ISSN : 0216-8175 EISSN : 2303 - 2499

MIMBAR
Jurnal Sosial dan Pembangunan

Publisher : UPT Publikasi Ilmiah Unisba
Jalan Taman Sari No. 20, Bandung, Jawa Barat, 40116, Indonesia.
Phone : (022) 4203368, 4205546 ext. 6737
Email : mimbar@unisba.ac.id
Website : https://ejournal.unisba.ac.id/index.php/mimbar/index

Legal Review Of Liability From Deepfake Artificial Intelligence That Contains Pornography

[1] MUHAMMAD ILMAN ABIDIN*, [2] AHMAD FAIZAL ADHA,
[3] SALMA SUROYYA YUNIYANTI, [4] CHICHA CHAIRUNNISA

Universitas Islam Bandung*
Correspondance author: muhammadilmanabidin@unisba.ac.id*

Article

Article History
Received: 5/10/2023
Reviewed: 18/12/2023
Accepted: 28/12/2023
Published: 28/12/2023

DOI:
doi.org/10.29313/mimbar.v39i2.2965`

Volume : 39
No. : 2
Month : Desember
Year : 2023
Pages : 344-352

To cite this article (APA Style):

Author, second author. (2023). The article title is sentence case style. Jurnal Mimbar. 0(0), 00-00. https://doi.org/....

Abstract

This article seeks to determine who is responsible for the widespread use of deepfake AI to create pornographic content and how Indonesian law governs it. Deepfakes, a subfield of artificial intelligence, can manipulate visual media by superimposing facial features on the bodies of others, creating misleading videos. Deepfakes were first used in movies and then in gadgets. However, deepfakes have been used to make explicit pornographic videos. This research is normative law-based. This study found that Indonesia has no specific legislation on artificial intelligence technology, except for Law Number 19 of 2016, which amends Law Number 11 of 2008 on Electronic Information and Transactions. Number 44 of 2008 on Pornography prohibits pornographic content creation and provides criminal penalties to hold offenders accountable. In Government Regulation (PP) Number 71 of 2019, which regulates electronic systems and transactions, pornographic platform providers cannot use deepfake technology.

Keywords: Artificial Intelligence, Deep Fake, Pornography.

Introduction

The advancement of information and communication technology has experienced significant and rapid growth. The development of internet media (online) that is so fast can be seen (Agus Syihabudin, et al., 2019). In the past, the crime that often occurred was a street crime, now along with the development of the times and technology, cybercrime (digital crime) is more prevalent in society (Lisa Adhrianti et al., 2022). Thus, this advancement is widely used to meet people's different needs. Modern information and communication technology has many positive consequences on human life. These include fast information exchange, business transactions, and entertainment. The use of digital technology can lead to the spread of false information (called "hoax"), unauthorized access to electronic data (called "hacking"), and the facilitation of discriminatory or immoral digital content.

Naturally, the many uses described above are linked to the broad use of the Internet, which is a result of information and

communication technology breakthroughs that have infiltrated worldwide culture. The concept of a worldwide library can be attributed to the internet, which enables universal access and utilization for all individuals, irrespective of their societal standing (Istiarni & Kurniasari, 2020). Global life is heavily influenced by the internet, which is available to anyone. As said, the negative consequences of internet usage also need its use. Information and communication technology development and use are like two sides of a coin. Technology has improved human well-being and civilization. However, on the other hand, it has also given rise to activities that are in violation of legal norms (Hudini, 2017).

The latest technological developments have sparked an artificial intelligence (AI) technology whose existence has not been concretely regulated in International Law. According to Russel Stuart in his book: "Artificial Intelligence is often used to describe machines (or computers) that mimic "Cognitive" functions that humans associate with the human mind, such as "Learning" and "Problem Solving" (Russel, 2009). AI refers to computational systems, such as computers, that mimic human cognitive skills like learning and problem-solving. AI technology begins automating and digitizing manufacturing and administration. The first hypotheses of artificial intelligence (AI) emerged in 1941. The 1956 Dartmouth conference introduced the term "artificial intelligence" for the first time. Since its inception, artificial intelligence (AI) has undergone continuous development, driven by numerous studies that explore its ideas and principles, which are also subject to ongoing refinement (Sutojo, 2011).

Artificial intelligence (AI) technology has been widely adopted throughout numerous countries worldwide, with the primary objective of enhancing efficiency and simplifying various tasks or occupations traditionally performed by humans. Indonesia, being a developing nation, has initiated the utilization of artificial intelligence technology. However, its implementation remains limited throughout all sectors of society in comparison to more industrialized nations. Intelligence technology in Indonesia is presently being extensively employed and implemented by start-up enterprises, which leverage artificial intelligence technology to bolster their fundamental operational infrastructure. Prominent examples include Kata.ai, Snapcart, BJTech, and Sonar (Tantri et al., 2022). These four start-up organizations offer functionalities that enable individuals to develop chatbots utilizing artificial intelligence technologies. Furthermore, the utilization of artificial intelligence (AI) in Indonesia extends to the industrial domain, where robots and AI technology have been employed to automate production and manufacturing processes. Manufacturing is widely recognized as a complex network of interrelated activities encompassing design, material procurement, production, management, planning, and marketing (Lubis, 2021).

The development of AI has sparked a certain algorithm called Deepfake Technology. According to Marissa Koopman, Andrea Macarulla Rodriguez, and Zeno Geradts in their journal shed light on Deepfake Technology as an algorithm, in the form of: "The Deepfake algorithm allows a user to switch the face of one actor in a video with the face of a different actor in a photorealistic manner" (Koopman, 2018). Deepfake refers to an algorithmic technique that enables users to seamlessly replace the facial appearance of one actor with that of another actor in a visually convincing manner within a photorealistic film. Deepfake technology has emerged as a novel method for manipulating videography in recent years. This technology enables the alteration of an individual's facial appearance by seamlessly superimposing it onto another person's face within a video format. What distinguishes Deepfake from other forms of video manipulation? Firstly, the potential for achieving photorealistic outcomes is evident, since the algorithm has the capability to generate full facial representations for each performer. Given sufficient time, the resulting movie is likely to exhibit a high level of visual authenticity.

Additionally, the usability of publicly available Deepfake apps like FaceApp and Reface for non-experts. Humans have built various tools and methods to help with different activities, including Deepfake technology. Technology, especially the internet, has pros and cons. Facilitating information communication offers several opportunities for its growth. Conversely, external privacy invasions create new risks. Digital data distribution ignores physical and jurisdictional boundaries, making it easy and unlawful to transmit or manipulate personal data without the data owner's agreement or control. Deepfake has attracted attention for its use in creating explicit celebrity material, spreading false information, deceitful schemes, and financial malfeasance. Furthermore, this has prompted reactions from both corporate and government entities aimed at identifying and restricting its utilization (Clarke, 2019). The utilization of deepfake technology involves the utilization of personal data in the form of facial images of persons. This technology possesses the potential to be exploited, particularly in the context of illegal activities such as the dissemination of propaganda, creation of pornographic content, perpetration of identity theft, and other privacy-related concerns.

In this instance, the phenomenon of deepfakes has also made its way into Indonesia, as seen by the utilization of aforementioned applications by Indonesian individuals, which incorporate deepfake technology in their functionalities. However, it is worth noting that a majority of Indonesians

are unaware of the presence of deepfake capabilities inside these applications. In a similar vein to the modified TikTok video featuring Tom Cruise through the utilization of deepfake technology, it has come to light that a number of pornographic videos portraying Indonesian musicians Gisella Anastasia and Nagita Slavina have been circulating inside the country. Telematics specialist Roy Suryo suggests that the aforementioned films may have been fabricated using deepfake technology (Riantrisnanto, 2020). The absence of empirical support indicates that the utilization of deepfakes technology in the creation of the two videos is unsubstantiated (Kurnia, 2021). Based on the author's research and analysis, it is evident that there exists a legal void that currently fails to effectively govern the misuse of deepfakes as a manifestation of artificial intelligence technology. The utilization of deepfake technology presents a potential avenue for the production of pornographic video material wherein an individual's face is manipulated to falsely attribute their identity to the perpetrator depicted in the video. This practice is explicitly prohibited by the Pornography Law. In addition, the dissemination of pornographic videos with the purpose of gaining financial advantages or defaming individuals via social media is a legally proscribed action as stipulated by the Information and Electronic Transactions (ITE) Law.

The author aims to investigate the allocation of responsibility among parties involved in the misuse of deepfake AI technology, specifically in the creation of a substantial volume of pornographic content. This inquiry pertains to determining whether the culpable party is the individual utilizing the technology or if the creator and administrator of the deepfake AI platform can be held accountable under Indonesian legislation.

Research Method

The research employed the normative juridical research method, which seeks to reconcile the legal provisions governing the protection of norms and other legal regulations pertaining to the implementation of legal regulations in the field (Asikin, 2016). Normative juridical study is conducted through the examination of library materials, namely secondary data or legal research conducted within libraries. This article aims to explore and analyze the regulatory framework surrounding artificial intelligence (AI) technology in Indonesia. Additionally, it will investigate the illicit utilization of deepfakes in the creation of pornographic videos through the application of AI technology, within the context of Indonesian legislation.

Results & Discussion

Deepfake AI Regulation in Indonesia Compared to Regulation of Deeofake AI in Various Countries

Indonesia is recognised as a nation governed by the rule of law, as specifically stated and enshrined in Article 1, paragraph (3) of the 1945 Constitution of the Republic of Indonesia (UUD 1945). Moreover, on November 25, 2016, the Indonesian government enacted Law Number 19 of 2016, which pertains to the regulation of technology, information, and communication law. This law serves as a revision of the previous legislation, Law Number 11 of 2008, specifically addressing electronic transaction information. The objective of harmonisation is to ensure the continuing application of laws stipulated in the ITE Law, thereby establishing a definitive and transparent legal framework for the utilisation of information and communication technology (ICT) in society (Muchtar, 2018). The presence of explicit arrangements governing artificial intelligence technology in Indonesia can be seen in the ITE Law, which aligns with the author's perspective on this matter.

Regulation of deepfake AI varies from country to country. Here are some examples of how deepfakes are regulated in different countries:

1. China has implemented measures to regulate AI-generated content, such as deepfakes, in order to exercise control over its dissemination. The objective is to exert authority over the utilisation of algorithms, deep learning, virtual reality, and other artificial intelligence (AI) technologies for the purpose of generating or modifying content. Chinese companies engaged in the production of material for the metaverse are subject to regulatory guidelines pertaining to artificial intelligence (AI) content (Beijing acts to control AI-generated content, 2022).
2. The United States has yet to enact dedicated regulations specifically addressing the issue of deepfakes. Nevertheless, many deliberations and suggestions for legislative measures have been put out to tackle the aforementioned matter. Certain states have implemented legislation that renders the act of producing and disseminating deepfakes with harmful intent, such as revenge pornography or intervention in elections, a criminal offence. Furthermore, social media companies such as Facebook and Twitter have enacted regulations in order to mitigate the dissemination of deepfakes. (Ahmed, 2023)

 DOI: https://doi.org/10.29313/mimbar.v39i2.2965

3. The regulation of deepfake artificial intelligence (AI) exhibits variation among different nations. Certain nations have enacted legislation that particularly focuses on addressing the concerns associated with deepfakes, but others depend on pre-existing legal frameworks to tackle this matter. An instance of this can be observed in the European Union's proposition of legislation that mandate platforms to eliminate deepfake content and provide information regarding its source. The creation and distribution of deepfakes without consent has been criminalised in Canada. Australia has implemented legislation that prohibits the production and dissemination of deepfakes with malicious intent. (Struensee, S.V., 2021).

The author delineates the attributes of artificial intelligence (AI) technology by drawing explicit connections to the provisions outlined in the Information and Electronic Transactions (ITE) Law. This alignment can be observed in the shared characteristics with the concept of a "Electronic Agent," as defined in Article 1, point 8 of the ITE Law (Law No.19, 2016). According to this definition, an Electronic Agent refers to an electronic system device designed to autonomously execute actions on specific Electronic Information, under the direction of a human operator. The author's interpretation of the term "automatic" in the description of "Electronic Agent" in the article reflects their personal perspective. However, it is worth noting that according to the KBBI (Kamus Besar Bahasa Indonesia), the term "automatic" carries a different connotation, specifically referring to the ability to function independently. In addition to this, according to the conceptualization proposed by John McCharthy, artificial intelligence technology is characterised as a computational system capable of autonomous cognition and decision-making. The aforementioned explanations share similarities that suggest a correlation between the attributes of artificial intelligence (AI) technology and the attributes of the "Electronic Agent" itself.

Based on the provided information, the author posits that the legislation pertaining to "Electronic Agents" can potentially be extended to encompass artificial intelligence (AI) technology. Moreover, the ITE Law delineates Electronic Agents as a subset of Electronic System Implementation (PSE), as defined in Article 1 number 6, which encompasses the utilisation of Electronic Systems by governmental officials, individuals, corporate entities, and/or the general public (Law No.19, 2016). Moreover, as stated in Article 1, clause 5 of Law No.19, 2016, the Electronic System encompasses a set of electronic equipment and protocols designed to undertake various tasks such as the preparation, collection, processing, analysis, storage, display, announcement, transmission, and/or dissemination of Electronic Information. Based on the information presented in the article, it may be inferred that the electronic agent organiser functions as an electronic system organiser, with the same rights and responsibilities applying to both entities, albeit with necessary modifications. The ITE Law stipulates that the utilisation of electronic systems, in the form of implementing electronic systems, is restricted to individuals, state administrators, corporate entities, and/or the community. This issue is also connected to the concept of liability inside a Public Service Entity (PSE), as outlined in Article 15 of the Information and Electronic Transactions (ITE) Law (Law No.19, 2016).

In relation to the author's discourse on deepfakes, it can be inferred that the regulations governing artificial intelligence technology, as explicitly outlined in the previous ITE Law, are equally applicable to the utilization of deepfakes in Indonesia. These regulations impose similar limitations on the presence of artificial intelligence technology within the country. The author contends that the ultimate responsibility for the deployment of artificial intelligence technology as an electronic agent lies with the entity overseeing its development. However, if we were to draw a parallel between human-AI interactions and the technology itself, it becomes evident that without more comprehensive legislation governing artificial intelligence technology in Indonesia, the debate surrounding this issue will persist indefinitely.

Deepfakes is a synthetic approach that utilizes artificial intelligence technology and its thinking algorithms to manipulate human images. The proliferation of deepfakes serves as evidence of the advancing capabilities of artificial intelligence technology, enabling it to perform complex tasks that would often require considerable time and expertise if executed by humans. Deepfakes refer to the utilization of a comprehensive and foundational scanning methodology of human images through deep learning, a machine learning technique, to fabricate or manipulate visual content, such as images or videos, within a given context. This process involves the application of a machine learning framework called Generative Adversarial Network (GAN) (Schwartz, 2018). In summary, deepfakes enable the utilization of extensive datasets comprising numerous photos or videos, which are then subjected to artificial intelligence algorithms for processing and learning. This facilitates the creation and generation of novel images or videos that mimic authentic content. Subsequently, deepfakes have been employed for the purpose of editing, wherein a pre-existing facial image of an individual is amalgamated with the body of another person from a distinct video source. This process results in

the creation of a counterfeit video that exhibits a high degree of verisimilitude to an authentic recording.

Drawing on the preceding elucidation on the functionality and application of deepfakes, the author posits that the employment of deepfakes is a manifestation of using and harnessing a lawful entity regulated or executed by an individual acting within the confines of the law. This pertains to the utilization of deepfakes in various functionalities of popular applications such as MyHeritage, FaceApp, and Deepfake Studio. These three applications have garnered significant global downloads and user engagement, including users from Indonesia, who employ them primarily for entertainment purposes. According to the stipulations outlined in Article 1 number 6 of Government Regulation No. 71 of 2019, which pertains to the Implementation of Electronic Systems and Transactions, the aforementioned entities can be classified as Private Scope Electronic System Operators (PSEs) due to their organizational structure being affiliated with a commercial enterprise.

Moreover, the author also posits that these three entities can be seen as purveyors of artificial intelligence technology, since they harness the capabilities of deepfakes as a manifestation of artificial intelligence technology integrated into their functionalities. The author has also familiarized themselves with the Terms and Conditions of the MyHeritage, FaceApp, and Deepfake Studio programs. The Term and Condition is a documented agreement that outlines the terms and conditions governing the relationship between the service provider, specifically the application provider, and the service users, who are the application users. It encompasses the rights, obligations, and responsibilities of both parties, as well as the rules pertaining to the utilization of the service (G, 2016).

The aforementioned applications are categorized as Private Scope Electronic System Operators (PSE), each with its own specific provisions outlined in their respective Terms and Conditions. These provisions are designed to ensure the reliable and secure functioning of the electronic system (application) and impose responsibility for its proper operation, as stipulated in Article 15, paragraph (1) of the ITE Law. The author discovers, upon examining the Terms and Conditions of the three applications, that the contractual agreement between the application providers and users regarding the utilization of the application entails the transfer of accountability for the outcomes of content or products generated by users through the application's available features to said users. Naturally, this principle extends to the utilization of functionalities that incorporate the capabilities of deepfakes.

Based on the aforementioned data, it can be inferred that the three aforementioned applications can be classified as providers of Private Scope Electronic Systems, mostly centered around User Generated Content. Based on the findings of the Organization for Economic Co-Operation and Development (OECD), User Generated Content (UGC) refers to content that is created and shared on the internet, showcasing the creative expression of users and originating from non-professional contexts (Dwityas, 2016). Moreover, the provisions outlined in Article 11 of Regulation No. 5 of 2020, issued by the Minister of Communication and Information Technology, pertain to the regulation of Private Sphere Electronic System Providers that operate on the basis of User Generated Content (UGC). These providers are granted exemption from legal liabilities associated with the dissemination of Electronic Information or Electronic Documents that are prohibited from being circulated through their Electronic Systems. The specific details of this exemption are as follows: (Minister of Communication Regulation No. 5, 2020)

1. Has performed the obligations as referred to in Article 9 Paragraph (3) and Article 10;
2. Provides Electronic System User Information (Subscriber Information) that uploads prohibited Electronic Information and/or Electronic Documents in the context of supervision and/or law enforcement; and
3. Performs Access Termination (take down) of prohibited Electronic Information and/or Electronic Documents.

The third providers of the aforementioned applications also include respective terms and conditions that regulate limitations and prohibitions in the creation of content/products that users are not allowed to produce when utilizing the features within the applications. The limitations and prohibitions that the author deduces from the three aforementioned points exhibit a commonality in asserting that user-generated content/products must not contain pornographic content.

Currently, there are many deepfake sites that are actually intended to create pornographic content, such as the website nudify.net and many others. Individuals who employ this electronic system are referred to as private scope electronic system organizers (Private PSE). According to Article 1 point 6 of the Minister of Communication and Information Technology Regulation Number 5 of 2020, also known as Permenkominfo 5/2020, Private Sphere Electronic System Providers (Private PSE) are defined as electronic system providers operated by people, commercial entities, and

 DOI: https://doi.org/10.29313/mimbar.v39i2.2965

communities. To ensure efficient functioning of its business operations, Private PSE must prioritize the enhancement of user ease inside its electronic system. It is imperative to mitigate any issues that may impede user activity and perhaps jeopardize the integrity of the Private PSE.

Private Public Service Entities (PSEs) bear the responsibility of effectively arranging electronic systems and ensuring the reliable, secure, and responsible management of information and electronic documents inside said systems, as stipulated in Article 9, paragraph (1) of Permenkominfo 5/2020. One of the key aspects to consider is the verification of the electronic system utilized, confirming its compliance with the regulations outlined in Article 9, paragraph (3) of Permenkominfo 5/2020. The term "containing prohibited information and electronic documents" refers to information and electronic documents that include explicit content such as pornography and/or materials related to gambling. The provision outlined in Article 15, paragraph (1), letter b of Permenkominfo 5/2020 encompasses the inclusion and/or facilitation of information and electronic documents pertaining to gambling.

According to Article 13, paragraph (1) of Permenkominfo 5/2020, the Private PSE is required to cease access to electronic information and documents that contain banned content. In the event that an independent takedown is not conducted, members of the public have the option to file a formal request for takedown to the Minister, as stipulated in Article 15, paragraph (1), letter b of Permenkominfo 5/2020. Moreover, it should be noted that the Minister has the authority to issue a directive to the Private PSE, instructing them to remove any information and documents pertaining to gambling and/or pornography transmitted over electronic mail (e-mail) or other electronic systems, as stipulated in Article 15, paragraph (5) of the Permenkominfo 5/2020. The act of taking down content is executed within a maximum period of 24 hours subsequent to the receipt of the warrant, as stipulated in Article 15, paragraph (6), letter b of the Regulation of the Minister of Communication and Information Technology No. 5 of 2020. In the event that the information and electronic documents are of an urgent nature. In the context of its impact on societal tranquility and the maintenance of public order.

The process of takedown is promptly executed without any delay, ensuring that it is completed within a maximum time frame of four hours subsequent to the receipt of the warning, as stipulated in Article 15, paragraph 9 of Permenkominfo 5/2020. In the context of PSE User Generated Content (PSE UGC), it is noteworthy that a maximum of three warning letters are issued for content removal. The time limit for removal is equivalent to the timeframe allotted for private Public Service Enterprises (PSEs) in a broad context. Failure to comply with the directive issued by PSE UGC may result in the imposition of administrative penalties, specifically in the form of monetary fines, as stipulated in Article 15, paragraph 10 of Permenkominfo 5/2020. According to Article 15, paragraph (9) in conjunction with paragraph (12) of Permenkominfo 5/2020, the Minister has the authority to implement access blocking or issue directives to Internet Service Providers for the purpose of preventing access to electronic systems.

Liability of Perpetrators of Abuse of Deepfakes in Artificial Intelligence Technology in Pornographic Content Based on Indonesian Laws

The issue addressed by the author in this article is closely intertwined with the ramifications of employing deepfakes, a byproduct of advancements in artificial intelligence technology. The author has discovered a number of videos containing explicit material in Indonesia that are suspected to have been created utilizing deepfake techniques. The movies in question featured prominent individuals from the country, specifically Gisella Anastasia and Nagita Slavina, whose images were combined with explicit content. Upon the dissemination of the film across many social media platforms, its rapid virality inside Indonesia prompted an influx of inquiries directed towards the two prominent individuals involved, who found themselves confronted with probing interrogations concerning their alleged involvement in a pornographic video. (Faqih, 2022)

According to the aforementioned explanation, this behavior can be categorized as a type of cybercrime, specifically falling under the category of unauthorized content (Suseno, 2012). In the realm of cybercrime, it is imperative that those who engage in criminal activities assume full accountability for the damages they have inflicted. Moreover, they have responsibility for any additional losses stemming from their negligence or lack of prudence. The realization of a legally recognized entitlement and duty invariably necessitates the presence of a corresponding legal accountability. Hans Kelsen posits that the notion of legal obligation is intrinsically linked to the notion of legal responsibility. Hence, individuals bear the duty to assume legal accountability for specific behaviors, so assuming legal responsibility, which entails being held liable for the outcomes resulting from their activities (Bachtiar et al., 2021). The regulation of pornography in Indonesia is

governed by Law No. 44 of 2008, which is commonly referred to as the Pornography Law. Pornography refers to a wide range of visual and auditory materials, including images, sketches, illustrations, photos, writings, sounds, moving images, animations, cartoons, conversations, gestures, or other forms of messages.

These materials are disseminated through various forms of communication media and/or public performances. It is important to note that pornography is characterized by its explicit depiction of obscenity or sexual exploitation, which is deemed to be in violation of the prevailing standards of decency within society. This definition is outlined in Article 1, paragraph (1) of the Pornography Law. According to Article 4, paragraph (1) of the Pornography Law, individuals are explicitly forbidden from engaging in activities such as producing, creating, replicating, distributing, broadcasting, importing, exporting, offering, trading, renting, or providing pornography. According to the stipulations outlined in the article, an individual (referred to as the perpetrator) can be held legally accountable by satisfying the constituent parts of the criminal offense, which include: (1) Engaging in the act of creating or producing, and (2) The specific object of said conduct, namely pornography that depicts sexual intercourse. According to the criminal requirements outlined in Article 29, in conjunction with Article 4 paragraph (1) of the Pornography Law, an individual who commits an offense (referred to as the offender) may face a maximum jail sentence of 12 (twelve) years and/or a maximum fine of Rp. 6,000,000,000.00 (six billion rupiah). The author previously elucidated the concept of deepfakes, wherever an individual might seamlessly superimpose the visage of one person onto another film by amassing a substantial collection of photographs for analysis and subsequent utilization by the deepfakes algorithm.

The accessibility of deepfake technology facilitates the production of explicit video content by those with malicious motives. The illicit utilization of deepfake technology to create pornographic videos that feature non-consenting individuals is unequivocally prohibited under the Pornography Law. This transgression is compounded by the fact that the creation of such videos occurs without the knowledge or consent of the individual whose likeness is manipulated using deepfake techniques (as stipulated in Article 9 of the Pornography Law). According to the stipulations outlined in Article 8 of the Pornography Law, individuals are expressly forbidden from purposefully or willingly subjecting themselves to being shown or portrayed as objects or models in materials containing pornographic content. According to the stipulations outlined in Article 9 of the Pornography Law, individuals who engage in the unauthorized pairing of individuals' faces can be held legally accountable. This liability arises from the fulfillment of two essential elements of the criminal offense: (1) the act of creating such pairings, and (2) the specific object of the act, which involves using another person as a subject or model in the production of pornographic material. According to the criminal provisions outlined in Article 35 in conjunction with Article 9 of the Pornography Law, an individual who commits an offense (referred to as the offender) may face a punitive measure of up to 12 (twelve) years of imprisonment and/or a maximum monetary penalty of Rp. 6,000,000,000.00 (six billion rupiah).

Conclusions

The current regulatory framework in Indonesia lacks particular legislation pertaining to the governance of artificial intelligence (AI) technology. Consequently, the legal parameters for AI are mostly derived from the interpretations and rules outlined in the Information and Electronic Transactions (ITE) Law. This encompasses the regulation pertaining to the utilization of deepfakes under the jurisdiction of Indonesia. The imperative for the state to assume its regulatory function necessitates the expeditious formulation of more precise legislation pertaining to artificial intelligence (AI) technology in Indonesia. Given that the advancement and use of AI necessitate legal frameworks for its progress, it is incumbent upon the state to undertake this task. Certainly, the establishment of clear legal parameters is essential to ensure confidence in defining the boundaries of usage and exploitation, while also mitigating the risk of a legal void in case of potential future misuse. In addition to this, it is imperative for the government to ensure the dissemination of comprehensive information and awareness among the general populace concerning the appropriate usage and application of deepfakes, with the aim of preventing their misuse for unlawful purposes. Certainly, it is imperative to establish stringent regulations in the foreseeable future pertaining to accountability and just penalties for individuals who exploit the capabilities of deepfake.

References

Ahmed, Saifuddin, Wei Ting Ng, Sheryl, Wei Ting Bee, Adeline. (2023). Understanding the role of fear of missing out and deficient self-regulation in sharing of deepfakes on social media: Evidence from eight countries. Front Psychol. 2023; 14. https://doi.org/10.3389/fpsyg.2023.1127507

 DOI: https://doi.org/10.29313/mimbar.v39i2.2965

Agus Syihabudin, Asep Wawan Jatnika, Alamta Singarimbun, Shohib Khoiri. (2019). The Development of Information Technology Applications of Religious Charity Through Humanities Technology Approach. MIMBAR Jurnal Sosial dan Pembanugnan, Vol. 35 No. 2, https://doi.org/10.29313/mimbar.v35i2.4885.

Asikin, Z. (2016). Pengantar metode penelitian hukum. Rajawali Pers.

Bachtiar, E., Duwila, A. A., Chaerul, M., Affandy, N. A., Makbul, R., Tanjung, R., Purba, B., Saidah, H., Sutrisno, E., & Sari, M. (2021). Pengetahuan Kebencanaan dan Lingkungan. Yayasan Kita Menulis. https://doi.org/10.59141/jiss.v3i08.661

Dwityas, N. A. (2016). Komunikasi dan Pariwisata: Peran User Generated Content Bagi Traveler dalam Media Sosial. Jurnal Simbolika, Volume 2, 4. https://doi.org/10.31289/simbollika.v2i1.224

Edison H Manurung. (2019). Peran Hukum dan Tantangan Penegak Hukum dalam Menghadapi Era Revolusi Industri 4.0. Jurnal Penelitian Hukum, Volume 1, 129. http://ojs.mputantular.ac.id/index.php/sj/article/view/354/276

Efendi, Y. (2018). Internet of Things (IOT) sistem pengendalian lampu menggunakan Raspberry PI berbasis mobile. Jurnal Ilmiah Ilmu Komputer Fakultas Ilmu Komputer Universitas Al Asyariah Mandar, 4(1), 19–26. https://doi.org/10.35329/jiik.v4i1.48

Faathurrahman, M. Faqih, Soerjati, Enni. (2022). Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia. Jurnal Indonesia Sosial Teknologi, Vol. 3, 11. http://dx.doi.org/10.36418/jist.v3i11.528

G, W. S. dan E. (2016). Membuat Term & Conditions. https://usahasosial.com/wpcontent/uploads/2016/06/membuat_terms_conditions_2016JunWed00183445310.pdf.

Hudini, T. (2017). Teknologi Informasi dan Komunikasi Bagi Mahasiswa dalam Pemanfaatan Diplomasi Digital: Nasional dan Internasional. Faktor Exacta, 10(2), 172–182. https://doi.org/10.30998/faktorexacta.v10i2.1305

Istiarni, A., & Kurniasari, E. (2020). Peran Perpustakaan Digital Dalam Menciptakan Ruang Publik (Studi Kasus Perpustakaan Digital Universitas Lampung). Fihris: Jurnal Ilmu Perpustakaan Dan Informasi, 15(1), 31–53. https://doi.org/10.14421/fhrs.2020.151.31-53

Khusna, I. H., & Pangestuti, S. (2019). Deepfake, Tantangan Baru Untuk Netizen (Deepfake, A New Challenge For Netizen). Promedia (Public Relation Dan Media Komunikasi), 5(2). https://doi.org/10.52447/promedia.v5i2.2300

Kurnia, M. A. A. . & A. (2021). Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi. Volume 2, 48.

Lisa Adhrianti, Indah Septirisani, Neneng Cucu Marlina. (2022). Communication Patterns of Cybercrime in The Financial Technology Business During The Covid-19 Pandemic. MIMBAR Jurnal Sosial dan Pembanugnan, Vol. 38 No. 2, https:// https://doi.org/10.29313/mimbar.v0i0.10077.

Lubis, M. S. Y. (2021). Implementasi Artificial Intelligence Pada System Manufaktur Terpadu. Seminar Nasional Teknik (SEMNASTEK) UISU, 4(1), 1–7. https://jurnal.uisu.ac.id/index.php/semnastek/article/view/4134

Muchtar, M. A. dan H. N. (2018). Cyberlaw: Perlindungan Hukum Bagi Orang Terkenal dari Cybersquatting. Logoz Publishing.

Novi, A. (2019). Internet of Things dan Kecerdasan Buatan Pengenalan, Penerapan dan Studi Kasus Industri. CV. Tampuniak Mustika Edukarya. http://repository.unas.ac.id/2269/1/buku pertama upload.pdf

Riantrisnanto, R. (2020). Pamer Hasil Analisa Video Mirip Gisel, Roy Suryo Minta Waspada Deepfake. https://www.liputan6.com/showbiz/read/4403933/pamer-hasil-analisa-video-mirip-gisel-roy-suryo-minta-waspada-deepfake

Schwartz, O. (2018). You thought fake news was bad? Deep fakes are where truth goes to die. Guardian. https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth

Struensee, S.V. (2021). Analyzing Dilemmas Posed by Artificial Intelligence and 4IR Technologies Requires using all Available Models, Including the Existing International Human Rights Framework and Principles of AI Ethics. SSRN Electronic Journal June 25, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3874279

Suseno, S. (2012). Yurisdiksi Tindak Pidana Siber. Refika Aditama.

Tantri, A. H., Riyadi, M. A. F., & Wanabil, N. (2022). Pemanfaatan Kecerdasan Buatan Dalam Kegiatan Pengabdian Masyarakat di Indonesia: Sebuah Tinjauan Pustaka Sistematis. Notasi, 1(2), 21–28. https://journal.kallabs.ac.id/index.php/home/article/view/25.

 DOI: https://doi.org/10.29313/mimbar.v39i2.2965