] Pavankumar Mulgund and Samina Lohawala, "Deepfake: The Lay of the Land," *ISACA JOURNA* 1 (2021): 2.

[25] Catherine de Weever and Sebastian Wilczek, "Deepfake Detection through PRNU and Logistic Regression Analyses," Research Paper (Amsterdam: University of Amsterdam, May 7, 2020), 3.

[26] Maryam Taeb and Hongmei Chi, "Comparison of Deepfake Detection Techniques through Deep Learning," *Journal of Cybersecurity and Privacy* 2, no. 1 (2022): 90, https://doi.org/10.3390/jcp2010007.

[27] Yi Yan, "Deep Div Deep Dive into Deepfak o Deepfakes—Safeguarding Our Digital Identity," *Brooklyn Journal of International; Law* 48, no. 2 (2023): 770.

[28] Kirsty Phillips et al., "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies," *Forensic Sciences* 2, no. 2 (2022): 385, https://doi.org/10.3390/forensicsci2020028.

category. The use of AI in these crimes not only amplifies the scale and speed at which such content can be produced and distributed but also complicates efforts to detect, prevent, and prosecute these offenses. The technology behind deepfakes enables the creation of content that is often indistinguishable from real footage, making it difficult for victims to prove the falsity of the material and seek redress.[29]

The AI's role in producing and disseminating deepfake pornography without human oversight or intervention is a definitive illustration of a Type III cybercrime, as categorized by Sarre, Lau, and Chang. This classification reflects the advanced technological mechanisms at play, where Generative Adversarial Networks (GANs) autonomously create hyper-realistic, yet entirely fabricated, pornographic images and videos. Unlike traditional cybercrimes that may involve direct human manipulation or technical expertise, Type III cybercrimes are distinguished by their reliance on autonomous systems that operate independently of human control. This autonomous nature not only amplifies the scale and impact of the crime but also complicates regulatory and legal responses. The sophisticated technology behind deepfakes allows for the rapid generation and distribution of nonconsensual pornographic content, significantly challenging existing legal frameworks and necessitating new approaches to effectively address these emerging threats.[30]

In transitioning to the broader issue of nonconsensual pornography, it is essential to explore how deepfake pornography exacerbates the already pervasive problem of unauthorized and exploitative sexual content.[31] Nonconsensual pornography, which involves the distribution of sexually explicit material without the subject's consent, has long been a pressing issue, but deepfake technology introduces a new dimension of complexity.[32] By enabling the creation of convincing yet entirely fictitious sexual content, deepfakes undermine personal privacy and consent in unprecedented ways, thereby intensifying the need for comprehensive legal reforms and robust protections against such forms of exploitation.[33]

The non-consensual creation and distribution of deepfake pornography represent a severe form of cybercrime that disproportionately targets women, turning their bodies and faces into digital commodities for exploitation. By utilizing a woman's image without her consent, deepfake technology reinforces a digital environment that

[29] Rick Sarre, "Perspectives on Policing Post-Pandemic Cybercrime," in *Cybercrime in the Pandemic Digital Age and Beyond*, ed. Russell G. Smith et al. (Cham: Springer International Publishing, 2023), 173–92, https://doi.org/10.1007/978-3-031-29107-4_9.

[30] Rick Sarre, Laurie Yiu-Chung Lau, and Lennon Y.C. Chang, "Responding to Cybercrime: Current Trends," *Police Practice and Research* 19, no. 6 (November 2, 2018): 515–18, https://doi.org/10.1080/15614263.2018.1507888.

[31] Brooklynn Armesto-Larson, "Nonconsensual Pornography: Criminal Law Solutions to a Worldwide Problem," *Oregon Review Of International Law* 21 (2020): 195.

[32] Moncarol Y. Wang, "Don't Belie 't Believe Your Eyes: Fighting Deepfak Es: Fighting Deepfaked Nonconsensual Ed Nonconsensual Pornography with Tort Law," *University of Chicago Legal Forum* 2022 (2023): 419.

[33] Olivia B. Newton and Mel Stanfill, "My NSFW Video Has Partial Occlusion: Deepfakes and the Technological Production of Non-Consensual Pornography," *Porn Studies* 7, no. 4 (October 1, 2020): 411, https://doi.org/10.1080/23268743.2019.1675091.

objectifies and dehumanizes women, catering primarily to male consumption.[34] Studies indicate that an overwhelming 96% of the nearly 85,000 deepfakes circulating online involve sexually explicit content depicting women without their consent. Tools like DeepNude, which utilize Generative Adversarial Networks (GANs) to generate realistic nude images, exemplify the malicious potential of this technology. The widespread sharing of over 104,000 fake nudes of women, many of whom are minors, highlights the urgent need for stringent legal measures to address the exploitation and violation of women's rights in the digital space.[35] This alarming trend underscores the importance of recognizing deepfake pornography as a serious cybercrime, requiring robust legal frameworks and enforcement to protect individuals from such invasive and harmful acts.

Deepfake pornography is a rapidly emerging form of cybercrime, fueled by advancements in machine learning and computer vision technologies. In the past, the production of fake videos was considered nearly impossible due to the need for advanced equipment, specialized knowledge, and time-consuming techniques. [36] However, with the development of machine learning algorithms and the availability of high-throughput computing, creating deepfakes has become more accessible and commonplace.[37] A deepfake video is generated by using source material, such as films or other visual representations of an individual, which is then processed to produce a modified video that features the subject's face.[38][39] This process, known as deep learning, involves neural networks that are trained to automatically detect and replicate the facial expressions of the subject, enabling the creation of a synthetic video.[40]

Deepfake pornography, poses significant challenges due to the rapid and widespread dissemination of fake content, particularly through social media platforms.[41] Research has shown that false information, such as that generated by deepfake technology, can spread up to six times faster than accurate content, primarily because it is often more

[34] Benjamin T. Suslavich, "Nonconsensual Deepfakes: A" Deep Problem" for Victims," *Journal of Science and Technology* 33 (2023): 181.

[35] Jennifer Laffier and Aalyia Rehman, "Deepfakes and Harm to Women," *Journal of Digital Life and Learning* 3, no. 1 (2023): 8, https://doi.org/10.51357/jdll.v3i1.218.

[36] Gihun Lee and Mihui Kim, "Deepfake Detection Using the Rate of Change between Frames Based on Computer Vision," *Sensors* 21, no. 21 (2021): 3, https://doi.org/10.3390/s21217367.

[37] H. A. Khalil and S. A. Maged, "Deepfakes Creation and Detection Using Deep Learning," in *2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, 2021, 24, https://doi.org/10.1109/MIUCC52538.2021.9447642.

[38] Abdulqader M Almars, "Deepfakes Detection Techniques Using Deep Learning: A Survey," *Journal of Computer and Communications* 9, no. 5 (2021): 24, https://doi.org/10.4236/jcc.2021.95003.

[39]

Agnieszka McPeak, "The Threat of Deepfakes in Litigation: Raising the Authentication Bar to Combat Falsehood," *Vanderbilt Journal of Entertainment and Technology Law* 23, no. 2 (2021): 439, https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss2/5.

[40] Zubair Ahmed Khan and Asma Rizvi, "Deepfakes: A Challenge for Women Security and Privacy," *CMR University Journal For Contemporary Legal Affairs* 5, no. 1 (2023): 205.

[41] Samer Hussain Al-khazrajı et al., "Impact of Deepfake Technology on Social Media: Detection, Misinformation and Societal Implications," *The Eurasia Proceedings of Science Technology Engineering and Mathematics* 23 (September 2023): 431, https://doi.org/10.55549/epstem.1371792.

sensational and memorable.[42][43] This rapid proliferation makes it exceedingly difficult for victims to mitigate the damage, as once deepfake content is produced and circulated, it becomes nearly indistinguishable from genuine material and can persist indefinitely in digital archives.[44] Victims often struggle to prove the falsity of such content and to effectively counteract the harm caused.[45] The implications are profound, as deepfake pornography not only violates the privacy and dignity of individuals but also undermines fundamental rights such as freedom of expression.[46] It imposes a chilling effect, silencing victims and forcing them into self-censorship, particularly concerning their sexual orientation, while also exacerbating societal prejudices.[47]

Unlike traditional nonconsensual pornography or revenge porn, where the content typically involves real individuals whose privacy is directly violated, deepfake pornography raises unique issues due to its ability to fabricate sexual content that appears to depict real people but is entirely falsified through advanced digital techniques.[48] One of the critical challenges with deepfake pornography is the blurring of lines between reality and fabrication.[49] Although deepfakes do not depict real events or actual persons in the traditional sense, they can create a convincing illusion that may lead viewers to believe the content is genuine.[50] This misperception can cause significant harm to individuals whose likenesses are used without their consent, even though the depicted actions never occurred in reality. The implications are severe, as the individuals whose faces are superimposed onto pornographic content may suffer reputational damage, psychological distress, and a profound violation of their dignity.[51]

In 2021, the Federal Bureau of Investigation (FBI) recognized the growing threat of deepfake technology by formally categorizing it as a potential vector for cyberattacks

[42] Francesco Pierri and Stefano Ceri, "False News On Social Media: A Data-Driven Survey," *SIGMOD Rec.* 48, no. 2 (December 2019): 24, https://doi.org/10.1145/3377330.3377334.

[43] Srijan Kumar and Neil Shah, "False Information on Web and Social Media: A Survey," *ArXiv* 1, no. 1 (2018): 11, https://doi.org/10.48550/arXiv.1804.08559.

[44] A. Shaji George and A. S. Hovan George, "Deepfakes: The Evolution of Hyper Realistic Media Manipulation," *Partners Universal Innovative Research Publication* 1, no. 2 (December 11, 2023): 59, https://doi.org/10.5281/zenodo.10148558.

[45] Anne Pechenik Gieseke, ""The New W 'The New Weapon of Choice Eapon of Choice': Law' ": Law's Current Inability t Ent Inability to Properly Address Deepfake Pornography," *Vanderbilt Law Review* 73, no. 5 (2020): 1500, https://scholarship.law.vanderbilt.edu/vlr/vol73/iss5/4.

[46] Alex Barber, "Freedom of Expression Meets Deepfakes," *Synthese* 202, no. 2 (July 20, 2023): 40, https://doi.org/10.1007/s11229-023-04266-4.

[47] Yasemin Durmuş and Elif Yıldız, "Reconstruction of Discourses in Victims of Cyber Abuse in New Media: Derya Kuş Case," in *Media and Communication in the Digital Age: Changes and Dynamics* (Gaziantep: Özgür Yayın-Dağıtım Co. Ltd., 2023), 20.

[48] Karolina Mania, "The Legal Implications and Remedies Concerning Revenge Porn and Fake Porn: A Common Law Perspective," *Sexuality & Culture* 24, no. 6 (December 1, 2020): 2083, https://doi.org/10.1007/s12119-020-09738-0.

[49] Miriam Meckel and Léa Steinacker, "Hybrid Reality: The Rise of Deepfakes and Diverging Truths," *Morals & Machines* 1, no. 1 (2021): 18, https://doi.org/10.5771/2747-5174-2021-1-10.

[50] Nicolas Graber-Mitchell, "Artificial Illusions: Deepfakes as Speech," *Intersect* 14, no. 3 (2021): 7, https://ssrn.com/abstract=3876862.

[51] Rebecca A. Delfino, "Pornographic Deepfak Aphic Deepfakes: The Case for F Es: The Case for Federal Criminalization of al Criminalization of Revenge Porn's NNext Tragic Act," *Fordham Law Review* 3 (2019): 897.

within the newly defined framework of Business Identity Compromise (BIC). This classification reflects the escalating concerns within the international security community regarding the misuse of artificial intelligence (AI) and machine learning technologies to create hyper-realistic fake videos, images, and audio. Deepfakes, which were initially popularized for entertainment purposes, have evolved into tools with the potential to cause significant harm, not only on a personal level but also at a corporate and national scale. By acknowledging deepfakes as a cyberattack vector, the FBI underscores the increasing sophistication of cyber threats that leverage AI to breach corporate defenses, manipulate markets, and even disrupt national security by undermining trust in digital communications and media.[52]

Various organizations, such as the Cyber Civil Rights Initiative (CCRI), Electronic Frontier Foundation (EFF), and the International Centre for Missing & Exploited Children (ICMEC), are at the forefront of combating these crimes. Surveys conducted by these organizations reveal alarming trends, including a significant increase in deepfake abuse and child sexual exploitation material online. The United Nations Office on Drugs and Crime (UNODC) and WePROTECT Global Alliance highlight the need for stronger collaboration between governments, law enforcement, and private entities to address these challenges effectively. The Internet Watch Foundation (IWF) and the National Center for Missing and Exploited Children (NCMEC) have reported substantial efforts to remove harmful content from the internet, yet the rapid evolution of cybercrime necessitates continued innovation in detection and prevention technologies, as emphasized by the Deepfake Detection Consortium and Stanford University's Center for Internet and Society. This underscores the urgent need for comprehensive legal frameworks, particularly in Indonesia, to hold perpetrators accountable and protect vulnerable populations from the escalating threat of cybercrime.[53]

Deepfakes present a range of harms, varying significantly based on the quality of the content and the individual targeted. High-quality deepfakes, which seamlessly merge fabricated content with real imagery, are particularly dangerous as they are more likely to be perceived as genuine, leading to serious consequences.[54] These include the spread of misinformation, the creation of hoaxes, and the instigation of social unrest. In the context of deepfake pornography, this technology perpetuates gender-based violence by enabling the creation and distribution of nonconsensual sexual content,[55] often referred to as "revenge porn." Such misuse of deepfake technology not only damages reputations but also inflicts profound psychological and emotional harm on victims. Given the escalating sophistication of deepfake technology, there is an urgent need to analyze and

[52] Lorenzo DAMI, "Analysis and Conceptualization of Deepfake Technology as Cyber Threat" (School of Political Science "Cesare Alfieri," 2021), 14.

[53] Geeta Singh Chetry and Uzzal Sharma, "Emerging Technologies as a Tool for Cybercrime Against Women and Children," *SSRN Electronic Journal*, 2024, 2, https://dx.doi.org/10.2139/ssrn.4765788.

[54] Marco Viola and Cristina Voto, "Designed to Abuse? Deepfakes and the Non-Consensual Diffusion of Intimate Images," *Synthese* 201, no. 1 (January 13, 2023): 29, https://doi.org/10.1007/s11229-022-04012-2.

[55] Rangita de Silva de Alwis, "A Rapidly Shifting Landscape: Why Digitized Violence Is the Newest Category of Gender-Based Violence," *SciencesPo Law Review* 25 (2024): 7.

address these issues within the framework of criminal law in Indonesia, ensuring that perpetrators are held accountable and that victims receive appropriate protection.[56]

Beside of that, the non-consensual portrayal of an individual in a pornographic setting reduces the person to a mere object of sexual exploitation and exposure. This form of digital assault strips away the dignity of the victims, leaving them feeling dehumanized, degraded, and violated by the misrepresentation and misappropriation of their identity. One victim articulated the profound impact, stating that it was "dehumanizing, degrading, and violating to see oneself being misrepresented and misappropriated in such a manner". The psychological toll of such invasions can be so pervasive that some victims have been compelled to change their identities to escape the associated stigma and continuous harassment. The intrusion into sexual privacy, a fundamental human right, often results in significant psychological and physical harm. This was exemplified by the case of Indian journalist Rana Ayyub, who became the target of a pornographic deepfake that led to severe psychological distress and public humiliation.[57]

Deepfake pornography poses a significant threat to sexual privacy, a fundamental aspect of personal autonomy and dignity. Sexual privacy allows individuals to control the exposure of their bodies and manage intimate boundaries, which is crucial for maintaining personal agency, intimacy, and equality. The violation of sexual privacy through deepfake technology not only undermines an individual's autonomy but also exploits their vulnerability, as trust and self-disclosure are core elements of sexual privacy.[58] The harm inflicted by deepfake pornography extends beyond the immediate violation, as it perpetuates gender-based violence and severely damages the dignity of the victims.[59] This concept of dignity, deeply rooted in human rights and recognized in legal precedents, highlights the need for robust legal protections. In the Indonesian context, addressing deepfake pornography requires a nuanced understanding of the interplay between privacy, dignity, and the evolving nature of digital threats, underscoring the importance of a comprehensive legal framework to safeguard individuals from such invasive cybercrimes.[60]

3.2 Criminal Responsibility of Deepfake Pornography Perperator

3.2.1 Criminal responsibility of Perperator Based on ITE Law

In the context of Indonesian criminal law, the criminal liability of individuals involved in the distribution of deepfake pornography can be analyzed under the provisions of the Electronic Information and Transactions Law (UU ITE). Although UU ITE and its amendments do not explicitly use the term "pornography," they address "content violating decency" under Article 27, paragraph (1). This article stipulates that anyone

[56] Tyrone Kirchengast, "Deepfakes and Image Manipulation: Criminalisation and Control," *Information & Communications Technology Law* 29, no. 3 (September 1, 2020): 312, https://doi.org/10.1080/13600834.2020.1794615.

[57] Emily Pascale, "Deeply Dehumanizing, Degrading, And Violating: Deepfake Pornography And The Path To Legal Recourse," *Syracuse Law Review* 73 (2023): 340.

[58] Danielle Keats Citron, "Sexual Privacy," *The Yale Law Journal Company* 128, no. 7 (2019): 1922.

[59] Chidera Okolie, "Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns," *Journal of International Women's Studies* 25, no. 2 (2023): 7.

[60] Gowri Dev and Akshay Pramodh, "An Age Where Eyes Can't Be Trusted: Image Manipulation Through Deepfakes," *DNLU Student Law Journal* 2 (2023): 107.

who intentionally and without right distributes, transmits, or makes accessible electronic information and/or electronic documents containing content that violates decency may be subject to criminal sanctions.[61]

In cases of deepfake pornography, the content that violates decency is clearly applicable, as deepfake pornography involves the use of artificial intelligence to manipulate someone's face and body to create pornographic material without their consent. The distribution of such content not only breaches decency norms but also infringes upon the honor and dignity of the individual whose image is used without permission. Therefore, those who distribute deepfake pornography can be held criminally liable under Article 27, paragraph (1) of UU ITE, with a focus on the intent to distribute or make accessible content that violates decency.

This article regulates actions related to the distribution of electronic information that violates decency, which is directly relevant to the transmission and accessibility of deepfake pornographic content. Below the analysis of the elements:[62]

a. The subjective elements of this article emphasize two key aspects. First, the element of intent ("sengaja") indicates that the perpetrator acts with full awareness and purpose. In the context of deepfake pornography, this implies that the individual deliberately engages in distributing, displaying, transmitting, or making accessible electronic information or documents that violate decency. The second subjective element, "without rights" ("tanpa hak"), refers to the perpetrator’s lack of legal authorization to carry out such actions, such as not having permission from the content owner to distribute or broadcast electronic information that breaches societal decency norms.

b. On the objective side, the act of distributing, transmitting, or making accessible such electronic information or documents refers to the various ways in which indecent content can be spread or accessed by others. This includes publishing, uploading, or disseminating it through electronic media, which aligns closely with how deepfake pornography is shared on digital platforms. Furthermore, the content in question must contain material that contravenes the prevailing norms of decency within society ("muatan yang melanggar kesusilaan").

The article defines key terms that directly relate to the dissemination of deepfake content, making it particularly relevant for addressing the challenges posed by this form of cybercrime. "Broadcasting" encompasses the actions of transmitting, distributing, and making accessible electronic information or documents within an electronic system. This is significant in the context of deepfake pornography, as it involves not only the creation but also the widespread distribution of non-consensual explicit material. "Distributing,"

[61] Vera Rimbawani Sushanty, “Pornografi Dunia Maya Menurut Kitab Undang-Undang Hukum Pidana, Undang-Undang Pornografi Dan Undang-Undang Informasi Elektronik,” *Jurnal Gagasan Hukum* 1, no. 01 (September 24, 2019): 123, https://doi.org/10.31849/jgh.v1i01.2894.

[62] Yuni Shaputri, Siti Nurewah, and Yusep Mulyana, “Penegakan Hukum Bagi Pengguna Aplikasi Michat Sebagai Sarana Tindak Pidana Prostitusi Online Dikaitkan Dengan UU Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,” *UNES Law Review* 6, no. 4 (2024): 12353, https://doi.org/10.31933/unesrev.v6i4.2244.

as defined, refers to sending or disseminating electronic information to multiple individuals or parties, typically through digital platforms, which is a common characteristic of deepfake pornography's circulation. Similarly, "transmitting" involves sending such material directly to another party, a frequent method used to spread non-consensual pornography in private or public online spaces. "Making accessible" broadens the scope, capturing any action that leads to the exposure of explicit content to the public, even if it doesn't involve direct transmission or distribution. Crucially, the concept of "violating decency" under this law refers to the depiction of nudity, sexual organs, or sexual activities that contradict societal norms at the time and place of the offense. This interpretation of decency is fluid and adapts to the prevailing contemporary community standards, making it flexible enough to address the evolving nature of digital crimes like deepfake pornography. Given that deepfake pornography involves the non-consensual creation and dissemination of explicit content, this law provides a strong legal basis for prosecuting such acts. The law's provision that electronic content becomes "publicly known" when accessible to a large group of individuals, most of whom are unknown to each other, aligns directly with the nature of deepfake pornography's viral spread online. This underscores the law's relevance in regulating not just the act of creating such content, but also its widespread distribution.[63]

The penalty of the distribution of deepfake pornography can be addressed under Article 45, section (1). This provision stipulates that individuals who intentionally and without authority distribute, transmit, or make accessible electronic information or documents containing materials that violate societal norms, such as decency and morality, as outlined in Article 27, section (1), are subject to a maximum imprisonment of six years and/or a fine of up to Rp. 1,000,000,000 (one billion rupiahs). This provision plays a crucial role in addressing the growing issue of deepfake pornography, as it applies to the intentional distribution of electronically manipulated content that violates decency. The broader scope of this law allows for the prosecution not only of those who create deepfake pornography but also of those who facilitate its distribution, access, or transmission. This aligns with Balkin's (2019) argument that the crime of pornography includes not only the creation of explicit content but also the facilitation of access to such material, thereby extending criminal liability to any individual who provides the means to distribute or access pornographic content. In the case of deepfake pornography, this legal framework serves as a vital tool for regulating and penalizing the spread of non-consensual, sexually explicit content, reinforcing the need for stricter law enforcement to combat the misuse of technology for criminal purposes[64]

3.2.2 Criminal responsibility of Perperator Based on Law on Personal Data Protection

Article 66 of the Law on Personal Data Protection (PDP) stipulates criminal sanctions against any party that unlawfully obtains, uses, processes, or discloses personal data, leading to harm or damage to an individual's privacy and dignity.[65] This provision

[63] Nurul aulia et al., "Protection of ITE Law Against Sexting By Teenagers," *Proceeding of The 1st International Conference of Religion Health Science and Technology* 1, no. 1 (2024): 400.

[64] Aldo Andrieyan Putra Makaminan and Eko Soponyono, "The Urgency of Criminal Code Bill Ratification in Criminal Law Policy Frame on The Spreading of Pornographic Content Offence," *Law Reform* 17, no. 1 (2021): 41.

[65] Lilik Prihatin, Muhammad Achwan, and Citra Candra Dewi, "Kajian Yuridis Regulasi Perlindungan Hukum Terhadap Penyalahgunaan Data Privasi Dalam Perspektif Undang-

plays a crucial role in addressing offenses associated with deepfake pornography, which frequently involves the unauthorized collection and manipulation of personal data, such as images, videos, or the likenesses of individuals, to fabricate sexually explicit content. [66] Such unauthorized use and public dissemination of manipulated content without the individual's consent not only breach privacy laws but also represent a serious violation of personal integrity[67], often resulting in psychological distress, reputational harm, and even social ostracization for the victims.[68][69] In the context of deepfake pornography, perpetrators engage in acts that are both technologically sophisticated and inherently malicious, implicating them under overlapping data protection and cybercrime laws.[70] The PDP Law, through Article 66, underscores the importance of addressing such offenses by enhancing scrutiny on perpetrators' actions and intent.[71] By emphasizing both the intent (mens rea) and the tangible acts (actus reus) involved in the unauthorized use of personal data[72], the provision effectively ensures that criminal liability extends to those who knowingly and maliciously exploit sensitive personal data for unlawful purposes.[73] This legal approach not only highlights the intent of lawmakers to prioritize personal data protection but also reinforces the imperative need for stringent regulatory measures that protect victims and act as a deterrent to potential offenders by imposing severe penalties, such as imprisonment and significant financial sanctions. This illustrates the gravity with which data misuse in cases of technology-driven sexual exploitation is addressed.

Article 68 of the Personal Data Protection Law (PDP Law) provides a crucial layer of criminal liability for perpetrators of deepfake pornography, particularly those who deliberately fabricate or falsify personal data. [74] This provision stipulates that any

Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *UNES Law Review* 5, no. 4 (2023): 4136, https://doi.org/10.31933/unesrev.v5i4.731.

[66] Putri Nurayu Wafda, Abdul Rokhim, and Nofi Sri Utami, "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Dalam Aplikasi Pinjaman Online," *DIVERSI : Jurnal Hukum; Vol 10 No 1 (2024): Diversi Jurnal HukumDO - 10.32503/Diversi.V10i1.4842* 10, no. 1 (July 25, 2024): 40, https://doi.org/10.32503/diversi.v10i1.4842.

[67] Jaspreet Kaur, Kapil Sharma, and MP Singh, "Exploring the Depth: Ethical Considerations, Privacy Concerns, and Security Measures in the Era of Deepfakes," in *Navigating the World of Deepfake Technology* (IGI Global, 2024), 157.

[68] Emily Chapman, "Unveiling the Threat-AI and Deepfakes' Impact on Women," *Eagle Scholar*, 2024, 9, https://scholar.umw.edu/student_research/567.

[69] Debarati Halder and Subhajit Basu, "Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment and Legal Challenges in India," *Information & Communications Technology Law*, 2024, 5, https://doi.org/10.1080/13600834.2024.2408914.

[70] Audrey de Rancourt-Raymond and Nadia Smaili, "The Unethical Use of Deepfakes," *Journal of Financial Crime* 30, no. 4 (January 1, 2023): 1066, https://doi.org/10.1108/JFC-04-2022-0090.

[71] Inggou David Purba, "Delik Pidana Yang Dapat Terjadi Dalam Virtual Reality Dan Akibat Hukumnya," *Jurnal Tana Mana* 5, no. 1 (2024): 82, https://doi.org/10.33648/jtm.v5i1.474.

[72] Alessandro Stasi, "Actus Reus and Mens Rea," in *General Principles of Thai Criminal Law*, ed. Alessandro Stasi (Singapore: Springer Singapore, 2021), 25, https://doi.org/10.1007/978-981-15-8708-5_3.

[73] Ulfia Hasanah and Budiman Basarah, "Transaksi Online Menurut Hukum Perjanjian Dikaitkan Dengan Pelindungan Konsumen Di Indonesia," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasiona* 12, no. 2 (October 7, 2023): 315, http://dx.doi.org/10.33331/rechtsvinding.v12i2.1224.

[74] Hari Sutra Disemadi et al., "Perlindungan Data Pribadi Di Era Digital: Mengapa Kita Perlu Peduli?," *Sang Sewagati Journal* 1, no. 2 (2023): 79, https://doi.org/10.37253/sasenal.v1i2.8579.

individual who intentionally creates false personal data or forges personal data for self-gain or to benefit another party, resulting in potential harm to others, faces a maximum prison sentence of six years and/or a fine of up to six billion rupiah.[75] This is particularly relevant in cases of deepfake pornography, where offenders often exploit technology to manipulate victims' personal images or data without consent, aiming for various types of gain, whether through notoriety, financial profit, or harm to the victim's reputation.[76]

The unauthorized manipulation and falsification of personal data in deepfake cases, such as altered images, videos, or other aspects of an individual's identity, pose significant threats to victims' privacy and dignity.[77] Article 68 strengthens the legal framework by imposing stringent penalties for the deliberate falsification of personal data, emphasizing the necessity of establishing intent (mens rea) and concrete actions (actus reus) during legal proceedings.[78] This framework serves as a strong deterrent by highlighting the severe criminal consequences for those who unlawfully exploit personal data for personal benefit, without consideration of the damaging impacts on the victims involved.[79]

This provision supports a broader legal ecosystem that demands greater accountability in the use of personal data in the digital era.[80] By enforcing stringent penalties, Article 68 demonstrates Indonesia's commitment to protecting its citizens from the misuse of technology that threatens fundamental human rights such as privacy and dignity.[81] In relation to deepfake pornography, this provision closes existing legal loopholes by providing victims with a robust avenue to seek justice and hold offenders criminally accountable.[82] The integration of the PDP Law with the Information and Electronic

[75] Jofani Johanes Maramis, Adi Tirto Koesoemo, and Boby Pinasang, "Analisis Yuridis Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online," *LEX PRIVATUM* 13, no. 2 (2024): 9.

[76] Yolanda Frisky Amelia, Arfan Kaimuddin, and Hisbul Luthfi Ashsyarofi, "Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia," *Dinamika* 30, no. 1 (2024): 9680.

[77] Dr Rupak Kumar Joshi Aman Gautam, Aastha Narula, and Neha Sharma, "Mitigating Human Rights Violations Caused by Deepfake Technology," *Library Progress International* 44, no. 3 (2024): 4630.

[78] Muhammad Alfian Kusnaldi, Nadira Fadila Syani, and Yukiatiqa Afifah, "Perlindungan Data Pribadi Dalam Penyelenggaraan Pemilu: Tantangan Dan Tawaran," *Lex Renaissance* 7, no. 4 (August 3, 2023): 721, https://doi.org/10.20885/JLR.vol7.iss4.art3.

[79] Aulia Dean Puspita Sari and Erny Herlin Setyorini, "Perlindungan Hukum Data Pribadi Yang Disalahgunakan Untuk Kegiatan Prostitusi," *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance* 2, no. 1 (April 30, 2022): 719, https://doi.org/10.53363/bureau.v2i1.162.

[80] Ainun Najib, "Perlindungan Hukum Keamanan Data Cyber Notary Berdasarkan Undang-Undang Perlindungan Data Pribadi," *ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan* 7, no. 1 (December 30, 2024): 56, https://doi.org/10.23920/acta.v7i1.1680.

[81] Cindy Gladys Pratiwi Sianturi, Roida Nababan, and Ria Juliana Siregar, "Peran Hukum Dalam Melindungi Data Pribadi," *Innovative: Journal Of Social Science Research* 4, no. 5 (September 15, 2024): 14, https://doi.org/10.31004/innovative.v4i5.15192.

[82] Ni Made Dwi Gayatri Putri, Ni Luh Made Mahendrawati, and Ni Made Puspasutari Ujianti, "Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Jurnal Preferensi Hukum* 5, no. 2 (September 4, 2024): 243, https://doi.org/10.22225/jph.5.2.8087.240-245.

Transactions Law (ITE Law)[83], offers a comprehensive and cohesive legal mechanism to address the multifaceted harms posed by deepfake pornography, ensuring that offenders are held fully accountable for their actions.[84][85]

3.2.3 Criminal responsibility of Perperator Based on Law No. 44 of 2008 on Pornography

In analyzing the criminal responsibility for disseminating deepfake pornographic content under Law No. 44 of 2008 on Pornography, particularly through the lens of Article 4, paragraph (1), several key prohibitions become relevant. This law expressly forbids the production, creation, duplication, distribution, broadcasting, import, export, offering, sale, rental, or provision of pornography that explicitly features certain forms of sexual content. These include: (a) sexual intercourse, including deviant sexual acts; (b) sexual violence; (c) masturbation or onanism; (d) nudity or displays suggesting nudity; (e) genitalia; and (f) child pornography.[86]

When applied to the dissemination of deepfake pornography, the actions of individuals who distribute or make available these materials fall squarely within the scope of the prohibitions listed in Article 4. Deepfake pornography, which often features realistic but fabricated depictions of sexual acts involving non-consenting individuals, including nudity and explicit content, clearly aligns with several categories outlined in this law, especially items (a), (d), and (e).

From a legal standpoint, the use of deepfake technology to create and distribute pornographic content may not involve actual sexual acts or consent from those depicted, but the explicit nature of these deepfakes violates the prohibition against the distribution of indecent or sexually explicit materials. This expands the definition of pornographic offenses beyond traditional means of production and dissemination to include digitally manipulated content that may seem real but is entirely fabricated.

The broad scope of prohibited acts under the Pornography Law, which includes the creation, dissemination, and provision of such content, ensures that individuals involved in the spread of deepfake pornography can be held criminally responsible, regardless of whether they were the original creators or merely distributors. The severity of the penalties for violating these provisions reflects the Indonesian government's intent

[83] Ambar Alimatur Rosyidah, Farah Fajriyah, and Rahayu Rahayu, "Cyber Crime Against Women's Personal Data on Online Platforms and The Role of PDP Laws," *Jurnal Komunikasi Indonesia* 13, no. 2 (n.d.): 258, https://doi.org/10.7454/jkmi.v13i2.1229.

[84] Siti Yuniarti, "Protection Of Indonesia's Personal Data After Ratification Of Personal Data Protection Act," *Progressive Law Review* 4, no. 02 (November 23, 2022): 67, https://doi.org/10.36448/plr.v4i02.85.

[85] M Riansyah Aksar Tarigan and Patricia Riniwigati, "Comparison of the Republic of Indonesia ITE Law No 19 Of 2016 with PDP Law No 27 of 2022 and the Role of the Police in Handling Cases Of Personal Data Dissemination (Doxing)," *Path of Science* 10, no. 7 (2024): 5047, http://dx.doi.org/10.22178/pos.106-35.

[86] Anastasia Pritahayu Ratih Daniyati et al., "Pemidanaan Terhadap Pelaku Penyebaran Konten Pornografi Melalui Internet Perspektif Teori Keadilan Bermartabat," *Collegium Studiosum Journal* 7, no. 1 (June 19, 2024): 42, https://doi.org/10.56301/csj.v7i1.1202.

to regulate and curb all forms of pornography, including technologically advanced iterations such as deepfakes.

In analyzing the criminal responsibility for disseminating deepfake pornographic content under Law No. 44 of 2008 on Pornography, particularly in relation to Article 29, the law provides strict sanctions for individuals involved in the production, creation, duplication, distribution, broadcasting, import, export, offering, sale, rental, or provision of pornographic materials as outlined in Article 4, paragraph (1). The law mandates that any person found guilty of these offenses is subject to a minimum imprisonment of 6 months and a maximum of 12 years, along with a fine ranging from IDR 250 million to IDR 6 billion.[87]

Article 29 explicitly lists actions such as producing, making, duplicating, distributing, broadcasting, importing, exporting, offering, selling, renting, or providing pornographic content.[88] In the case of deepfake pornography, these actions could include the use of AI tools to fabricate explicit material featuring the likeness of individuals, as well as uploading, sharing, or otherwise making such content available to the public via digital platforms. This broad range of activities ensures that individuals at different stages of content creation and dissemination can be held criminally liable. The law does not differentiate between those who directly create deepfake pornography and those who enable its distribution or public access, thus capturing the entire supply chain of deepfake content.

Criminal responsibility under this law requires proving the subjective element of intent, or "mens rea."[89] This means that the perpetrator must have knowingly engaged in the act of producing or disseminating deepfake pornography. The intention is central to establishing liability, as the individual must be aware that they are creating or sharing explicit content, often with the knowledge that it may harm the individuals whose likenesses are used without consent.[90] In the case of deepfake pornography, the absence of consent from the individuals depicted in the content further exacerbates the criminal nature of the act, as it infringes on personal rights and dignity. The law's requirement that the perpetrator acts "without authorization" is particularly relevant to deepfake cases, where the use of someone's image without their permission is inherently a violation of their rights.

[87] Melianggraini, Irman Syahriar, and Khairunnisah, "Tinjauan Terhadap Tindak Pidana Pornografi Dalam Dunia Maya Berdasarkan Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi," *LEGALITAS : Jurnal Ilmiah Ilmu Hukum* 7, no. 2 (2022): 95, https://doi.org/10.31293/lg.v7i2.7594.

[88] Veronica Agustina Darida and Slamet Tri Wahyudi, "Politik Kriminal Optimalisasi Perlindungan Hukum Terhadap Anak Sebagai Korban Tindak Pidana Revenge Porn," *Jurnal Interpretasi Hukum* 5, no. 2 (2024): 893, https://doi.org/10.22225/juinhum.5.1.8502.889-902.

[89] Rizki Kurniawati, Armansyah ., and Rocky Marbun, "Identify Mens Rea in Language Use from a Criminal Law Perspective," *KnE Social Sciences* 9, no. 1 (January 5, 2024): 872, https://doi.org/10.18502/kss.v8i21.14803.

[90] Kumar Apurv, "Mens Rea of a Criminal – A Short Review," *International Journal of Advanced Research and Interdisciplinary Scientific Endeavours* 1, no. 7 (July 30, 2024): 147, https://doi.org/10.61359/IJARISE2434.

The objective element, or "actus reus," refers to the actual conduct of producing, distributing, or making available the pornographic content. Deepfake pornography typically involves the manipulation of images or videos to create explicit material, which is then disseminated through digital platforms, making it accessible to a wide audience.[91] The law covers all methods of dissemination, including uploading content to websites, sharing it on social media, or providing access through online links or forums. By encompassing such a wide variety of actions, the law ensures that individuals who contribute to the spread of deepfake pornography, whether directly or indirectly, can be prosecuted. In this context, those who run websites, provide hosting services, or even share links to deepfake content may also be held criminally liable under Article 29.[92]

The sanctions provided under Article 29 are severe, reflecting the seriousness with which the law views pornography-related offenses. Imprisonment terms range from 6 months to 12 years, and fines can reach up to IDR 6 billion. These penalties serve as a deterrent, especially in cases where deepfake pornography is disseminated on a large scale. The financial penalties also reflect the significant harm that can be caused to individuals whose likenesses are used in deepfake content, as well as the broader societal harm caused by the spread of explicit material. The high financial penalties are meant to dissuade individuals and organizations from engaging in or facilitating the distribution of such content, recognizing the far-reaching consequences of deepfake pornography on victims' reputations, mental health, and personal dignity. The severe penalties outlined in Article 29 emphasize the Indonesian government's stance on curbing not only traditional forms of pornography but also the dissemination of digitally manipulated content like deepfakes. The law seeks to address the harm caused by these materials, particularly when they involve non-consensual use of an individual's likeness, as this can cause significant damage to the victim's reputation and privacy.[93]

The application of Law No. 44 of 2008 to deepfake pornography highlights the adaptability of Indonesian criminal law to new technological challenges. While deepfake technologies are relatively new, their use in creating non-consensual explicit content falls squarely within the legal definition of pornography. The law's comprehensive approach to criminalizing both the creation and distribution of pornographic materials ensures that deepfake pornography is treated as a serious offense.[94] Furthermore, the law's emphasis on "providing access" or "making available" pornography broadens its application to modern digital platforms, where deepfake content can be easily shared

[91] Alaa Saud, "Criminal Liability about the Use of Artificial Intelligence: Investigating the Actus Reus Element of AI-Driven Technology," *American Journal of Law* 6, no. 1 (2024): 3, https://doi.org/10.47672/ajl.1648.

[92] Yulia Hesti et al., "Korelasi Antara Kebebasan Berekspresi Dalam Peningkatan Kasus Kejahatan Asusila Di Media Digital (Sextorsi)," *Journal of Law Education and Business* 2, no. 1 (2024): 526, https://doi.org/10.57235/jleb.v2i1.1890.

[93] Syafirah Khansa Aribah Milansari, "Pertanggungjawaban Pidana Terhadap Pelaku Perbuatan Kekerasan Berbasis Gender Online Dengan Tipe Morphing," *Jurist-Diction* 7, no. 1 (2023): 152, https://e-journal.unair.ac.id/JD/article/view/54841.

[94] Benjamin N. Jacobsen and Jill Simpson, "The Tensions of Deepfakes," *Information, Communication & Society* 27, no. 6 (April 25, 2024): 1099, https://doi.org/10.1080/1369118X.2023.2234980.

across networks, often without the knowledge or consent of the individuals depicted.[95] By applying traditional legal frameworks to contemporary technological threats, Indonesia demonstrates a forward-looking approach to protecting individual rights in the digital age.

When applied to the dissemination of deepfake pornography, this article has significant implications. Deepfake pornography involves the use of artificial intelligence to create realistic but fabricated explicit content, often without the consent of those depicted. This technological manipulation falls within the scope of prohibited acts under Article 4, which addresses the creation and distribution of pornographic content. By distributing or making available deepfake pornographic material, individuals are effectively violating the legal prohibitions on the dissemination of pornography.[96] The imposition of both imprisonment and substantial financial penalties underscores the seriousness with which the Indonesian legal system treats offenses related to pornography, including the modern challenge posed by deepfakes. Given the broad definition of pornography in Law No. 44 of 2008, the application of these sanctions to deepfake content represents an important step in adapting legal frameworks to the evolving nature of digital crimes.[97]

4. Conclussion

The proliferation of deepfake pornography represents a critical evolution in cybercrime, leveraging advanced technologies like Generative Adversarial Networks (GANs) to autonomously create hyper-realistic, nonconsensual sexual content, posing severe legal, social, and ethical challenges. This crime disproportionately targets women, with 96% of deepfake content involving female victims, reducing them to objects of exploitation and reinforcing gender-based violence. The rapid dissemination of deepfakes, particularly through social media, makes it difficult to mitigate harm, as false content spreads faster than verified information, leading to long-lasting psychological, reputational, and social damage. Deepfake pornography's violation of sexual privacy and personal dignity raises profound concerns, as victims face dehumanization, stigmatization, and, in some cases, the need to alter their identities to escape the associated harassment. International organizations and legal experts highlight the urgent need for comprehensive legal reforms to address this emerging threat, with a focus on protecting sexual privacy and ensuring accountability for perpetrators. In Indonesia, as in other countries, the lack of adequate legal frameworks complicates efforts to combat deepfake pornography,

[95] Lalu Putra Kurniawan, Fathur Rauzi, and Ika Yuliana Susilawati, "Tinjauan Yuridis Terhadap Tindak Pidana Kejahatan Pornografi Bedasarkan Undang-Undang Informasi Transaksi Elektronik: (Studi Putusan Nomor 82/PID.B/2023/PN.SBG)," *Unizar Recht Journal (URJ)* 3, no. 1 (April 29, 2024): 97.

[96] Bruce Anzward et al., "Perlindungan Hukum Terhadap Anak Sebagai Korban Tindak Pidana Pornografi Dalam Ruang Siber Di Kota Balikpapan," *UNES Law Review* 6, no. 4 (2024): 270, https://doi.org/10.31933/unesrev.v6i4.

[97] Alfira Destriannisya, "Analisis Pornografi Balas Dendam (Revenge Porn) Dan Regulasinya Di Indonesia," *Journal of Contemporary Law Studies* 1, no. 3 (May 5, 2024): 123, https://doi.org/10.47134/lawstudies.v2i2.2222.

necessitating a more robust, nuanced approach that balances the protection of fundamental human rights with the rapid advancement of technology.

Criminal liability for perpetrators of deepfake pornography in Indonesia under various legal frameworks, including the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), and Law No. 44 of 2008 on Pornography, reveals a comprehensive legal response to this evolving cybercrime. The UU ITE addresses the distribution of content that violates decency, emphasizing intentional actions without legal rights and the broad scope of dissemination methods for such material. The UU PDP complements this by targeting the unauthorized use and manipulation of personal data, focusing on protecting privacy and dignity, with significant penalties for those engaging in data falsification and misuse. Finally, the Pornography Law reinforces the regulation of explicit content, encompassing digitally manipulated depictions and ensuring that all stages of deepfake content creation and distribution are legally scrutinized. This multi-layered legal approach underscores Indonesia's commitment to combating deepfake pornography through stringent criminal responsibility mechanisms, effectively safeguarding victims' rights, and promoting technological accountability in a rapidly changing digital landscape.

References

A. Shaji George and A. S. Hovan George. "Deepfakes: The Evolution of Hyper Realistic Media Manipulation." *Partners Universal Innovative Research Publication* 1, no. 2 (December 11, 2023): 58–74. https://doi.org/10.5281/zenodo.10148558.

Abdulqader M Almars. "Deepfakes Detection Techniques Using Deep Learning: A Survey." *Journal of Computer and Communications* 9, no. 5 (2021). https://doi.org/10.4236/jcc.2021.95003.

Agnieszka McPeak. "The Threat of Deepfakes in Litigation: Raising the Authentication Bar to Combat Falsehood." *Vanderbilt Journal of Entertainment and Technology Law* 23, no. 2 (2021). https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss2/5.

Alaa Saud. "Criminal Liability about the Use of Artificial Intelligence: Investigating the Actus Reus Element of AI-Driven Technology." *American Journal of Law* 6, no. 1 (2024). https://doi.org/10.47672/ajl.1648.

Aldo Andrieyan Putra Makaminan and Eko Soponyono. "The Urgency of Criminal Code Bill Ratification in Criminal Law Policy Frame on The Spreading of Pornographic Content Offence." *Law Reform* 17, no. 1 (2021).

Alfira Destriannisya. "Analisis Pornografi Balas Dendam (Revenge Porn) Dan Regulasinya Di Indonesia." *Journal of Contemporary Law Studies* 1, no. 3 (May 5, 2024): 115–28. https://doi.org/10.47134/lawstudies.v2i2.2222.

Al-khazrajı, Samer Hussain, Hassan Hadi Saleh, Adil Ibrahim Khalıd, and Israa Adnan Mıshkhal. "Impact of Deepfake Technology on Social Media: Detection, Misinformation and Societal Implications." *The Eurasia Proceedings of Science Technology Engineering and Mathematics* 23 (September 2023): 429–41. https://doi.org/10.55549/epstem.1371792.

Aman Gautam, Dr Rupak Kumar Joshi, Aastha Narula, and Neha Sharma. "Mitigating Human Rights Violations Caused by Deepfake Technology." *Library Progress International* 44, no. 3 (2024): 4628–37.

Amelia, Yolanda Frisky, Arfan Kaimuddin, and Hisbul Luthfi Ashsyarofi. "Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan

Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia." *Dinamika* 30, no. 1 (2024): 9675–91.

Anastasia Pritahayu Ratih Daniyati, Asri Winnie Irawati Sularto, Naufan Mufti Sudarmono, Surya Lung, Zahra, and Rizky Karo Karo. "Pemidanaan Terhadap Pelaku Penyebaran Konten Pornografi Melalui Internet Perspektif Teori Keadilan Bermartabat." *Collegium Studiosum Journal* 7, no. 1 (June 19, 2024): 37–44. https://doi.org/10.56301/csj.v7i1.1202.

Anne Pechenik Gieseke. ""The New W 'The New Weapon of Choice Eapon of Choice': Law' ": Law's Current Inability t Ent Inability to Properly Address Deepfake Pornography." *Vanderbilt Law Review* 73, no. 5 (2020). https://scholarship.law.vanderbilt.edu/vlr/vol73/iss5/4.

Armia, Muhammad Siddiq. *Penentuan Metode & Pendekatan Penelitian Hukum*. Banda Aceh: Lembaga Kajian Konstitusi Indonesia, 2022.

Barber, Alex. "Freedom of Expression Meets Deepfakes." *Synthese* 202, no. 2 (July 20, 2023): 40. https://doi.org/10.1007/s11229-023-04266-4.

Benjamin T. Suslavich. "Nonconsensual Deepfakes: A" Deep Problem" for Victims." *Journal of Science and Technology* 33 (2023).

Brooklynn Armesto-Larson. "Nonconsensual Pornography: Criminal Law Solutions to a Worldwide Problem." *Oregon Review Of International Law* 21 (2020).

Bruce Anzward, Elvina Avriani, Rivaldi Nugraha, and Atika Fitriani. "Perlindungan Hukum Terhadap Anak Sebagai Korban Tindak Pidana Pornografi Dalam Ruang Siber Di Kota Balikpapan." *UNES Law Review* 6, no. 4 (2024). https://doi.org/10.31933/unesrev.v6i4.

Burkell, Jacquelyn, and Chandell Gosse. "Nothing New Here: Emphasizing the Social and Cultural Context of Deepfakes." *First Monday* 24, no. 12 (December 2, 2019). https://doi.org/10.5210/fm.v24i12.10287.

Catherine de Weever and Sebastian Wilczek. "Deepfake Detection through PRNU and Logistic Regression Analyses." Research Paper. Amsterdam: University of Amsterdam, May 7, 2020.

Chapman, Emily. "Unveiling the Threat-AI and Deepfakes' Impact on Women." *Eagle Scholar*, 2024. https://scholar.umw.edu/student_research/567.

Chidera Okolie. "Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns." *Journal of International Women's Studies* 25, no. 2 (2023).

Danielle Keats Citron. "Sexual Privacy." *The Yale Law Journal Company* 128, no. 7 (2019).

Di Silvestro, Lorenzo, and Cristina Iurissevich. "Pornografia Contemporanea: Il Deepfake Come Forma Di Abuso." *European Public & Social Innovation Review* 9 (July 24, 2024): 1–20. https://doi.org/10.31637/epsir-2024-370.

Disemadi, Hari Sutra, Lu Sudirman, Junimart Girsang, and Arwa Meida Aninda. "Perlindungan Data Pribadi Di Era Digital: Mengapa Kita Perlu Peduli?" *Sang Sewagati Journal* 1, no. 2 (2023): 66–90. https://doi.org/10.37253/sasenal.v1i2.8579.

Emily Pascale. "Deeply Dehumanizing, Degrading, And Violating: Deepfake Pornography And The Path To Legal Recourse." *Syracuse Law Review* 73 (2023).

Eric Kocsis. "Deepfakes, Shallowfakes, and the Need for a Private Right of Action." *DICKINSON LAW REVIEW* 126, no. 2 (2022).

Geeta Singh Chetry and Uzzal Sharma. "Emerging Technologies as a Tool for Cybercrime Against Women and Children." *SSRN Electronic Journal*, 2024. https://dx.doi.org/10.2139/ssrn.4765788.

Gowri Dev and Akshay Pramodh. "An Age Where Eyes Can't Be Trusted: Image Manipulation Through Deepfakes." *DNLU Student Law Journal* 2 (2023).

H. A. Khalil and S. A. Maged. "Deepfakes Creation and Detection Using Deep Learning." In *2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, 1–4, 2021. https://doi.org/10.1109/MIUCC52538.2021.9447642.

Halder, Debarati, and Subhajit Basu. "Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment and Legal Challenges in India." *Information & Communications Technology Law*, 2024, 1–24. https://doi.org/10.1080/13600834.2024.2408914.

Hancock, Jeffrey T., and Jeremy N. Bailenson. "The Social Impact of Deepfakes." *Cyberpsychology, Behavior, and Social Networking* 24, no. 3 (March 1, 2021): 149–52. https://doi.org/10.1089/cyber.2021.29208.jth.

Hasanah, Ulfia, and Budiman Basarah. "Transaksi Online Menurut Hukum Perjanjian Dikaitkan Dengan Pelindungan Konsumen Di Indonesia." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasiona* 12, no. 2 (October 7, 2023). http://dx.doi.org/10.33331/rechtsvinding.v12i2.1224.

Hilbert, Martin. "Digital Technology and Social Change: The Digital Transformation of Society from a Historical Perspective." *Dialogues in Clinical Neuroscience* 22, no. 2 (June 30, 2020): 189–94. https://doi.org/10.31887/DCNS.2020.22.2/mhilbert.

Jacobsen, Benjamin N., and Jill Simpson. "The Tensions of Deepfakes." *Information, Communication & Society* 27, no. 6 (April 25, 2024): 1095–1109. https://doi.org/10.1080/1369118X.2023.2234980.

Jennifer Laffier and Aalyia Rehman. "Deepfakes and Harm to Women." *Journal of Digital Life and Learning* 3, no. 1 (2023). https://doi.org/10.51357/jdll.v3i1.218.

Kareem Gibson. "Deepfakes and Involuntary Pornography: Can Our Current Legal Framework Address This Technology." *Wayne Law Review* 66 (2020).

Kate Kobriger, Janet Zhang, Andrew Quijano, and Joyce Guo. "Out of Our Depth with Deep Fakes: How the Law Fails Victims of Deep Fake Nonconsensual Pornography." *Richmond Journal of Law & Technology* XXVIII, no. 2 (n.d.).

Kaur, Jaspreet, Kapil Sharma, and MP Singh. "Exploring the Depth: Ethical Considerations, Privacy Concerns, and Security Measures in the Era of Deepfakes." In *Navigating the World of Deepfake Technology*, 141–65. IGI Global, 2024.

Kirchengast, Tyrone. "Deepfakes and Image Manipulation: Criminalisation and Control." *Information & Communications Technology Law* 29, no. 3 (September 1, 2020): 308–23. https://doi.org/10.1080/13600834.2020.1794615.

Kumar Apurv. "Mens Rea of a Criminal – A Short Review." *International Journal of Advanced Research and Interdisciplinary Scientific Endeavours* 1, no. 7 (July 30, 2024): 146–48. https://doi.org/10.61359/IJARISE2434.

Kwok, Andrei O. J., and Sharon G. M. Koh. "Deepfake: A Social Construction of Technology Perspective." *Current Issues in Tourism* 24, no. 13 (July 3, 2021): 1798–1802. https://doi.org/10.1080/13683500.2020.1738357.

Lalu Putra Kurniawan, Fathur Rauzi, and Ika Yuliana Susilawati. "Tinjauan Yuridis Terhadap Tindak Pidana Kejahatan Pornografi Bedasarkan Undang-Undang Informasi Transaksi Elektronik: (Studi Putusan Nomor 82/PID.B/2023/PN.SBG)." *Unizar Recht Journal (URJ)* 3, no. 1 (April 29, 2024): 93–104.

Lee, Gihun, and Mihui Kim. "Deepfake Detection Using the Rate of Change between Frames Based on Computer Vision." *Sensors* 21, no. 21 (2021). https://doi.org/10.3390/s21217367.

Lorenzo DAMI. "Analysis and Conceptualization of Deepfake Technology as Cyber Threat." School of Political Science "Cesare Alfieri," 2021.

Mania, Karolina. "Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study." *Trauma, Violence, & Abuse* 25, no. 1 (January 1, 2024): 117–29. https://doi.org/10.1177/15248380221143772.

———. "The Legal Implications and Remedies Concerning Revenge Porn and Fake Porn: A Common Law Perspective." *Sexuality & Culture* 24, no. 6 (December 1, 2020): 2079–97. https://doi.org/10.1007/s12119-020-09738-0.

Maramis, Jofani Johanes, Adi Tirto Koesoemo, and Boby Pinasang. "Analisis Yuridis Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online." *LEX PRIVATUM* 13, no. 2 (2024).

Maryam Taeb and Hongmei Chi. "Comparison of Deepfake Detection Techniques through Deep Learning." *Journal of Cybersecurity and Privacy* 2, no. 1 (2022). https://doi.org/10.3390/jcp2010007.

Matthew B. Kugler and Carly Pace. "Deepfake Privacy: Attitudes and Regulation." *Northwestern Public Law Research Paper* 116, no. 3 (2021). https://dx.doi.org/10.2139/ssrn.3781968.

Melianggraini, Irman Syahriar, and Khairunnisah. "Tinjauan Terhadap Tindak Pidana Pornografi Dalam Dunia Maya Berdasarkan Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi." *LEGALITAS : Jurnal Ilmiah Ilmu Hukum* 7, no. 2 (2022). https://doi.org/10.31293/lg.v7i2.7594.

Miha Šepec and Melanija Lango. "Virtual Revenge Pornography as a New Online Threat to Sexual Integrity." *Balkan Social Science Review* 15 (2020).

Mika Westerlund. "The Emergence of Deepfake Technology: A Review." *Technology Innovation Management Review* 9, no. 11 (2019). https://doi.org/10.22215/timreview/1282.

Miriam Meckel and Léa Steinacker. "Hybrid Reality: The Rise of Deepfakes and Diverging Truths." *Morals & Machines* 1, no. 1 (2021). https://doi.org/10.5771/2747-5174-2021-1-10.

Moncarol Y. Wang. "Don't Belie 't Believe Your Eyes: Fighting Deepfak Es: Fighting Deepfaked Nonconsensual Ed Nonconsensual Pornography with Tort Law." *University of Chicago Legal Forum* 2022 (2023).

Muhaimin, Muhaimin. *Metode Penelitian Hukum*. Mataram: Mataram University Press, 2020.

Muhammad Alfian Kusnaldi, Nadira Fadila Syani, and Yukiatiqa Afifah. "Perlindungan Data Pribadi Dalam Penyelenggaraan Pemilu: Tantangan Dan Tawaran." *Lex Renaissance* 7, no. 4 (August 3, 2023): 710–25. https://doi.org/10.20885/JLR.vol7.iss4.art3.

Nagel, Emily van der. "Verifying Images: Deepfakes, Control, and Consent." *Porn Studies* 7, no. 4 (October 1, 2020): 424–29. https://doi.org/10.1080/23268743.2020.1741434.

Najib, Ainun. "Perlindungan Hukum Keamanan Data Cyber Notary Berdasarkan Undang-Undang Perlindungan Data Pribadi." *ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan* 7, no. 1 (December 30, 2024): 43–59. https://doi.org/10.23920/acta.v7i1.1680.

Newton, Olivia B., and Mel Stanfill. "My NSFW Video Has Partial Occlusion: Deepfakes and the Technological Production of Non-Consensual Pornography." *Porn Studies* 7, no. 4 (October 1, 2020): 398–414. https://doi.org/10.1080/23268743.2019.1675091.

Nicolas Graber-Mitchell. "Artificial Illusions: Deepfakes as Speech." *Intersect* 14, no. 3 (2021). https://ssrn.com/abstract=3876862.

Nurul aulia, Ridwan, Syamsuddin, Hadijah, Didik Irawansah, Tiara, Sahrul Ramadhan, Syahrudin, and Imran. "Protection of ITE Law Against Sexting By Teenagers." *Proceeding of The 1st International Conference of Religion Health Science and Technology* 1, no. 1 (2024).

Nurul Qamar and Farah Syah Rezah. *Metode Penelitian Hukum: Doktrinal Dan Non-Doktrinal*. Makassar: CV. Social Politic Genius (SIGn), 2020.

Olivia Debroy and Bhargavi D Hemmige. "Psycho-Social Impact of Deepfake Content in Entertainment Media." *INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD* 10, no. 5 (2024). https://doi.org/:10.2015/IJIRMF/202405032.

Pavankumar Mulgund and Samina Lohawala. "Deepfake: The Lay of the Land." *ISACA JOURNA* 1 (2021).

Phillips, Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies." *Forensic Sciences* 2, no. 2 (2022): 379–98. https://doi.org/10.3390/forensicsci2020028.

Pierri, Francesco, and Stefano Ceri. "False News On Social Media: A Data-Driven Survey." *SIGMOD Rec.* 48, no. 2 (December 2019): 18–27. https://doi.org/10.1145/3377330.3377334.

Prihatin, Lilik, Muhammad Achwan, and Citra Candra Dewi. "Kajian Yuridis Regulasi Perlindungan Hukum Terhadap Penyalahgunaan Data Privasi Dalam Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *UNES Law Review* 5, no. 4 (2023): 4126–39. https://doi.org/10.31933/unesrev.v5i4.731.

Purba, Inggou David. "Delik Pidana Yang Dapat Terjadi Dalam Virtual Reality Dan Akibat Hukumnya." *Jurnal Tana Mana* 5, no. 1 (2024): 73–91. https://doi.org/10.33648/jtm.v5i1.474.

Putri, Ni Made Dwi Gayatri, Ni Luh Made Mahendrawati, and Ni Made Puspasutari Ujianti. "Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Jurnal Preferensi Hukum* 5, no. 2 (September 4, 2024): 240–45. https://doi.org/10.22225/jph.5.2.8087.240-245.

Rancourt-Raymond, Audrey de, and Nadia Smaili. "The Unethical Use of Deepfakes." *Journal of Financial Crime* 30, no. 4 (January 1, 2023): 1066–77. https://doi.org/10.1108/JFC-04-2022-0090.

Rangita de Silva de Alwis. "A Rapidly Shifting Landscape: Why Digitized Violence Is the Newest Category of Gender-Based Violence." *SciencesPo Law Review* 25 (2024).

Rebecca A. Delfino. "Pornographic Deepfak Aphic Deepfakes: The Case for F Es: The Case for Federal Criminalization of al Criminalization of Revenge Porn's NNext Tragic Act." *Fordham Law Review* 3 (2019).

Regina Rini and Leah Cohen. "Deepfakes, Deep Harms." *Journal of Ethics and Social Philosophy (JESP)* XXII, no. 2 (2022).

Riana Pfefferkorn. "'Deepfakes' in the Courtroom." *Boston University Public Interest Law Journal* 29, no. 2 (2020). https://ssrn.com/abstract=4321140.

Rizki Kurniawati, Armansyah ., and Rocky Marbun. "Identify Mens Rea in Language Use from a Criminal Law Perspective." *KnE Social Sciences* 9, no. 1 (January 5, 2024). https://doi.org/10.18502/kss.v8i21.14803.

Rosyidah, Ambar Alimatur, Farah Fajriyah, and Rahayu Rahayu. "Cyber Crime Against Women's Personal Data on Online Platforms and The Role of PDP Laws." *Jurnal Komunikasi Indonesia* 13, no. 2 (n.d.): 7. https://doi.org/10.7454/jkmi.v13i2.1229.

Ruddin, Isra and Subhan Zein SGN. "Evolution of Cybercrime Law in Legal Development in the Digital World." *Jurnal Multidisiplin Madani* 4, no. 1 (January 29, 2024): 168–73. https://doi.org/10.55927/mudima.v4i1.7962.

Sami Alanazi, Seemal Asif, and Irene Moulitsas. "Examining the Societal Impact and Legislative Requirements of Deepfake Technology: A Comprehensive Study." *International Journal of Social Science and Humanity* 14, no. 2 (2024). https://doi.org/10.18178/ijssh.2024.14.2.1194.

Sari, Aulia Dean Puspita, and Erny Herlin Setyorini. "Perlindungan Hukum Data Pribadi Yang Disalahgunakan Untuk Kegiatan Prostitusi." *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance* 2, no. 1 (April 30, 2022): 703–21. https://doi.org/10.53363/bureau.v2i1.162.

Sarre, Rick. "Perspectives on Policing Post-Pandemic Cybercrime." In *Cybercrime in the Pandemic Digital Age and Beyond*, edited by Russell G. Smith, Rick Sarre, Lennon Yao-Chung Chang, and Laurie Yiu-Chung Lau, 173–92. Cham: Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-29107-4_9.

Sarre, Rick, Laurie Yiu-Chung Lau, and Lennon Y.C. Chang. "Responding to Cybercrime: Current Trends." *Police Practice and Research* 19, no. 6 (November 2, 2018): 515–18. https://doi.org/10.1080/15614263.2018.1507888.

Sianturi, Cindy Gladys Pratiwi, Roida Nababan, and Ria Juliana Siregar. "Peran Hukum Dalam Melindungi Data Pribadi." *Innovative: Journal Of Social Science Research* 4, no. 5 (September 15, 2024): 2607–24. https://doi.org/10.31004/innovative.v4i5.15192.

Siti Yuniarti. "Protection Of Indonesia's Personal Data After Ratification Of Personal Data Protection Act." *Progressive Law Review* 4, no. 02 (November 23, 2022): 54–68. https://doi.org/10.36448/plr.v4i02.85.

Sloot, Bart van der, and Yvette Wagensveld. "Deepfakes: Regulatory Challenges for the Synthetic Society." *Computer Law & Security Review* 46 (September 1, 2022): 105716. https://doi.org/10.1016/j.clsr.2022.105716.

Srijan Kumar and Neil Shah. "False Information on Web and Social Media: A Survey." *ArXiv* 1, no. 1 (2018). https://doi.org/10.48550/arXiv.1804.08559.

Stasi, Alessandro. "Actus Reus and Mens Rea." In *General Principles of Thai Criminal Law*, edited by Alessandro Stasi, 25–30. Singapore: Springer Singapore, 2021. https://doi.org/10.1007/978-981-15-8708-5_3.

Syafirah Khansa Aribah Milansari. "Pertanggungjawaban Pidana Terhadap Pelaku Perbuatan Kekerasan Berbasis Gender Online Dengan Tipe Morphing." *Jurist-Diction* 7, no. 1 (2023). https://e-journal.unair.ac.id/JD/article/view/54841.

Tarigan, M Riansyah Aksar, and Patricia Riniwigati. "Comparison of the Republic of Indonesia ITE Law No 19 Of 2016 with PDP Law No 27 of 2022 and the Role of the Police in Handling Cases Of Personal Data Dissemination (Doxing)." *Path of Science* 10, no. 7 (2024): 5031–48. http://dx.doi.org/10.22178/pos.106-35.

Vera Rimbawani Sushanty. "Pornografi Dunia Maya Menurut Kitab Undang-Undang Hukum Pidana, Undang-Undang Pornografi Dan Undang-Undang Informasi Elektronik." *Jurnal Gagasan Hukum* 1, no. 01 (September 24, 2019): 109–29. https://doi.org/10.31849/jgh.v1i01.2894.

Veronica Agustina Darida and Slamet Tri Wahyudi. "Politik Kriminal Optimalisasi Perlindungan Hukum Terhadap Anak Sebagai Korban Tindak Pidana Revenge Porn." *Jurnal Interpretasi Hukum* 5, no. 2 (2024). https://doi.org/10.22225/juinhum.5.1.8502.889-902.

Viola, Marco, and Cristina Voto. "Designed to Abuse? Deepfakes and the Non-Consensual Diffusion of Intimate Images." *Synthese* 201, no. 1 (January 13, 2023): 30. https://doi.org/10.1007/s11229-022-04012-2.

Wafda, Putri Nurayu, Abdul Rokhim, and Nofi Sri Utami. "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Dalam Aplikasi Pinjaman Online." *DIVERSI : Jurnal Hukum; Vol 10 No 1 (2024): Diversi Jurnal HukumDO - 10.32503/Diversi.V10i1.4842* 10, no. 1 (July 25, 2024). https://doi.org/10.32503/diversi.v10i1.4842.

Yasemin Durmuş and Elif Yıldız. "Reconstruction of Discourses in Victims of Cyber Abuse in New Media: Derya Kuş Case." In *Media and Communication in the Digital Age: Changes and Dynamics*. Gaziantep: Özgür Yayın-Dağıtım Co. Ltd., 2023.

Yi Yan. "Deep Div Deep Dive into Deepfak o Deepfakes—Safeguarding Our Digital Identity." *Brooklyn Journal of International; Law* 48, no. 2 (2023).

Yulia Hesti, Bagas Satria Wijaya, Dewi Maharani, and Aliffia Dewi F. "Korelasi Antara Kebebasan Berekspresi Dalam Peningkatan Kasus Kejahatan Asusila Di Media Digital (Sextorsi)." *Journal of Law Education and Business* 2, no. 1 (2024). https://doi.org/10.57235/jleb.v2i1.1890.

Yuni Shaputri, Siti Nurewah, and Yusep Mulyana. "Penegakan Hukum Bagi Pengguna Aplikasi Michat Sebagai Sarana Tindak Pidana Prostitusi Online Dikaitkan Dengan UU Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *UNES Law Review* 6, no. 4 (2024). https://doi.org/10.31933/unesrev.v6i4.2244.

Yuri Tikhomirov, Nikolai Kichigin, Fatima Tsomartova, and Sayana Balkhayeva. "Law and Digital Transformation." *Legal Issues in the Digital Age,* 2 (2021). https://doi.org/10.17323/2713-2749.2021.2.3.20.

Zubair Ahmed Khan and Asma Rizvi. "Deepfakes: A Challenge for Women Security and Privacy." *CMR University Journal For Contemporary Legal Affairs* 5, no. 1 (2023).