Law and Humanities Quarterly Reviews

Hafiz, M. (2024). The Era of Artificial Intelligence: Examining Indonesia's Adaptability and Legal Challenges. *Law and Humanities Quarterly Reviews*, 3(3), 85-93.

ISSN 2827-9735

DOI: 10.31014/aior.1996.03.03.128

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research Law and Humanities Quarterly Reviews is a peer-reviewed International Journal of the Asian Institute of Research. The journal covers scholarly articles in the interdisciplinary fields of law and humanities, including constitutional and administrative law, criminal law, civil law, international law, linguistics, history, literature, performing art, philosophy, religion, visual arts, anthropology, culture, and ethics studies. The Law and Humanities Quarterly Reviews is an Open Access Journal that can be accessed and downloaded online for free. Thus, ensuring high visibility and increase of citations for all research articles published. The journal aims to facilitate scholarly work on recent theoretical and practical aspects of law.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Law and Humanities Quarterly Reviews
Vol.3, No.3, 2024: 85-93
ISSN 2827-9735

DOI: 10.31014/aior.1996.03.03.128

The Era of Artificial Intelligence: Examining Indonesia's Adaptability and Legal Challenges

Maulana Hafiz[1]

[1] School of Law, Gadjah Mada University, Yogyakarta, Indonesia

Correspondence: Maulana Hafiz, School of Law, Gadjah Mada University, Bulaksumur, Caturtunggal, Depok, Sleman Regency, Special Region of Yogyakarta 55281, Indonesia. E-mail: maulana.hafiz@mail.ugm.ac.id

Abstract
The rapid progress in artificial intelligence (AI) technology has given rise to a range of legal complexities, particularly pertaining to deepfake technology. This research delves into the impacts of deepfake media, with a specific focus on areas such as deepfake pornography, defamation, and image-based sexual abuse. The widespread use of deepfake technology has resulted in substantial concerns relating to privacy breaches, harm to reputation, and transnational abuse, posing distinctive challenges for legal enforcement and judicial systems. Furthermore, it is noted that the current legal framework in Indonesia, particularly the TPKS Law and the Revised Criminal Code (KUHP), is inadequate in addressing the intricacies of AI-driven offenses. The paper underscored the necessity for updated legislation and enhanced technological capabilities within law enforcement agencies to effectively combat AI-enabled crimes. While acknowledging the potential applications of AI in various sectors, including cybersecurity, the study emphasizes the urgency of aligning Indonesia's legal framework with the evolving landscape of artificial intelligence. This research serves as a comprehensive exploration of the legal implications of AI and deepfake technology in Indonesia, advocating for proactive measures to mitigate the risks posed by these technological advancements.

Keywords: Artificial Intelligence (AI), Defamation, Deepfake Pornography, Legal Framework, Indonesia

1. Introduction

Artificial intelligence (AI) presents a growing number of concerns in addition to major scientific achievements. However, rapid advancements in AI technology have made it easier for venues for technological crimes that were once made conventional especially in areas like deepfake technology. Deepfakes are a common tool for abusing and harming other people, which is not surprising considering how readily available and simple the technology is (Maras & Alexandrou, 2018). It is imperative that all nations confront the legal ramifications of these AI-driven damages since they represent major risks to social trust, reputation, and personal privacy (Akpuokwe et al., 2024).

Deepfake media are hyper-realistic videos, images, and digital forgeries created with the use of artificial intelligence and machine learning imagery (Cover et al., 2022). There are numerous types of deepfake varying

from face swap, voice modification, and puppeteering to even complex synthetic content to a video (commonly used for perverse content). These deepfakes often involve superimposition of an individual face to another individual body, depicting a scene that serves only to fuel a personal interest or agenda leading to the victims developing emotional distress, reputational damage, or privacy violations (Shahzad et al., 2022).

One of the most concerning manifestations of AI misuse is deepfake pornography, where AI is used to create realistic but fabricated explicit videos or images of individuals without their consent. In addition to violating the victims' right to privacy and dignity, this puts them at risk for serious psychological damage, extortion, and harassment. The topic of deepfake pornography has gained significant traction globally (Martin, 2022). Unlike physical violence to which it requires people to be in the same vicinity to happen. Deepfake pornography has a unique characteristic to which it includes possibility for cross-jurisdictional abuse, meaning that the abuser could stay anonymous, making legal enforcement have a hard time in investigating the crime even so far as adjudicating it (Karasavva, 2020).

The other possibility of AI misuse is defamation. Defamation has been defined as a false publication calculated to bring a person into disrepute, or "an attack on the reputation of another, and includes the ideas of calumny and aspersion by lying, and the injury to another's reputation by such means (Martin, 2012). Deepfake defamation poses particular difficulties for judicial systems. Due to the capacity to effectively change audio and video evidence, people may unjustly be accused of crimes or scandals, harming their reputation beyond repair. Because of these deepfakes, victims find it difficult to demonstrate that the content is false, which puts them in a risky legal scenario where the burden of evidence is too high (Van Der Sloot & Wagensveld, 2022).

The criminal justice system’s response to image-based sexual abuse has not been adequately addressed, indicating the need for additional means of prevention and control (DeKeseredy, 2021). Similar thing happened in Indonesia. AI-driven crimes in Indonesia present serious legal issues. The complexities of disinformation produced by AI are beyond the scope of Indonesia's existing deepfake pornography, deepfake identity theft and deepfake defamation laws. The nation's TPKS Law and the Information and Electronic Transactions Act (UU ITE) offer a foundational legal framework to address sexual assault and cybercrimes, but they are not entirely up to date with the rapidly developing field of artificial intelligence. Due to the absence of specific laws for crimes involving artificial intelligence (AI) and the difficulties in gathering trustworthy evidence in cases involving deepfakes or AI-generated material, legal enforcement is still problematic. Additionally, there may be gaps in the prosecution process as law enforcement organizations do not yet have the technological know-how to properly address crimes enabled by artificial intelligence.

Deepfake technology has received a lot of significance in the academic world, with multiple researches looking at its potential applications in a variety of sectors as well as the harm it would procure (Jones, 2020). As an example, research by Csongor and Toth (2024) in their study called “Artificial intelligence in cyber security :examining liability, crime dynamics, and preventive strategies” they similarly talked about the dangers of Artificial intelligence in the scope of cyber security, the difference that this paper has against mine is the subject of research of the paper, whereas in this paper they appeased to the EU country, my paper examines the readiness of Indonesia which both have different legal framework and backgrounds.

Another study relating to this paper is “Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia” made by Hailtik and Afifah (2024), where they examine an AI-Criminal liability models that apprehend those that commit crimes, in their research they mentioned that there exist 3 models of the said AI criminal liability, to how this differentiates to the author research is that it is based on the scope of the research. In my research the purpose is to examine the readiness of Indonesian vast legal framework in battling AI driven crimes, whereas in theirs, they focused on the criminal liability aspect of the law and whether AI can be utilized in making that happen.

This research examined the negative effects of AI-based crimes and how prepared Indonesia's judicial system is to handle them. Among of these concerns is the rise of deepfake pornography and Deepfake Defamation. The

research also made suggestions for updating current laws or creating new legislation to more effectively control damages caused by AI based on these results.

2. Method

The statutory method and normative juridical research were used to analyze current Indonesian legislation and address the negative impacts of artificial intelligence, including defamation, deepfake pornography, and identity theft. The study examined the legislative purpose, found any legal loopholes, and analysed the wording of these laws to see how applicable they are to crimes using artificial intelligence. The research will make suggestions for updating current laws or creating new legislation to more effectively control damages caused by AI based on these results.

3. Discussion

3.1. Understanding AI-Driven Crimes

Crimes utilizing Artificial Intelligence (AI) technology to facilitate, improve, or perpetrate unlawful acts are known as AI-driven crimes (King et al., 2019). These crimes make use of AI's strengths in automation, data processing, and content creation to commit acts detrimental to people, groups, or society as a whole. Because AI-driven crimes are driven by complex and constantly changing technology, it is more difficult for established legal systems to adequately handle them (Ejjami, 2024). These are a few prominent categories of AI-driven crimes that will be analyzed in this paper:

1) Deepfake Pornography: Deepfakes are AI-generated or edited videos that may swap faces or voices to produce fake but convincing material. Deepfake pornography uses AI technology to make pornographic movies or photographs of people without their knowledge, violating their privacy and causing substantial psychological, reputational, and financial harm to victims. (Okolie, 2023.)
2) AI-Based Defamation: AI techniques may be used to create phony audio or video recordings that purport to show someone saying or doing things they never did. Deepfakes may be used to propagate falsehoods, defame people, or damage reputations, with serious legal and personal ramifications. (Samoilenko & Suvorova, 2023)

3.2. Deepfake Pornography vs Revenge Pornography

The proliferation of deepfake pornography can be caused by several factors. At the forefront is that the rapid advancement of artificial intelligence and machine learning technologies, which have created venues for people to create hyper-realistic content that encourages this violence. Anonymity is also a key factor to why deepfake pornographic content spreads rapidly across platforms, the idea that the creators can operate from anywhere in the world and distribute it through a chain of sites and third-party people, makes it even more harder to track down who created the content, is it made by a particular person, or is it made by an app that the availability is provided to anyone with access through the internet, possibly causing irreparable harm to victims before it can be contained.

In the span of 6 years, deepfake pornographic content has become the bread and butter of sexual fantasy, as consumers can find sexual content of any female in the world or make it on their own through several applications / machine learning software that could be addressed as “bots” in numerous platforms, such as X and Telegram. Deepfake pornography can enable the fantasy of men who want more than the regular content on adult sites could provide.

In many societies, victims of sexual violence, especially women, face significant challenges like stigmatise responses and victim-blaming reactions from people around, misogynistic remarks, that hinder deepfake pornography case resolution altogether. The pervasive objectification of women in media and entertainment

reinforces harmful ideas, which can then be weaponised by those that create and distribute this particular content.

3.3. Indonesian Legal Frameworks regarding AI-Driven Crimes

Indonesia has several laws indirectly addressing similar issues to deepfake pornography through various laws that have been implemented in the past and recently passed down laws. However, the victims of the said crimes still to this day struggle to gain their rights to justice and legal protection due to the limited scope and narrow perspective that hasn't yet accommodated deepfake pornographic content as a violation of sexual conduct. Indonesia has promulgated 5 and amended 1 law to combat pornographic content.

First, according to the article 4 (1) of the Pornography law, it is mentioned that everyone is prohibited from producing, making, reproducing, reduplicate, distributing, broadcast, importing, export, offering, selling, renting or providing that explicitly contains:
a. sexual intercourse, including deviant sexual intercourse;
b. sexual violence;
c. masturbation or masturbation;
d. nudity or display of nudity;
e. genitals; or
f. child pornography.

When referring to the Pornography Law, article 4 (1) of the Pornography Law experiences variable limitations in its law, namely in the procedures for distributing it, in its technological elements, because it is not regulated regarding production and distribution using technology, like AI. Then, in Article 29 of the Pornography Law explains that someone who violates Article 4 paragraph (1) which includes acts such as Producing, making, distributing or providing pornography will be subject to a maximum prison sentence of a minimum of 6 (six) months and a maximum of 12 (years) and/or be subject to a fine of at least Rp. 250,000,000 (two hundred and fifty million rupiah) and a maximum of IDR 6,000,000,000 (six billion rupiah). This kind of effort hopes to provide a deterrent effect for perpetrators who create and spread pornographic content as well as has been explained in the Pornography Law.

Secondly, although the Law number 28 of the year 2014 regarding copyright law doesn't directly address pornography content, however the concept of deepfake intersects with aspect of the copyrights law, that being the content of the visual itself. Most deepfake pornographic contents take a picture of someone face and let AI to learn from it to then be attached to a sexual graphic content from adult sites to create that hyper-realistic sexual content. Most would argue this law doesn't bring enough relevance to the topic of deepfake pornography, however, the author argues that this law creates another perspective to it. Furthermore, according to Article 40 paragraph (1) letter k and I of the copyright law state that photographic content is protected works.

Moreover, Based on Article 9 paragraph (3) of the copyright laws states that any person without the permission of the Creator or Copyright Holder is prohibited in doing duplication and/or Commercial Use of Works. If you look at the element "Doubling and/or Commercial use" then it can be said to be a copyright violation if the work from Deepfake Porn is intended for commercial purposes, namely selling it to other people by promoting it via social media., in accordance with Article 50 Copyright laws which explains that every person is prohibited Announce, distribute or communicate works that are contrary to morals, religion, morality, public order, or state defence and security.

Thirdly, Indonesia also has the law regarding Anti-Sexual Violence or commonly known as TPKS, which is a recently passed down law that is mostly used to convict those that violate violence against gender (mostly women), this law is famous as for the past 16 years, people had finally had a law to addresses domestic violence, stalking, and even revenge porn. However, how does the law manage against new threat so-called deepfake pornography? In the TPKS Law, it is regulated in Article 14 paragraphs (1) and (2) which relate to criminal acts in the form of recording/taking images with sexual nuances without consent, transmitting electronic

information/documents with sexual content, as well as stalking or tracking using an electronic system. to people who become objects of information/electronic documents for sexual purposes, either by blackmail, threats, or coercion, as well as misleading/deceiving someone. However, even with the popularity of the TPKS law, there are several clauses which haven't been included in several articles in the law, such as, Unwanted creation of electronic material with sexual nuances, modification of material with sexual nuances, sale of electronic material with sexual nuances. Which essentially is the descriptive product of deepfake pornography.

Moreover, Article 30 paragraph (1) of the TPKS Law states that victims have the right to receive restitution and recovery services. If the perpetrator is unable to pay restitution or if the perpetrator's confiscated assets do not cover the cost of restitution, the state will compensate the victim for the amount of the lack of restitution in accordance with the court decision. This compensation can be paid through the Victim Assistance Fund which can be obtained from philanthropy, society, individuals, corporate social and environmental responsibility, other legal and non-binding sources, as well as the state budget in accordance with the provisions of statutory regulations.

Fourthly, Indonesia also accommodates the protection of personal data. this law is relevant due to theft of personal data is unavoidable from Deepfakes in that using someone's face for content without the permission of the face owner to benefit oneself is theft of personal data and harms other people. This violates Article 66 that states "Everyone is prohibited from creating false personal data or falsifying personal data with the intention of benefiting themselves or others which could result in harm to others." Sanctions for perpetrators of falsifying Deepfake personal data can be punished according to Article 68 of the Personal Data Protection Law, imprisonment for a maximum of 6 years and a fine of a maximum of 6 billion Rupiah.

Lastly, Deepfake pornography abuse is also regulated in Law Number 1 of 2024 concerning the Criminal Code. Article 407 paragraph (1) of the new Criminal Code regulates the abuse of Deepfake with pornographic mutations which states "Every person who produces, creates, reproduces, duplicates, disseminates, broadcasts, imports, exports, offers, sells, rents or provides pornography, shall be punished by imprisonment. a minimum of 6 (six) months and a maximum prison sentence of 10 (ten) year.

Aside from the regulation relating to Deepfake Pornography, Indonesia has also addressed the issue relating to technological crimes such as defamation and identity theft in the Present Criminal code and Indonesian Personal Data Protection Law. Article 310 (defamation) and Article 311 (slander) of the Criminal Code (KUHP) may be invoked in situations of deepfake defamation in Indonesia. These articles discuss the damage that may be done to someone's reputation when they are falsely accused or have their honour violated. These rules do not specifically address the unique character of content created by AI, even though they can be used to penalize anyone who creates or distributes deepfakes that harm people's reputations. Further protection is provided by Article 66 of the Personal Data Protection Law (PDP Law), which makes it illegal to use, change, or distribute personal data without authorization, which is frequently the situation when creating deepfakes.

This article provides an additional legal path for claims involving the modification of a person's image or private information in deepfakes. Nonetheless, these legislative tools continue to be inadequate in tackling the intricacies and technical subtleties of deepfake defamation, underscoring the necessity for more AI-specific legal rules.

Table 1: Legal Framework Relating to AI-Driven Crimes in Indonesia

No.	Legal Framework	Articles
1	Law no. 44 of the year 2008 regarding Pornography	Article 4 paragraph (1)
2	Law no. 28 of the year 2014 regarding copyright law	Article 40 paragraph (1) letter k and I
3	Law no. 14 of the year 2022 regarding Anti-Sexual Violence (TPKS)	Article 14 paragraphs (1) and (2)
		Article 30 paragraph (1)

4	Law no. 27 of the year 2022 regarding Personal Data Protection	Article 66
5	Law Number 1 of 2024 concerning the Revised Criminal Code	Article 310
		Article 311
		Article 407 paragraph (1)

Source: JDIH BPK

The complexities of AI-generated deepfakes, such as demonstrating the falsity of manipulated content or determining the intent behind creating the deepfake, are not specifically addressed in these articles, despite the fact that they cover traditional defamation and slander and regulate traditional pornography and electronic media-based pornography to some extent. These rules need to be revised to specifically address deepfake technology and its potential for defamation, as seen by how vaguely they address AI-generated material.

Regrettably, Indonesia has not regulated the use of AI, particularly deepfakes, although there are regulations that govern this activity, the concept of deepfake conduct in Indonesia is not definitively defined in positive law. Deepfakes may be made illegal by using several of the aforementioned law prohibitions. But even then, the reality of the enforcement of the violation is still challenged and faces many obstacles, one of the major challenges comes from the legal enforcer department.

3.4. Indonesian Legal Efficacy in handling AI-Driven Crimes

In essence, Indonesia follows a civil law legal system, which regrettably unable to decide matters in the absence of a legal norm governing them. For legal certainty, legislative reforms pertaining to deepfake crimes must be implemented in a way that upholds the criminal law's legitimacy premise. Asshiddiqie, (2016) Clarifies that law enforcement, is the process of trying to make the law work and/or sustain legal standards by using it as a guide for conduct in relationships with the state and society. The legal system now faces additional difficulties as a result of the quick development of AI technology, particularly when it comes to instances involving deepfake pornography and defamation motivated by AI. Existing legislation in Indonesia, such as the Indonesian Anti-Sexual Violence Act (TPKS Law) and the present Criminal Code (KUHP), These laws, however, find it difficult to capture the complexity and dynamic character of material created by AI.

Regarding AI-driven defamation, which involves manipulating videos, sounds, or pictures to harm someone's reputation, the present Criminal Code (KUHP) and UU ITE defamation regulations do not take into consideration the special qualities of deepfakes. It is very difficult for victims to demonstrate that the defamatory information is false due to the production of very convincing fake media, and the burden of evidence in these situations frequently rests disproportionately on the victim. Furthermore, enforcement and prosecution are forced to depend on antiquated legal interpretations that were not intended to manage disinformation produced by artificial intelligence (AI) as the law does not specifically address the technological components of deepfakes.

Likewise, deepfake pornography is a new problem that is not well addressed by the regulations in place. The TPKS Law, which aims to prevent sexual assault, offers some defense against the unintentional sharing of private photos. It does not, however, specifically address situations in which people are falsely depicted in pornographic material without their consent through the use of deepfakes. Because present legal regulations frequently overlook the particular injury produced by these digital manipulations, victims of deepfake pornography have little redress due to this vacuum in the legal framework. Because of this, those who commit such crimes could avoid punishment, and victims are left vulnerable to the emotional, societal, and financial damage brought on by the broad dissemination of deepfakes.

Since deepfake pornography is arguably a new concept on the legal horizon in Indonesia, law makers are struggling in creating a clear and narrow definition to address deepfake pornography. Although, some laws may be able to accommodate current cases of deepfake pornography, but the efficacy of said laws depends greatly on how legal enforcer interpret the article and provisions. This create certain legal uncertainty for the victims,

furthermore since the subject of deepfake pornography is spread across numerous different laws, it further creates an overlap to what can be used and avoided in managing deepfake pornography cases.

Deepfake pornography presents serious legal issues for Indonesia within the confines of its current legal system, mainly because of ambiguous laws, technological constraints, and cultural differences. The main legal weapon against sexual assault, the Law on the Elimination of Sexual assault (TPKS Law), does not specifically address the special and complicated character of deepfake pornography. This law does not specifically address the production and dissemination of deepfakes; rather, it focuses largely on physical acts of violence and internet harassment. Because of this, it is challenging to successfully prosecute criminals in deepfake situations because of the significant uncertainty in the law. The legal system frequently leaves victims without a clear legal foundation on which to pursue justice since deepfakes cause injury that is not completely recognized by the law.

Moreover, the technical expertise required to look into and prosecute deepfake incidents is usually lacking in Indonesia's law enforcement organizations. Because deepfakes are created using sophisticated artificial intelligence (AI) technology, it may be difficult to identify and verify their validity. Additionally, because the internet is anonymous and worldwide, it can be difficult to find the offenders, who may be based in various countries. The inability of authorities to adequately handle deepfake pornography is severely hampered by this technological gap, which results in unresolved cases and increased victimization. Sexual assault victims in Indonesian society, particularly those who are the subject of deepfakes, frequently experience severe shame and victim-blaming, which deters them from reporting their abuse. Even if people do report these occurrences, the legal system could not completely acknowledge or authenticate their experiences because of the general lack of knowledge of deepfake technology. The idea that the law is insufficient to protect victims and hold offenders accountable is influenced by this social context.

In addition, victims of deepfake pornography are not given any particular remedies under the TPKS statute. Without well-defined legal procedures for deleting offensive material, requesting reimbursement, or obtaining counseling, victims are forced to negotiate a convoluted legal system on their own with no help or direction. Due to the TPKS law's jurisdictional limitations, the global nature of deepfake pornography—where producers and distributors could reside outside of Indonesia—complicates judicial proceedings even more. All of these elements combine together to render the existing legal system inadequate in combating the rising problem of deepfake pornography, putting victims at risk and justice elusive.

4. Recommendations

To summarize, while laws such as the Indonesian Anti-Sexual Violence Act (TPKS Law), and Revised Criminal Code (KUHP) which play a major role in regulating these acts, they fall short of addressing the specific complexity created by AI technology. The fast advancement of AI, notably in the production of deepfakes and automated identity theft, outpaces the present legal system, leaving victims vulnerable and criminals unaccountable. Without immediate legislative reforms and enforcement enhancements, the abuse of AI will continue, exploiting these weaknesses and causing further harm to individuals and society. The deficiencies in the legal system, ranging from ambiguous terminology to a lack of victim assistance systems, highlight the need for thorough legislative reform and increased enforcement capacities. To address these issues, many critical recommendations must be put into action.

First, Indonesia should prioritize legislative change by revising current laws to specifically target AI-related crimes. For example, the TPKS Law could be changed to include prohibitions on deepfake pornography and other forms of digital exploitation, and a new, AI-specific rule may be developed to thoroughly address crimes such as identity theft and defamation caused by AI technology. To further safeguard persons from the dangers of deepfake pornography, numerous suggestions should be explored. First, there is an urgent need for legislative change that clearly addresses deepfake technology, either within the scope of the TPKS Law or through new, specialized legislation. This change should contain precise definitions of digital sexual assault, specific restrictions for creating and distributing deepfake content, and harsher consequences for violators. Second, law enforcement organizations must have the technological skills and resources to adequately investigate and

prosecute deepfakes. This might include specialized training programs and the formation of alliances with technology specialists and digital professionals. Third, public awareness initiatives are critical for educating society about the risks of deepfake pornography and combating the stigma and victim blaming connected with sexual assault. Finally, cross-border collaboration and legislative harmonization with other jurisdictions should be undertaken to address the global character of deepfake crimes, ensuring that criminals cannot avoid prosecution merely by working across national borders.

Secondly, it is vital to provide law enforcement and judicial systems with the required technological skills. Specialized training programs should be developed to help investigators and prosecutors better comprehend and manage AI-related matters. Furthermore, specialized AI-focused divisions inside law enforcement organizations may increase the ability to investigate, acquire evidence, and prosecute AI-related offenses more efficiently.

Thirdly, public awareness campaigns are essential for encouraging proactive reporting and educating the public about the dangers of AI misuse, including deepfake pornography and identity theft. The establishment of victim support measures, such as aid with digital evidence and legal advice, would bolster the protection and response system for persons affected by AI crimes.

Finally, considering the worldwide scope of AI-related crimes, Indonesia must strengthen international collaboration by working with other jurisdictions and international organizations. Cross-border legal frameworks and mutual aid treaties will be required to combat AI-related crimes that cross national borders. By implementing these changes, Indonesia can build a more robust legal system that is better suited to dealing with the increasing risks posed by AI-driven crimes, ensuring that victims are protected and criminals are held accountable in the face of technological breakthroughs.

Author Contributions: The author contributed to the overall preparation, conception, or design of the work, or interpretation of data, drafted the work, and substantively revised it.

Funding: Not applicable

Conflicts of Interest: The authors declare no conflict of interest.

Informed Consent Statement/Ethics approval: Not applicable.

Data Availability Statement: The data used in this research are public records and journal articles, therefore, can be found publicly.

References

Asshiddiqie, J. (2006). Introduction to constitutional law. (*Pengantar ilmu hukum tata negara*.)

Akpuokwe, N. C. U., Adeniyi, N. a. O., Bakare, N. S. S., & Eneh, N. N. E. (2024). LEGAL CHALLENGES OF ARTIFICIAL INTELLIGENCE AND ROBOTICS: A COMPREHENSIVE REVIEW. Computer Science & IT Research Journal, 5(3), 544–561. https://doi.org/10.51594/csitrj.v5i3.860

Bothamley, S., & Tully, R. J. (2018). Understanding revenge pornography: public perceptions of revenge pornography and victim blaming. Journal of Aggression Conflict and Peace Research, 10(1), 1–10. https://doi.org/10.1108/jacpr-09-2016-0253

Cover, R., Haw, A., & Thompson, J. D. (2022). The visual in an era of hyperreality and disinformation: the deepfake video. In Emerald Publishing Limited eBooks (pp. 63–76). https://doi.org/10.1108/978-1-80117-876-120221005

Csongor, H., & Tóth, D. (2024). Artificial Intelligence In Cybersecurity: Examining Liability, Crime Dynamics, And Preventive Strategies. EU And Comparative Law Issues and Challenges Series. https://doi.org/10.25234/eclic/32299

DeKeseredy, W. S. (2021). Image-Based sexual abuse: social and legal implications. *Current Addiction Reports*, *8*(2), 330–335. https://doi.org/10.1007/s40429-021-00363-x

Ejjami, R. (2024). AI-driven Justice: Evaluating the impact of artificial intelligence on legal systems. *International Journal for Multidisciplinary Research*, *6*(3). https://doi.org/10.36948/ijfmr.2024.v06i03.23969

Hailtik, A. G. E., & Afifah, W. (2024). Criminal responsibility of artificial intelligence committing deepfake crimes in Indonesia. Asian Journal of Social and Humanities, 2(4), 776–795. https://doi.org/10.59888/ajosh.v2i4.222

Jones, V. A. (2020.). *Artificial intelligence enabled deepfake technology: the emergence of a new threat - ProQuest*. https://search.proquest.com/openview/60d6b06b94904dccf257c4ea7c297226/1?pq-origsite=gscholar&cbl=18750&diss=y

Karasavva, V. (2020). *IPreDator: Image-Based Sexual Abuse Risk factors and Motivators*. Carleton University Institutional Repository. https://repository.library.carleton.ca/concern/etds/zc77sr22z

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2019). Artificial Intelligence Crime: an interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0

Law no. 44 of year 2008 regarding Pornography (Indonesia)

Law no. 28 of year 2014 regarding copyright law (Indonesia)

Law no. 14 of year 2022 regarding Anti-Sexual Violence (TPKS) (Indonesia)

Law no. 27 of the year 2022 regarding Personal Data Protection (Indonesia)

Law no. 1 of 2024 concerning the Revised Criminal Code (KUHP) (Indonesia)

Martin, B. (2022). Mixing old and new wisdom for the protection of image-based sexual abuse victims. *South African Journal of Criminal Justice*, *35*(3), 307–330. https://doi.org/10.47348/sacj/v35/i3a2

Martin, K. (1966). Defamation Defined. Chicago Kent Law. Review., 43, 2.

Maras, M., & Alexandrou, A. (2018). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. *The International Journal of Evidence & Proof*, *23*(3), 255–262. https://doi.org/10.1177/1365712718807226

Nwachukwu, F. (2023). Identity Theft, Cyber Bullying, and Human Illusion: A Global Security Exposee into the Use of Artificial Intelligence in Deep Fake Technology. Cyber Bullying, and Human Illusion: A Global Security Exposee into the Use of Artificial Intelligence in Deep Fake Technology. https://ssrn.com/abstract=4487820

Okolie, C. (2023). *Artificial Intelligence-Altered videos (Deepfakes), Image-Based sexual abuse, and data privacy concerns*. Virtual Commons - Bridgewater State University. https://vc.bridgew.edu/jiws/vol25/iss2/11/

Öhman, C. (2020). Introducing the pervert's dilemma: A contribution to the critique of Deepfake Pornography. Ethics and Information Technology, 22(2), 133-140. https://doi.org/10.1007/s10676-019-09522-1

Shahzad, H. F., Rustam, F., Flores, E. S., Mazón, J. L. V., De La Torre Diez, I., & Ashraf, I. (2022). A review of image processing techniques for Deepfakes. *Sensors*, *22*(12), 4556. https://doi.org/10.3390/s22124556

Samoilenko, S. A., & Suvorova, I. (2023). Artificial intelligence and deepfakes in strategic deception campaigns: the U.S. and Russian experiences. In *Springer eBooks* (pp. 507–529). https://doi.org/10.1007/978-3-031-22552-9_19

Van Der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: regulatory challenges for the synthetic society. *Computer Law & Security Review*, *46*, 105716. https://doi.org/10.1016/j.clsr.2022.105716