

Construction of Legal Protection for Consumers Against the Misuse of Deepfakes in Advertising Social

Dewi Nur Hidayah 

Universitas Negeri Semarang, Semarang, Indonesia
dewingnjik@students.unnes.ac.id

Ubaidillah Kamal 

Universitas Negeri Semarang, Semarang, Indonesia
ubaidillahkamal@mail.unnes.ac.id

Abstract

Deepfakes, which utilize artificial intelligence to produce hyper-realistic audiovisual content in social media advertisements, are increasingly being misused by irresponsible businesses, who are exploiting deepfake technology to create advertising content. This study aims to identify existing regulatory frameworks in Indonesia and consumer legal protection against the misuse of deepfake technology, and to provide recommendations for strengthening the legal system to combat content manipulation by deepfake abuse. This study employs a normative juridical method, employing a statute approach. The data used in this study include both primary and secondary legal materials, including relevant regulations and related literature. The data collection technique used a literature study. The results of the study indicate a legal vacuum and significant difficulties in detecting and proving deepfake violations in social media advertisements. Although regulations exist, the misuse of deepfake technology is not yet explicitly regulated, so legal protection for consumers is not optimal. Consumer legal protection can be provided



through two approaches: preventive legal protection and repressive legal protection. The increasingly sophisticated development of AI also increases the risk of misuse that harms consumers and society, necessitating adaptive legal responses to ensure more effective protection in this era of technological advancement. This research is expected to serve as a reference for regulators in developing strategic steps to address the threat of deepfakes.

KEYWORDS

Legal Protection, Consumers, Artificial Intelligence, Deepfake, Advertising

Introduction

Technological advances are now developing rapidly, one of which is the emergence of *Artificial Intelligence technology* or we know it as AI which has the meaning of artificial intelligence or artificial intelligence that can make human work easier. The development of AI is supported by a number of sub-fields including "*machine learning*" and "*deep learning*".¹ *Machine learning* is a branch of AI that focuses on using algorithms and data to mimic the process of how humans think, while *deep learning* is a branch of *machine learning* that uses "*neural networks*" or artificial neural networks to process data in a more complex way.²

Along with the development of *deep learning*, *deepfake technology* emerged which was born from the combination of the words *deep learning* and *fake*, which refers to the technique of creating fake content by utilizing artificial intelligence using *deep learning methods*. Deepfake technology produces visual manipulation in the form of merging or replacing a person's

¹ Imam Robandi, *Artificial Intelligence " Mengupas Rekayasa Kecerdasan Tiruan"* (Yogyakarta: CV Andi Offset, 2019).

² Bramcov Stivens Situmeang, Ingrid Yolanda Silitonga, Reskina Felida Silaen, Tiurmaida Siringo-ringo, Ester Esari Sipayung, " Pengaruh Artificial Intelligence Terhadap Tingkat Kasus Deep Fake Pada Selebritas di Twitter," *Jurnal Device* 14, no.1 (2024): 80-91.

face in a certain image or video so that it looks like a real condition.³ Thus, the difference between AI and *deepfakes* lies in the position of both. Deepfakes are a technique in the application of AI, specifically deep learning technology, that is used to generate or manipulate media content, both videos and images, making it difficult for the human eye to distinguish it from real content without the help of technology. Meanwhile, AI itself is a technology that allows devices or machines to mimic human behavior.

The development of *deepfake* technology is one example of the development of technology from AI that is often used in creating very convincing photos, audio or videos. The use of *deepfakes* itself can be beneficial in the film and entertainment sector which has been widely used by filmmakers to be able to revive deceased actors or portray fictional characters with stunning realism, but *deepfakes* also have the potential to be misused in the dissemination of misleading or manipulative information. *Deepfakes* have become an important issue in discussions about ethics, privacy, and information security due to their ability to produce convincing content.⁴

But the problem is that nowadays many people abuse the use of this AI technology, resulting in illegal activities including the spread of false information, privacy violations, fraud and cybercrime. The human eye is having a harder time distinguishing between real and fake content due to advances in *deepfake* technology. In its development, *deepfake* technology often raises legal problems such as the dissemination of misleading or incorrect information so that it can affect public views and even damage the reputation of individuals. Until the most common problem in *deepfake technology* is the results of pornographic photos and videos manipulated by *deepfakes*.

³ Rindang Gici Oktavianti, Abdurrahman Muqsith, Isma Nadia, " Penyalahgunaan Deepfake Era Canggihnya Teknologi Memicu Kejahatan Media," *Jurnal IUS* 13, no.1 (2025): 114-122.

⁴ *Ibid*, p. 116.

Along with the development of *deepfake abuse cases* in Indonesia, currently *deepfakes* are not only abused in the creation of manipulative content in the criminal or political realm, but the abuse of *deepfakes* itself has spread in the economic realm such as commercial content. There are at least 500,000 deepfake videos and audios circulating on social media in 2023 and this figure is projected to jump to around 8 million content by 2025, this shows a very rapid growth in the misuse of *deepfake technology*.⁵ In the commercial realm, the digital marketing report notes that business actors use *deepfakes* to create advertisements and promotions that display the faces or voices of public figures and consumers in providing false testimonials, in order to increase social media engagement and can reduce content production costs.⁶

The consequence of creating fake content in advertisements on social media that utilize *deepfake* technology is that consumers do not get honest and correct information about the product. Not only consumers are victims of this action, but those who have the potential to become victims of *deepfake* photos or videos in advertisements on social media are celebrities or public figures. Another example of how *deepfakes* can affect consumers and businesses is the case of Melaney Ricardo, a public figure from Indonesia who became a victim of drastic weight loss advertising who used *deepfake* technology to use her face in advertising.

Several legal studies have confirmed that the use of *deepfakes* in advertising has the potential to mislead consumers due to information manipulation and obscuring the identity of business actors and endorser. Not only that, this also damages consumers' rights to honest and correct information about a product or service offered, as guaranteed in the UUPK.⁷

⁵ Keepnetlabs, *Deepfake Statistics & Trends 2025: Growth, Risks, and Future Insights*, <https://keepnetlabs.com/blog/deepfake-statistics-and-trends> accessed 2025.

⁶ Amra & Elma, *Best Deepfake Marketing Statistics 2025*, <https://www.amraandelma.com/deepfake-marketing-statistics/> accessed 2025.

⁷ Ali Huristak Hartawan Hasibuan, David Novan Setyawan, Yanuriansyah Ar Rasyid, "Legal Protection For Consumers Against The Potential Harm Caused By Promotions Using Deepfakes," *Kyadiren Journal of Law* 6, no.2 (2025): 116-126.

The risks obtained by consumers are not only in the form of economic losses (the condition of the product based on false claims), but can also touch the aspects of privacy and personal data when a person's face or voice is used without permission for commercial purposes.⁸

Legal studies in Indonesia say that the protection of consumers who are harmed by the content resulting from *deepfake* abuse currently rests on a combination of the PK Law, the ITE Law and the PDP Law, but there are no rules that explicitly regulate the abuse of *deepfakes* in advertisements on social media that have the potential to harm businesses and consumers.⁹ The definition of AI or the results of AI such as *deepfakes* has not been clearly explained in the ITE Law which is a reference for related regulations in the Indonesian *cybercrime* world. In the case of manipulation of digital marketing content on social media, when reviewed in other regulations, there is a Consumer Protection Law as a special rule that explicitly regulates the protection of consumers. The Consumer Protection Act does not yet cover AI-based digital content manipulation such as *deepfakes*, which illegally utilize personal data. This regulation has a loophole in overcoming the challenges of AI technology, so legal updates are needed to address these developments.¹⁰

The misuse of *deepfakes* has caused concern among the public and has led to increased awareness of the potential dangers generated by the misuse of *deepfakes*. Article 1 paragraph (3) of the 1945 Constitution stipulates that "Indonesia is a country of law, so all aspects of life in the country should be regulated by law to prevent and reduce existing problems". Several countries have taken preventive steps in making new regulations related to

⁸ Zaenul Haq, "Perlindungan Konsumen Terhadap Ancaman Deepfake dalam Transaksi Digital: Tinjauan Regulasi dan Urgensi Mitigasi," *Journal of Authentic Research* 4, no.2 (2025): 2656-2669.

⁹ Indra Jaya Gunawan, Sylvia Janisriwati, "Legal Analysis on the Use of Deepfake Technology: Threats to Indonesian Banking Institutions," *Law and Justice* 8, no.2 (2023): 192-210.

¹⁰ Gabe Regan, *The State of Deepfake Regulations: What Businesses Need to Know*, <https://www.realitydefender.com/insights/the-state-of-deepfake-regulations> Accessed 2026.

the abuse of *deepfakes* or the results of other AI technologies. The current positive law in Indonesia is not fully able to accommodate the problems that arise due to the abuse of *deepfakes* in manipulated content in advertisements on social media and there is a legal vacuum in the regulations in Indonesia. In line with the rapid development of technology and cybercrime also developing, Indonesia must be adaptive to technological developments in order to protect consumer rights against the abuse of *deepfakes* in advertising on social media.¹¹

The current legal construction in Indonesia is not fully adaptive to the dynamics of technological developments, thus creating a widening legal gap between positive law and the substantive needs of society.¹² The rapid development of AI technology in the abuse of *deepfakes* is not balanced by special arrangements that explicitly regulate consumer rights, misinformation in digital marketing, special categories of losses suffered, and the vagueness of the responsibilities of business actors. This condition creates urgency to assess whether the current positive law in Indonesia is sufficient in tackling the abuse of *deepfakes*. Without progressive legal reforms, the potential for harm to individuals and threats to public order will increase. This is an important issue that needs to be reviewed from a positive legal perspective in Indonesia. This paper will focus on regulations that regulate the misuse of AI-based *deepfake* technology, as well as how the current positive laws in Indonesia are able to provide adequate legal protection for consumers in overcoming legal issues arising from the misuse of *deepfake technology* in advertising on social media.

Previous research used as a reference by researchers includes a journal entitled "The Urgency of Regulation Against the Abuse of *AI-Based*

¹¹ Madalaine Christella Seveney, Demas Brian Wicaksono, Irwan Kurniawan Soetijono, " Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi," *Disiplin : Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda* 31, no.2 (2025): 97-106.

¹² Beth Anastasia Nakita Manulang, Isna Khalimatussa'diah Azzahra, Salsa Alfi Widowati, Ghaida Raisya Ash-Syifa, Ubaidillah Kamal, " *Rekonstruksi Keadilan Substantif Di Era Digital Melalui Mitigasi Legal Gap Menanggapi Fenomena No Viral No Justice Di Indonesia*," *Jurnal Ilmiah Wahana Pendidikan* 11, no.12 (2025): 300-310.

Deepfakes (*Artificial Intelligence*) on Pornographic Content" written by Madalaine Christella Seveney, Demas Brian Wicaksono, and Iwan Kurniawan Soetijono from State University on August 17, 1945 Banyuwangi with the focus of the research being law enforcement against *deepfake acts* in pornographic content as well as arrangements related to deepfake-based pornographic content. In addition, a journal entitled "The Spread of *Deepfake Content* as a Criminal Offense: A Critical Analysis of Law Enforcement and Public Protection in Indonesia" written by Hendra Prayoga, and Hadi Tuasikal from the University of Muhammadiyah Sorong with a focus on research explaining the effectiveness of law enforcement and exploring the weaknesses of existing regulations.

Research on the urgency of the abuse of AI-based *deepfakes* in Indonesia has not been thoroughly conducted. Where in previous research, many researchers only focused on the criminal aspects such as the misuse of *deepfake* technology for pornographic crimes, personal data protection and Online-Based Gender Violence (KBGO). Meanwhile, the abuse of *deepfakes* also extends to economic aspects that both have legal implications, so the dimensions of consumer rights, misinformation in advertising, categories of economic losses and the escape of business actors' responsibilities also need to be studied more deeply. In order to avoid plagiarism and as a form of providing information that this research grows and exists from the ideas or thoughts of the researcher, therefore the researcher will include previous research papers that have similarities in the topic, but due to limitations in the object of study, the researcher expands the object of study, namely the misuse of *deepfake technology* in advertising on social media.

Based on this background, the topic of the research problem can be determined as follows: 1) Legal regulation of the misuse of deepfakes in advertising in Indonesia, 2) Legal protection for consumers against the misuse of deepfakes in advertising on social media. This research will also explore existing regulatory weaknesses and researchers encourage

responsive regulatory updates in addressing problems caused by *deepfake* abuse. It is hoped that by conducting this research, the contribution of researchers can help the Indonesian legal system adapt to new developments in digital technology and improve consumer protection. Therefore, the researcher decided to analyze this problem more deeply and was able to raise a journal with the title "CONSTRUCTION OF LEGAL PROTECTION AGAINST CONSUMERS FOR THE ABUSE OF *DEEPFAKES* IN ADVERTISING ON SOCIAL MEDIA".

Method

This study uses a type of normative juridical research with a qualitative method. Based on the applicable regulations by analyzing the law as a norm that becomes a guideline for behavior and conducting an inventory of positive laws in Indonesia to solve the legal problems faced.¹³ The approach used in this study has been adjusted to the type of research that has been taken by the researcher, using a statutory approach (*statue approach*), namely by researching a regulation that is relevant to the legal issues discussed. With regard to this, there is no specific law governing the misuse of *deepfake* technology. In the legislative approach, the researcher uses the PK Law, ITE Law, PDP Law, Permenkominfo-PSE and PP-PSTE.

The data used in this study consists of 2 (two) sources of legal materials, namely the primary sources of legal materials used are the PK Law, ITE Law, PDP Law, Permenkominfo-PSE and PP-PSTE as well as secondary sources of legal materials in the form of several journals from previous research, doctrines, books, documents, reports and relevant scientific articles. The technique used by researchers in collecting research data is using literature studies or library *research* to collect primary and

¹³ Vicky Srivastava, *Buku Ajar: Metode Penelitian Hukum* (Yogyakarta: Publika Global Media, 2024).

secondary legal materials.¹⁴

In carrying out the validity of the data, the researcher used the triangulation method. According to Lexy J. Moleong, "Triangulation is a technique of checking the validity of data that utilizes something else, outside of the data for the purpose of checking or as a comparison to the data".¹⁵ To ensure the validity of the data in this study, the researcher will use the triangulation method in conducting data validity by comparing information from various legal texts, case studies, and expert opinions to obtain valid conclusions based on academics. The data that has been obtained is analyzed using a qualitative method in a descriptive manner by providing an overview or explanation of the object and subject being studied and its findings.¹⁶ This data analysis consists of data classification, legal policy assessment, normative interpretation, and in-depth discussion of the effectiveness of the applicable law by not using numbers, but by providing an overview in the form of words. The purpose of this analysis is to identify the current regulatory framework, legal protection for consumers based on the positive laws that exist in Indonesia against the misuse of deepfake technology, and provide suggestions to improve the ability of the legal system to overcome content manipulation by deepfake misuse.

Results and Discussion

1. Legal Regulations Against the Abuse of *Deepfakes* in Advertising in Indonesia

One of the main components of a marketing strategy is advertising, which aims to inform consumers about product information. Advertising

¹⁴ Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Press, 2020).

¹⁵ Lexy J. Moleong, *Metodologi Penelitian Kualitatif* (Bandung: PT. Remaja Rosdakarya, 2017).

¹⁶ Gunardi, *Buku Ajar Metode Penelitian Hukum* (Jakarta: Damera Press, 2022).

has the potential to influence consumers in making purchasing decisions. Advertising is known as a series of communication efforts that aim to inform, convince, and remind consumers about the goods and services offered. According to Kotler and Keller, "advertising is *any form of non-personal presentation and promotion of ideas, goods, or services by a particular sponsor that must be paid*". Therefore, it can be said that advertising is any form of impersonal presentation that aims to spread knowledge about the attributes and advantages of a product supported by a particular sponsor.¹⁷

Before social media advertising, business actors promoted their merchandise through conventional media such as TV, radio, magazines, and others. Due to the increasing consumer need for ease of shopping, business actors have turned to marketing their merchandise online in line with the advancement of the digital era. Consumers only need to access the internet, search for the goods they want, and the business actor will arrange all the things necessary to send them to them.¹⁸ To get the best results, businesses must create an advertising plan that takes into account consumer needs and market characteristics.¹⁹

The use of deepfakes in advertising is a new breakthrough in marketing that uses artificial intelligence to produce highly realistic audio-visual content for advertising. This technology allows the creation of audio and video content featuring characters or people that can be used to capture the attention of consumers in new and engaging ways.²⁰ In the context of product marketing, businesses can use deepfakes to generate ads featuring

¹⁷ Emilia Ebby, Irawansyah, " Penggunaan Celebrity Endorser pada Media Sosial Instagram dalam Meningkatkan Brand Engagement," *Jurnal Ilmiah Wahana Pendidikan* 7, no.5 (2021): 73-86.

¹⁸ Ibid, p.74.

¹⁹ Adiawaty Susi, Albert Budiyanto Kambuno, Suryati Veronika, Salman Habeahan, and Bernard E Silaban, "The Influence of Promotion and Brand Image on Purchase Decisions on the Market Place Application," *Judicious* 3, no. 2 (2022): 370–373.

²⁰ Min Liu, Xijin Zhang, "Deepfake Technology and Current Legal Status of It," (2023): 1308–14.

celebrities or other famous people promoting their goods, even if the individual has never done so and has not received payment.²¹

There are various advantages to using deepfakes in creating advertisements on social media. First, deepfakes can help businesses to better tailor advertising messages, reaching a wider market. Second, this technology can increase the visual appeal of advertisements so that they are more attractive to potential consumers.²² To provide a more individualized and relevant experience, the resulting advertising videos can be tailored to the tastes of specific potential consumers. Third, it can reduce the cost of producing expensive advertising content and the cost of *endorsements* of certain artists or celebrities in promoting the goods/services to be offered.

Behind the various advantages of using deepfake technology, this can be used by irresponsible business actors who misuse deepfake technology for personal gain. This problem certainly has various bad influences that will have an impact on every level of society, not only consumers and celebrities but the general public can also be misused by personal photos for personal commercial interests. The misuse of deepfake technology can also pose serious dangers, such as consumer fraud through fake product claims, violation of the privacy of public figures, loss of public trust in digital advertising, and the risk of spreading hoaxes that have a wide impact on consumer health and finances.

However, the misuse of deepfake technology in advertising content on social media has not been explicitly regulated by laws and regulations in Indonesia, so its current supervision and enforcement only rely on general provisions in the UUPK, ITE LAW, PDP Law, Permenkominfo-PSE, and PP-PSTE which emphasize the principle of information honesty and the

²¹ Ali Huristak Hartawan Hasibuan, David Novan Setyawan, Yanuriansyah Ar Rasyid, *Op. cit*, p.119.

²² Willy Kristian, *Deepfake dan AI dalam Dunia Periklanan: Ancaman atau Peluang?*, <https://binus.ac.id/bekasi/2025/01/deepfake-dan-ai-dalam-dunia-periklanan-ancaman-atau-peluang/> accessed 2026.

prohibition of manipulating misleading content without specific norms for artificial intelligence technology such as deepfakes.

a. "Law Number 8 of 1999 concerning Consumer Protection"

Regarding consumer rights as stated in Article 4 letter a of the UUPK "consumers have the right to comfort, security, and safety in consuming the goods and/or services offered²³", so this can be seen as the most important and basic thing in providing protection to consumers. An inconvenient product or service is inherently unfit to be manufactured or distributed to the public, especially if it does not offer safety or potentially jeopardizes consumer safety. Therefore, consumers have the right to make decisions about the goods or services they want based on clear, open, accurate, and honest information to ensure that the goods or services used meet the aspects of convenience, safety, and do not pose a risk to consumers and also have the right to file complaints and receive protection in the form of advice, advocacy, fair treatment, and compensation or compensation in accordance with applicable law if applicable. deviations that cause losses.²⁴

According to the opinions of Ahmadi Miru and Sutarman Yodo, "the right that consumers have to security and safety is intended to ensure the security and safety of consumers in the use of the goods/services they obtain, so that consumers can avoid losses (physical or psychological) when consuming a product offered."²⁵ By referring to the case of a video of deepfake technology manipulation circulating on the social media platform TikTok regarding the promotion of products for people with diabetes by irresponsible business actors, using the faces of Najwa Shihab, a journalist,

²³ Article 4 letter a of Law Number 8 of 1999 concerning Consumer Protection.

²⁴ Rochani Urip Salami, I Ketut Karmi Nurjaya, and Krisnhoe Kartika, " Penerapan Pasal 4 Undang-Undang No.8 Tahun 1999 Tentang Perlindungan Konsumen Pada Jasa Pengiriman Dokumen Di PT. Kerta Gaya Pusaka Perwakilan Purwokerto," *Jurnal Dinamika Hukum* 8, no.2 (2008): 146-153.

²⁵ Ahmadi Miru, Sutarman Yodo, *Hukum Perlindungan Konsumen* (Jakarta: PT. RajaGrafindo Persada, 2004).

and Doctor Terawan Agus Putranto, a former Minister of Health of the Republic of Indonesia.

The case of misuse of deepfake technology using the faces of a journalist Najwa Shihab and a former Indonesian Minister of Health Dr. Terawan became the main highlight in discussions by the public about the threat of AI technology in cybercrime. The business actor misused deepfake technology to create an advertising video that featured Najwa Shihab as if she was directly promoting herbal medicine products for diabetics and added a video of Dr. Terawan which seemed to validate the promotion carried out by Najwa Shihab previously and added false claims related to the efficacy of the herbal medicine product using a medical point of view.

The video was then filmed or commonly known as "*stitch*" by a doctor named Greg Faldo on the social media platform TikTok with the same *username* on April 24, 2024. The doctor responded that the video from the results of the misuse of *deepfake* technology is very risky for people who believe in the hoax video, especially for diabetics who are now using insulin to control blood sugar levels to remain stable, then unilaterally stop using the insulin without consulting a doctor first and switch to drugs that are still scientifically unclear effectiveness or efficacy. This causes blood sugar levels to be increasingly uncontrolled and causes other complications such as stroke on the brain, blindness, heart failure and kidney failure.

Reflecting on this case, the misuse of deepfake technology allows perpetrators to produce content that appears as if it is authentic or real, creating a distortion of reality that can interfere with consumer rights, because consumers are influenced by false promotions that cause a false perception of the quality, safety, or benefits of goods/services. When deepfakes exploit the credibility of public figures to persuade purchase decisions, it has the potential to result in financial and non-financial losses for consumers who trust this information as a safe basis for consumption. This condition shows the importance of increasing vigilance by the public in

responding to every information received, especially information sourced from unofficial parties or channels.²⁶

In addition to Article 4 letter a, the misuse of deepfakes in the manipulation of advertising content can also violate consumer rights, namely "obtaining true, clear, and honest information about the conditions and guarantees of the goods/services offered" based on Article 4 letter c of the UUPK. This article expressly guarantees the consumer's right to information about goods and/or services, which is the main foundation for rational and safe purchase decisions. Every consumer, in principle, certainly does not want to suffer losses due to consuming certain goods or services. For consumers, accurate information about these goods or services is an essential need that is the basis for rational decision-making before allocating their financial resources such as salaries, wages, honorariums, or other forms of income to make transactions.²⁷

In addition, Article 3 letter d of the UUPK stipulates that "the purpose of consumer protection includes the creation of a system that ensures legal certainty, information disclosure, and information accessibility for consumers". Consumers' right to honest, accurate, and transparent information about the terms and conditions of the goods or services they consume is implied in the element of transparency and access to information, which is the responsibility of business people in realizing an efficient protection system. Thus, this provision is a normative basis for the enforcement of consumer rights to the provision of true, honest and non-misleading information.

Ahmadi Miru and Sutarman Yodo argue that the consumer's right to accurate and clear information is very important because poor information

²⁶ Yoan Shevila Kristiyenda, Jasmine Faradila, Christina Basanova, " Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan DeepfakePrabowo Subianto dalam Tawaran Bantuan Uang," *ALADALAH : Jurnal Politik, Sosial, Hukum dan Humaniora* 3, no.2 (2025): 149-164.

²⁷ Rochani Urip Salami, I Ketut Karmi Nurjaya, and Krisnhoe Kartika, *Op.cit*, p.149

from business people can be considered a type of product defect, especially instructional defects or defects caused by inadequate information. This right is intended to provide customers with a clear picture of a product, allowing them to choose goods or services that meet their unique needs and preventing possible losses due to misuse or mistaken beliefs about the condition of the product.²⁸

This is of course related to the obligations of business actors in Article 7 letter b of the UUPK, which requires the submission of true, clear and honest information, as well as the prohibition of misleading advertising in Article 17 paragraph (1) letter a of the UUPK. The use of deepfakes in advertising not only blurs the line between fact and fiction, but also prevents consumers from obtaining information on the actual condition of the product, thus not only harming consumers economically, but also causing immaterial losses such as loss of trust in digital marketing. Thus, the regulation of Article 4 letter c functions as a preventive and repressive instrument, allowing consumers to demand compensation under Article 19 of the UUPK for violations of false information, while encouraging the formation of specific regulations against manipulative technologies such as deepfakes in the realm of digital marketing.²⁹

Regarding the prohibition of misleading advertising by business actors in Article 17 paragraph (1) letter a of the UUPK, if MSME business actors hire the services of a third party in creating advertising content and the third party uses deepfakes in its manufacture without the knowledge of the MSME owner, then in cases like this, the first party to be held accountable is the MSME business actor because he has responsibility for the advertisements produced or marketed on behalf of his business. Meanwhile,

²⁸ Ahmadi Miru, Sutarman Yodo, *Op.cit*, p.41.

²⁹ Evita Lanosta, Tri Anggraini, " Perlindungan Konsumen Atas Informasi Yang Benar Terhadap Promosi Produk Dalam Transaksi Perdagangan Elektronik Menurut Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen," *Jurnal Hukum Adigama* 4, no.1 (2021): 534-559.

Article 19 emphasizes the obligation of business actors in providing compensation for consumer losses.

Internally, MSME business actors can sue third parties based on default if the third party violates the content of the agreement and if the MSME business actors do not know and never agree to the use of deepfakes, then the third party who creates advertising content can be held primarily responsible as the perpetrator of unlawful acts, especially if the element of intentionality and manipulation can be proven. The legal basis regarding the agreement refers to Article 1338 of the Civil Code, which emphasizes that agreements that have been agreed upon and made legally apply as laws to the parties, so that third parties as creators of advertising content are obliged to comply with mutually agreed agreements. Therefore, in the internal relationship between MSME business actors and advertising service providers, the responsibility for consumer losses remains attached to MSME business actors and can be sued back to third parties based on cooperation agreements (contracts) or the basis of unlawful acts.

Violations by business actors related to promotion may be subject to administrative sanctions and criminal sanctions. Based on Article 60 of the UUPK, it states that "BPSK is authorized to impose administrative sanctions on business actors who violate Article 19 paragraphs (2) and (3), Article 20, Article 25, and Article 26 in the form of determining compensation of a maximum of Rp.200,000,000.00 (two hundred million rupiah)."³⁰ Meanwhile, criminal sanctions against business actors and/or their administrators are regulated in Articles 61 to 63 of the UUPK. In addition to the criminal sanctions of imprisonment and fines, in Article 63 it is stated that, "these sanctions can be used as additional punishments in the form of confiscation of certain goods, announcement of a judge's decision, payment of compensation for orders to stop certain activities that cause consumer losses, obligation to withdraw goods from circulation or revocation of

³⁰ Article 60 of Law Number 8 of 1999 concerning Consumer Protection.

business licenses."³¹ The application of administrative sanctions and criminal sanctions is intended to defend consumer rights, increase business actors' compliance with the provisions of consumer protection regulations, and have a deterrent effect on business actors who violate consumer rights.

b. "Law Number 11 of 2008 concerning Information and Electronic Transactions"

In Indonesia, the misuse of deepfake technology has various legal implications, both in the criminal and civil realms, given its ability to manipulate media content such as audio, images, or videos that are harmful or misleading to other parties. Thus, the law should ideally be adaptive to the dynamics of the times by responding to changes that occur with a solid foundation, and serving the interests of the community while still being grounded in the moral values embodied by law enforcement. Until now, Indonesia has not specifically regulated artificial intelligence (AI) and the technology produced, including deepfakes. Since the features of AI technology can conceptually be compared to "electronic agents," these restrictions can be linked to a number of laws in force today, although there is no specific law that specifically regulates artificial intelligence or deepfakes as defined in the ITE Act.

It is explained in Article 1 paragraph (1) of the ITE Law, "Electronic Information is one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail (electronic mail), telegrams, telexes, telecopies or the like, letters, signs, numbers, access codes, symbols, or perforations that have a meaning or can be understood by people who are able to understand them".³² Meanwhile, the regulation regarding electronic agents that have conceptual similarities with artificial intelligence (AI) and deepfake technology is contained in Article 1 paragraph (8) of the ITE Law,

³¹ Article 63 of Law Number 8 of 1999 concerning Consumer Protection.

³² Article 1 paragraph (1) of Law Number 11 of 2008 concerning Information and Electronic Transactions.

"An Electronic Agent is a device of an Electronic System that is made to perform an action on a certain Electronic Information automatically organized by a Person".³³ The word "automatic" in the Great Dictionary of the Indonesian Language (KBBI), which refers to the ability to work independently, is the conceptual basis for equating the characteristics of artificial intelligence (AI) with electronic agents. Thus, it can be assumed that legal arrangements regarding "electronic agents" can also be applied to AI technologies that have similar functional tools.

The act of manipulating advertising content through the misuse of deepfake technology has not been specifically regulated in the legal realm of the ITE Law, so its implementation faces various challenges, especially in proving and collecting adequate evidence to ensnare irresponsible business actors. Article 1 paragraph (8) of the ITE Law explains that an electronic agent is a system that operates automatically, which conceptually has similarities with AI. However, AI technology does not yet have specific regulations because it is *open source* and difficult to track, in contrast to digital platforms such as *e-commerce* sites which are regulated on stricter electronic system settings. This ambiguity creates ambiguity regarding legal responsibility for the use of AI, given that there is no law explicitly outlining its accountability.³⁴

Although it has not been explicitly regulated regarding AI, the legal basis for regulating AI technology has been established by the ITE Law, especially in the context of deepfakes.³⁵ A series of acts committed by irresponsible business actors in creating advertising content on social media using celebrity faces for personal gain without payment of commercial rights by abusing deepfake technology, including acts that violate laws and

³³ *Ibid.*

³⁴ Madalaine Christella Seveney, Demas Brian Wicaksono, Irwan Kurniawan Soetijono, *Op.cit*, p.102.

³⁵ Sabrina Nur Syahirah, Bayu Prasetyo " Tinjauan Yuridis terhadap Penggunaan Teknologi Deepfake untuk Pornografi Melalui Artificial Intelligence (AI) di Indonesia," *Jurnal Inovasi Hukum dan Kebijakan* 6, no.1 (2025): 201.

regulations as stated in Article 35 of the ITE Law, "Every Person deliberately and without rights or against the law commits manipulation, creation, alteration, disappearance, destruction of Electronic Information and/or Electronic Documents with the aim that such Electronic Information and/or Electronic Documents are considered as if they were authentic data". The Article does not specifically regulate advertising content on social media, only regulates the manipulation of electronic information or electronic documents to make it look authentic without mentioning the specific type of content that contains economic aspects of digital marketing.

In the case of Melaney Ricardo, when the business actor manipulated the artist's face and voice to create a seemingly authentic advertising video, so that consumers get the fake testimonials as genuine and trustworthy recommendations. Melaney's clarification, which confirmed that she had never carried out the promotion, reinforces the element of deliberate manipulation that violates the norms of Article 35 with the aim of misleading the public about the authenticity of promotional information. This case not only causes economic losses for consumers who buy products based on false advertisements, but also undermines public trust in digital content, potentially triggering criminal charges by law enforcement officials or civil reports by victims. Violation of Article 35 of the ITE Law in the case of deepfake Melaney Ricardo is threatened with Article 12 of the ITE Law, which states "a maximum prison sentence of 12 (twelve) years and/or a maximum fine of Rp.12,000,000,000.00 (twelve billion rupiah)".

Meanwhile, if deepfakes are used to spread false information that can disturb public order, Article 28 paragraph (1) of the ITE Law can be applied. However, given that the difficulty in establishing digital crimes sometimes involves hard-to-identify perpetrators and evidence that is vulnerable to authenticity verification, the effectiveness of this law enforcement is still in doubt. This article punishes the spread of fake news that deliberately causes unrest in the community as stipulated in Article 45 paragraph (2), namely "with a maximum prison sentence of 6 years and/or a fine of Rp.1 billion".

In the perspective of the study, this article applies to deepfake advertisements that promote false claims about products (e.g., miracle drugs) that trigger irrational consumption decisions, mass economic losses, and public distrust of social media platforms as credible transaction spaces.

Based on positive law in Indonesia, it emphasizes the role of AI as an "electronic agent", which is a technology created to carry out automated activities on electronic information. However, complex concerns such as ethics, privacy, and the social impact of the use of AI technology are not adequately addressed by current legislation. The ambiguity of this legal framework also creates ambiguity regarding accountability in the use of AI. In addition, rather than directly regulating substantive actions such as deepfake manipulation in advertising, current regulations focus more on prohibiting the transmission, distribution, or provision of access to electronic information or documents that deceive and harm consumers.³⁶

The proof of deepfake videos as electronic evidence is regulated in Article 5 paragraphs (1) and (2) of the ITE Law, because it recognizes electronic information, electronic documents, and their printed results as valid legal evidence and the expansion of valid evidence in procedural law in Indonesia. Article 5 paragraph (4) of the ITE Law emphasizes that electronic information or electronic documents do not apply as evidence if they are made for purposes exempted by law, so the authenticity and context of their acquisition must still be tested. So that the validity of deepfake videos as electronic evidence must be tested through digital authentication and forensic examination, not only seen from its hyper-realistic appearance.

The judge is basically not enough to judge the appearance of the video that looks convincing, but must judge from the entire set of evidence rationally and based on beliefs supported by the facts of the trial. Therefore,

³⁶ Yolanda Frisky Amelia, Arfan Kaimuddin, Hisbul Luthfi Ashsyarofi, "Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia," *Dinamika Jurnal Ilmiah Hukum* 30, no.1 (2024): 9675-9691.

the authenticity of videos needs to be strengthened through digital forensics, namely technical examination through metadata, editing traces, file structure, and file origins to determine whether the content is an original recording or the result of deepfake manipulation. Data validation must also be carried out through cross-checking between technical analysis results, expert testimony, witnesses and supporting documents so that the judge has a sufficient basis to assess the authenticity of the electronic evidence.³⁷

The lack of regulation in the ITE Law related to the misuse of deepfake technology lies in the absence of clear and precise limits on the misuse of this technology, thus posing a number of challenges for law enforcement. Existing provisions must be interpreted to cover this gap due to the absence of a clear normative definition of deepfakes, which often leads to legal uncertainty and the possibility of conflicting interpretations in court. The increasingly complex advancement of deepfake technology is able to create content that is so similar to the real that it is difficult to distinguish from the real thing, further worsening the situation, as it complicates the process of identifying the perpetrator, verifying evidence, and proving intentionality in court. In addition, advances in increasingly sophisticated deepfake technology pose significant challenges in the detection and proof of violations of the law. Therefore, to protect the public from the negative impact of deepfakes, more comprehensive and specific regulations are needed to control their abuse.³⁸

c. "Law Number 27 of 2022 concerning Personal Data Protection"

As one of the AI-based technologies that is currently developing rapidly, deepfakes cause various legal challenges related to personal data protection.

³⁷ Wahyu Regal Putra, Abdul Hasan, " Kedudukan Bukti Digital dalam Bukti Perkara Perdata di Pengadilan," *Journal of Justice, Law Studies, and Politics (JUSTITIA)* 1, no.3 (2025): 81-89.

³⁸ Rafi Satria Arvito, " Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP," *Jurnal Ilmiah Hukum dan Hak Asasi Manusia (JIHAM)* 4, no.2 (2025): 73-82.

Within the framework of the PDP Law, the misuse of deepfake technology can violate an individual's rights to their personal data, such as using their voice or face without permission. Creating ad manipulation content using deepfakes can cause serious impacts on the reputation and privacy of the individual. Therefore, an in-depth study is very important to evaluate the effectiveness of the PDP Law in protecting individual privacy against deepfake abuse and optimizing applicable regulations to protect one's rights in today's digital era. As technology advances, the demand for data and information increases. Raising public awareness about the exploitation of deepfake technology as a form of manipulation, particularly among law enforcement officers, is the first step in protecting victims of personal data misuse using this technology.³⁹

The PDP Law plays a very important role in protecting a person's personal data in Indonesia, especially in the increasingly advanced digital era. Although the PDP Law does not specifically regulate deepfake technology, the provisions in the PDP Law can be used in dealing with the misuse of a person's personal data to create content based on deepfake technology. This law provides a legal basis in providing protection for the personal data of each individual from the misuse of deepfake technology. Articles 4 to 15 of the PDP Law regulate the right of every individual to obtain the protection of personal data used by other parties, meaning that personal data taken by others for any purpose, including the creation of deepfake technology-based advertising manipulation content must obtain consent from the data subject.

In this case, a person's right to ownership of their personal data is violated by a deepfake that alters a person's voice or image without the person's explicit consent. Deepfake technology by using photos, voices, and personal information without the knowledge or consent of the data subject, so that it can violate Article 20 paragraph (2) letter a of the PDP Law. which

³⁹ *Ibid*, p.78.

stipulates that "The Personal Data Controller is obliged to have the basis for the processing of personal data including the explicit valid consent of the Personal Data Subject for 1 (one) or several specific purposes that have been conveyed by the Personal Data Controller to the Personal Data Subject"⁴⁰

Referring to the case of Melaney Ricardo who occurred in 2024 became a victim of the abuse of deepfake technology in a slimming drug advertisement that was widely circulated on TikTok and other social media platforms, where her face and voice were realistically manipulated to give false testimonials about losing up to 25 kg in a month. Melaney firmly clarified through her personal TikTok account that she was never involved, did not receive payment, never saw or consumed the product, and was never contacted by the manufacturer. This content even caused some of Melaney's friends such as Andre Taulany, Titi DJ and her family to be deceived. This was acknowledged directly by Melaney when she was a guest star on the Brownis show on TRANS TV. This case highlights how deepfakes create misleading information so that it can affect consumers and weight fighters so that it is easy to be tempted by claims of instant diets that can harm consumers economically and health.

The clarification made by Melaney on her personal social media account, proves that her image and voice have been misused by irresponsible business actors without asking for Melaney's consent in using her personal data. So in this case, it is clear that it has violated the provisions of Article 20 Paragraph (2) letter a of the PDP Law where the personal data controller must first ask for consent from the personal data subject in processing personal data. Violation of this article in the case of Melaney Ricardo can be regulated in Article 68 of the PDP Law which states that "Every Person who deliberately makes false Personal Data or falsifies Personal Data with the intention of benefiting himself or others who may cause harm to others as referred to in Article 66 shall be sentenced to

⁴⁰ Article 20 Paragraph (2) letter a of Law Number 27 of 2022 concerning Personal Data Protection.

imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp.6,000,000,000, 00 (six billion rupiah)".⁴¹

There is still room for improvement even though the PDP Law offers a strong normative foundation to protect personal data in the era of technological advancements such as deepfakes. For example, there is no regulation that specifically regulates the misuse of deepfake technology in the PDP Law. Therefore, revisions or additions to specific articles are needed to regulate the misuse of personal data using deepfake technology, by clarifying legal responsibilities and sanctions for business actors who violate. The provisions in the PDP Law can be used to protect the public from the misuse of personal information in the creation of deepfake-based material, although the law does not specifically regulate deepfakes.

d. "Regulation of the Minister of Communication and Information Technology Number 10 of 2021 concerning Amendments to the Regulation of the Minister of Communication and Information Technology Number 5 of 2020 concerning Private Scope Electronic System Operators (Permenkominfo-PSE)"

The final and final protection that can be given to victims from the misuse of deepfake technology in advertising on social media is to provide repressive protection, so that the perpetrator gets sanctions for the losses obtained by the victim from these actions. The imposition of punishments, including fines and imprisonment, is an example of repressive legal protection. For example, repressive legal protection against the misuse of deepfake technology in creating advertising content on social media uses a *take down* mechanism or termination of access to infringing content.

If there is a case where there are business actors who abuse deepfake technology for personal interests in creating advertising content and hide

⁴¹ Article 68 of Law Number 27 of 2022 concerning Personal Data Protection.

behind anonymous accounts or servers that are outside the jurisdiction of Indonesian law, then the main responsibility remains attached to the creator or controller of the content as the party who commits the legal act. If the social media platform knows or should be aware of the existence of *deepfake* content that violates the law and does not immediately remove or terminate access, then the social media platform can also be held accountable because it has the obligation to control content and *takedown* the prohibited content. Thus, the construction of liability is multi-layered, namely the creator of the advertising content as the main actor and the controller of the social media platform as the party who is also administratively or civilly responsible if they are negligent in carrying out the obligation to take *down*, especially if the anonymous business actor is on an overseas server so that it is difficult to reach.

Referring to Article 1 number 15 of the Permenkominfo-PSE, access restriction is defined as an act that aims to block access, close accounts and/or delete content (*take down*). Actions regarding access termination have been regulated in Article 13 paragraph (1) of the Permenkominfo-PSE that "Private Scope PSE is obliged to take *down* Electronic Information and/or Electronic Documents that are prohibited as referred to in Article 9 paragraph (4)."⁴² Permenkominfo-PSE Article 9 paragraph (4) refers to the rules for prohibited electronic documents and/or information. The "right to be forgotten" is another type of legal protection that states and governments can offer in addition to the removal or termination of access.⁴³

⁴² Article 13 paragraph (1) of the Regulation of the Minister of Communication and Information Number 10 of 2021 concerning Amendments to the Regulation of the Minister of Communication and Information Number 5 of 2020 concerning Private Scope Electronic System Operators.

⁴³ Khansa Farinda Khalishah, Laely Wulandari, Ruli Ardiansyah, " Perlindungan Hukum Terhadap Perempuan Korban Balas Dendam Pornografi Dengan Menggunakan Aplikasi "Deepfake" Sebagai Kekerasan Berbasis Gender Online," *Jurnal Parhesia* 2, no.2 (2024): 1-14.

e. "Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP-PSTE)"

This right to be forgotten is further explained in more detail in PP-PSTE, as stipulated in Article 15 paragraph (1) that "Every Electronic System Operator is obliged to delete irrelevant Electronic Information and/or Electronic Documents under its control at the request of the person concerned."⁴⁴ This can be seen as an obligation to delete inappropriate data or electronic documents that are under its control at the request of the party concerned. Furthermore, regarding the removal from the search engine list, as stipulated in Article 15 paragraph (2) that "The obligation to delete Electronic Information and/or Electronic Documents that are irrelevant as intended in paragraph (1) consists of: deletion (*right to erasure*); and expenses from search engine listings (*right to delisting*)." According to the court ruling, the PSE, which oversees search engines, has the authority to remove and restrict access to electronic data and documents that are deemed redundant.⁴⁵

2. Legal Protection for Consumers Against Deepfake Abuse in Social Media Advertising

Along with the many cases of misuse of deepfake technology, various risks and potential abuses have emerged that can harm consumers and the wider community. One of the most crucial problems is the use of deepfakes in creating advertising content on social media that does not reflect reality, thus potentially misleading consumers such as manipulating images or celebrity voices without permission to increase product sales.

⁴⁴ Article 15 paragraph (1) of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

⁴⁵ Khansa Farinda Khalishah, Laely Wulandari, Ruli Ardiansyah, Op.cit, p.7.

Deepfake technology allows the creation of hyper-realistic fake digital content, including video, images, or audio, that can be leveraged for a variety of purposes, including product or service promotion. The use of deepfakes in the context of these promotions carries substantial risks that need to be seriously considered. First, deepfakes have the potential to cause confusion and a collapse of trust by consumers, because promotional content that appears authentic but turns out to be manipulative content can also damage the perception of brands and products, thus negatively impacting the company's reputation and image. Second, this technology can be used to spread misleading information or hoaxes, where deepfake promotional content is used to deceive consumers, form false perceptions, or even commit fraudulent practices, which not only harm consumers materially but also trigger legal consequences for business actors. Third, the application of deepfakes in promotion raises ethical and legal dilemmas, because the manipulation of an individual's identity or appearance without consent is a violation of the facial ownership rights and privacy of the subject being exploited.

Legal protection for consumers is an urgent need, considering the current phenomenon, the position of consumers is still considered very weak compared to business people. As a result, many consumers experience losses when buying and selling goods and/or services, either through conventional media or through electronic commerce platforms such as social media or e-commerce. Protection can be found within the legal framework of consumer protection, which is universal and reflects the common interests of all legal subjects.⁴⁶ This legal arrangement aims to address the consequences of conflicts between business actors and consumers, while ensuring legal certainty to provide comprehensive protection for consumers.

⁴⁶ Ubaidillah Kamal, "Konstruksi Perlindungan Konsumen Jasa Pengobatan Alternatif (Studi Kasus Di Kota Semarang)," *Journal of Private And Commercial Law* 1, no. 1 (2017): 69-84.

Legal protection, according to Philipus M. Hadjon, is "an effort to maintain human dignity and dignity through the recognition and respect of the human rights inherent in every subject of law based on the provisions of laws and regulations, in order to prevent arbitrary actions." Thus, legal protection can be understood as a set of norms or rules that function to protect certain interests from potential violations or unfair treatment.⁴⁷ Preventive and repressive measures are one type of legal protection available to consumers.⁴⁸

According to Philipus M. Hadjon, "legal protection is divided into 2, namely preventive legal protection and repressive legal protection". The purpose of preventive legal protection is to avoid conflicts or disputes and motivate the government to be careful when making decisions based on discretion. Meanwhile, repressive legal protection seeks to resolve disputes resolved by public or out-of-court courts.⁴⁹

Therefore, legal protection for consumers is very important against the misuse of deepfake technology that violates the law. These legal protections can be categorized into:

a. Preventive Legal Protection

According to Philipus M. Hadjon, "preventive legal protection is a form of legal protection where the public is given the opportunity to submit objections or opinions before a government decision takes an administrative form."⁵⁰ Preventive legal protection is an important legal tool to anticipate various problems that arise in social media-based e-commerce. The purpose of this type of preventive protection is to

⁴⁷ Edy Purwito, "Konsep Perlindungan Hukum Konsumen Dan Tanggung Jawab Hukum Pelaku Usaha Terhadap Produk Gula Pasir Kadaluarsa Di Kota Surabaya," *Jurnal Magister Ilmu Hukum 'DEKRIT'* 13, no.1 (2023): 110-129.

⁴⁸ Tiara Azzahra, Ubaidillah Kamal, "Perlindungan Konsumen Pengguna Smartphone Oppo Dan Realme Atas Pemasangan Aplikasi Pinjaman Online Tanpa Izin," *Jurnal Panorama Hukum* 10, no.1 (2025): 113-130.

⁴⁹ Satjipto Rahardjo, *Ilmu Hukum* (Bandung: PT. Citra Aditya Bakti, 2006) p.54.

⁵⁰ Evita Lanosta, Tri Anggraini, *Op.cit.*, p.553.

prevent consumer losses before they occur, which can be realized through:

1. Coaching for consumers.

Based on Article 29 paragraph (1) of the UUPK, namely: "The government is responsible for fostering the implementation of consumer protection which ensures the acquisition of the rights of consumers and business actors as well as the implementation of the obligations of consumers and business actors."⁵¹ Coaching to consumers is important to implement considering the low level of consumer awareness of their rights and the weak position of consumers when juxtaposed with business actors. Therefore, the government collaborates with LPKSM or the "Non-Governmental Consumer Protection Institute" to empower consumers through systematic coaching and education programs for consumers.⁵²

2. Supervision of consumers.

This is regulated in Article 30 paragraph (1) of the UUPK, namely: "Supervision of the implementation of consumer protection and the implementation of the provisions of its laws and regulations are carried out by the government, the community, and non-governmental consumer protection institutions." Supervision in the implementation of consumer protection and law enforcement is carried out synergistically by the community, the government, and LPKSM, where each party has the same commitment to realize the fulfillment of consumer protection.⁵³ If the results of the supervision indicate that there are irregularities that cause losses to consumers, then the perpetrators of violations can be sanctioned in accordance with the provisions of the applicable laws and regulations.

⁵¹ Article 29 paragraph (1) of Law Number 8 of 1999 concerning Consumer Protection.

⁵² Evita Lanosta, Tri Anggraini, *Op.cit*, p.553.

⁵³ Esther Masri, Oti Handayani, Rama Dhianty, Sri Wahyuni, *Buku Ajar Hukum Perlindungan Konsumen* (Surabaya: CV. Jakad Media Publishing, 2023)

b. Protection of repressive laws

According to Philipus M. Hadjon, "repressive legal protection is a form of legal protection which is more directed in the form of dispute resolution."⁵⁴ Dispute resolution is regulated in UUPK Article 45 paragraph (2), namely "the settlement of consumer disputes can be pursued through the court or out of court based on the voluntary choice of the parties to the dispute."⁵⁵ So that repressive legal protection efforts in the manipulation of deepfake-based advertising content can be pursued through litigation (court) and non-litigation (out of court).

1. Dispute resolution through the judiciary (litigation).

Based on Article 48 of the UUPK, it states that "Consumer dispute resolution through the courts refers to the provisions on the applicable general judiciary by paying attention to the provisions in Article 45."⁵⁶ Thus, this article stipulates that "dispute resolution through a lawsuit to the court can only be submitted if both parties to the dispute have not taken an out-of-court settlement attempt, and the attempt is declared to have failed by one or both parties to the dispute" as stipulated in Article 45 paragraph (4) of the UUPK.⁵⁷

Based on this, consumers who suffer material or immaterial losses as a result of the misuse of deepfake technology can file a lawsuit against business actors who create advertising manipulation content on social media through the general court in the jurisdiction where the plaintiff lives. The form of filing a lawsuit to the general court is divided into several groups, including: a) Small Claim Court, a type of court to resolve small disputes, b) Class Action, a type of lawsuit by a group of people with the same claim, c) Legal Standing, the right of individuals or consumer groups to file a lawsuit against

⁵⁴ Evita Lanosta, Tri Anggraini, *Op.cit*, p.554.

⁵⁵ Article 45 paragraph (2) of Law Number 8 of 1999 concerning Consumer Protection.

⁵⁶ Article 48 of Law Number 8 of 1999 concerning Consumer Protection.

⁵⁷ Article 45 paragraph (4) of Law Number 8 of 1999 concerning Consumer Protection.

business actors who abuse deepfake technology in creating advertising content on social media.⁵⁸

2. Out-of-court dispute resolution.

a) Peaceful dispute resolution.

Based on Article 45 paragraph (2) which states that, it is possible to resolve disputes peacefully based on mutual agreement between consumers and business actors peacefully based on mutual agreement. So in this mechanism, before the parties decide to use BPSK to resolve disputes, peaceful dispute resolution must be a top priority in this mechanism.⁵⁹

b) Dispute resolution through BPSK.

The UUPK provides an alternative mechanism for consumers who suffer losses through other means to sue business actors through the Consumer Dispute Resolution Institution (BPSK) in addition to the general court. Class actions are filed through the ordinary courts, while dispute filings through BPSK are limited to individual litigation and are based on the voluntary agreement and consent of the disputing parties. To speed up, simplify, and lower the cost of the case process, BPSK, a special court for consumer disputes (small claims court), is expected to resolve conflicts between consumers and corporate actors.

In addition to the general courts, the UUPK provides an alternative mechanism for consumers who have suffered losses to file a lawsuit against business actors through BPSK or the "Consumer Dispute Resolution Agency". Class action lawsuits are filed through the ordinary courts, but the filing of disputes through BPSK is limited to individual litigation and is based on the voluntary agreement and consent of the parties to the dispute. BPSK is a

⁵⁸ Esther Masri, Oti Handayani, Rama Dhianty, Sri Wahyuni, *Op.cit*, p. 222.

⁵⁹ Evita Lanosta, Tri Anggraini, *Op.cit*, p.556.

"*small claim court*" specifically designed to resolve consumer disputes between businesses and consumers, allowing case processes to run quickly, easily, and affordably.

It took place quickly because Article 55 of the UUPK has stipulated that "within a period of 21 working days, BPSK is obliged to give its decision. It is easy because of the simple administrative procedures and decision-making procedures". Cheap because of the affordable case costs as stipulated in Articles 49 to 56.⁶⁰ This BPSK mechanism provides a sense of security for consumers with a clear resolution path, so that consumers can file complaints related to losses due to deepfake advertising content to get a quick and fair settlement through mediation or deliberation between consumers and business actors.

Until now, the existing positive law in Indonesia has not specifically regulated the misuse of deepfake technology. In fact, if you look at the rapid development of AI that can threaten the rule of law, this is the urgency to immediately take preventive steps in updating regulations related to the misuse of deepfake technology.

Conclusion

The UUPK guarantees consumers' rights to comfort, security, and accurate, clear, and honest information based on Article 4 letters a and c, the obligations of business actors Article 7 letter b, the prohibition of the dissemination of advertisements Article 17 paragraph 1 letter a, and administrative sanctions of up to two hundred million rupiah or criminal sanctions Articles 60 to 63. However, legal regulations regarding the use of deepfakes in advertising in Indonesia are still general and not yet explicit.

⁶⁰ *Ibid*, p.556.

Article 1 paragraph 8 of the ITE Law classifies deepfakes as electronic agents. Companies that use deepfake technology to produce advertising content violate Article 35, which can be subject to a fine of twelve billion rupiah or a maximum prison sentence of twelve years. Sanctions for the dissemination of false information also apply to Article 12 and Article 28 paragraph 1. While the Permenkominfo-PSE and PP-PSTE offer repressive tools such as content removal in Article 13 and the right to be forgotten in Article 15, the PDP Law protects personal data such as faces and voices through explicit consent in Article 20 paragraph 2 with criminal sanctions in Article 68. The cases of Najwa Shihab, Doctor Terawan, and Melaney Ricardo highlight the dangers of fraud, health economic losses, and privacy violations, so that in order to achieve legal certainty and effective consumer protection, specific regulations must be created to address law enforcement weaknesses, difficulties of proof, and adaptation to advances in artificial intelligence.

According to Philipus M. Hadjon, preventive and repressive strategies offer consumers complete legal protection against the misuse of deepfakes in social media advertising. To prevent material and immaterial losses, preventive measures include consumer guidance under Article 29 of the Consumer Protection Law and supervision of cooperation by the public, government, and non-governmental consumer protection organizations (NGOs), as outlined in Article 30 of the Consumer Protection Law. Repressive mechanisms include settlement through peaceful channels or through Consumer Dispute Resolution Institutions, which are fast, easy, and affordable in accordance with Articles 45 to 56 of the Consumer Protection Law, as well as settlement through litigation in the general court under Article 48 of the Consumer Protection Law with the option of small claims courts, class action lawsuits, or legal channels after non-litigation channels fail. However, given the lack of specific laws and regulations related to deepfakes, it is very important that positive laws are immediately updated in Indonesia. This is because more adaptive legal measures are

needed to ensure legal certainty and effective protection amid the risk of fraud and loss of consumer trust.

Bibliography

- Abby, Emilia, and Irwansyah. 2021. "Penggunaan Celebrity Endorser Pada Media Sosial Instagram Dalam Meningkatkan Brand Engagement." *Jurnal Ilmiah Wahana Pendidikan* 7 (5): 73–86. <https://jurnal.peneliti.net/index.php/JIWP>.
- Adiawaty, Susi, Albert Budiyanto Kambuno, Suryati Veronika, Salman Habeahan, and Bernard E Silaban. 2022. "Pengaruh Promosi Dan Citra Merek Terhadap Keputusan Pembelian Pada Aplikasi Market Place." *JUDICIOUS* 3 (2): 370–73. <https://doi.org/10.37010/jdc.v3i2.1298>.
- Amelia, Yolanda Frisky, and Hisbul Luthfi Ashsyarofi. 2024. "Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia." *Dinamika Jurnal Ilmiah Hukum* 30 (1): 9675–91.
- Amra, Elma. 2026. "Best Deepfake Marketing Statistics 2025." Amra & Elma. 2026. <https://www.amraandelma.com/deepfake-marketing-statistics/>.
- Arvitto, Rafi Satria. 2025. "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP." *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia* 4 (2): 73–82. <https://doi.org/10.35912/jihham.v4i2.3937>.
- Azzahra, Tiara, and Ubaidillah Kamal. 2025. "Perlindungan Konsumen Pengguna Smartphone Oppo Dan Realme Atas Pemasangan Aplikasi Pinjaman Online Tanpa Izin." *Jurnal Panorama Hukum* 10 (1): 113–30. <https://doi.org/10.21067>.
- Christella Seveney, Madalaine, Demas Brian Wicaksono, and Irwan Kurniawan Soetijono. 2025. "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi." *Disiplin : Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda* 31 (2): 97–106.
- Elang Rinjani Utara, and Anis Widyawati. 2025. "Analysis of Criminal Law Enforcement on Non-Consensual Deepfake Pornography in the

- Dissemination of Manipulative Content in Indonesia.” *Al-Jinayah: Jurnal Hukum Pidana Islam* 11 (1): 125–53. <https://doi.org/10.15642/aj.2025.11.1.125-153>.
- Farinda Khalishah, Khansa, Laely Wulandari, and Ruli Ardiansyah. 2024. “Perlindungan Hukum Terhadap Perempuan Korban Balas Dendam Pornografi Dengan Mempergunakan Aplikasi ‘Deepfake’ Sebagai Kekerasan Berbasis Gender Online.” *Jurnal Parhesia* 2 (2): 1–14.
- Gabe Regan. 2025. “The State of Deepfake Regulations: What Businesses Need to Know.” *Reality Defender*. June 18, 2025.
- Gici Oktavianti, Rindang, Abdurrahman Muqsith, and Isma Nadia. 2025. “Penyalahgunaan Deepfake Era Canggihnya Teknologi Memicu Kejahatan Media.” *Jurnal Ilmiah Fakultas Hukum IUS* 13 (01): 114–22. <https://jak101fm.com/2023/10/mengenal->.
- Gunardi. 2022. *Buku Ajar Metode Penelitian Hukum*. Jakarta: Damera Press.
- Gunawan, Indra Jaya, and Sylvia Janisriwati. 2023. “Legal Analysis on the Use of Deepfake Technology: Threats to Indonesian Banking Institutions.” *Law and Justice* 8 (2): 192–210. <https://doi.org/10.23917/laj.v8i2.2513>.
- Haq, Zaenul. 2025. “Perlindungan Konsumen Terhadap Ancaman Deepfake Dalam Transaksi Digital: Tinjauan Regulasi Dan Urgensi Mitigasi.” *Journal of Authentic Research* 4 (2): 2656–69. <https://doi.org/10.36312/m4xwcw14>.
- Hasibuan, Ali Huristak Hartawan, David Novan Setyawan, and Yanuriansyah Ar Rasyid. 2025. “Legal Protection For Consumers Against The Potential Harm Caused By Promotions Using Deepfakes.” *JlHK* 6 (2): 116–26. <https://doi.org/10.46924/jlHK.v6i2.232>.
- Kamal, Ubaidillah. 2017. “Konstruksi Perlindungan Konsumen Jasa Pengobatan Alternatif (Studi Kasus Di Kota Semarang).” *Journal Of Private And Commercial Law* 1 (1): 69–84. www.depkes.go.id/seberapa-besar-manfaat-.
- Keepnetlabs. 2025. “Deepfake Statistics & Trends 2025: Growth, Risks, and Future Insights.” *Keepnetlabs*. 2025. <https://keepnetlabs.com/blog/deepfake-statistics-and-trends#financial-fraud>.
- Kristian, Willy. 2025. “Deepfake Dan AI Dalam Dunia Periklanan: Ancaman Atau Peluang?” *Binus University*. 2025.

<https://binus.ac.id/bekasi/2025/01/deepfake-dan-ai-dalam-dunia-periklanan-ancaman-atau-peluang/>.

Lanosta, Evita. 2021. "Perlindungan Konsumen Atas Informasi Yang Benar Terhadap Promosi Produk Dalam Transaksi Perdagangan Elektronik Menurut Undang–Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen." *Jurnal Hukum Adigama* 4 (1): 534–59.

Liu, Min, and Xijin Zhang. 2023. "Deepfake Technology and Current Legal Status of It." In , 1308–14. https://doi.org/10.2991/978-94-6463-040-4_194.

Manulang, Beth Anastasia Nakita, Isna Khalimatussa'diah Azzahra, Salsa Alfi Widowati, Ghaida Raisya Asy-Syifa, and Ubaidillah Kamal. 2025. "Rekonstruksi Keadilan Substantif Di Era Digital Melalui Legal Gap Menanggapi Fenomena No Viral No Justice Di." *Jurnal Ilmiah Wahana Pendidikan* 11 (12.B): 300–310. <https://doi.org/https://jurnal.peneliti.net/index.php/JIWP/article/view/12206>.

Masri, Esther, Oti Handayani, Rama Dhianty, and Sri Wahyuni. 2023. *Buku Ajar Hukum Perlindungan Konsumen*. Surabaya: Jakad Media Publishing.

Miru, Ahmadi., and Sutarman. Yodo. 2004. *Hukum Perlindungan Konsumen*. Jakarta: Raja Grafindo Persada.

Moleong, Lexy J.. 1989. *Metodologi Penelitian Kualitatif*. PT Remaja Rosdakarya.

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

Purwito, Edy. 2023a. "Konsep Perlindungan Hukum Konsumen Dan Tanggung Jawab Hukum Pelaku Usaha Terhadap Produk Gula Pasir Kadaluarsa Di Kota Surabaya." *Jurnal Magister Ilmu Hukum* 13 (1): 109–29. <https://doi.org/10.56943/dekrit.v13n1.152>.

Rahardjo, Satjipto. 2006. *Ilmu Hukum*. Bandung: Citra Aditya Bakti.

Robandi, I. 2021. *Artificial Intelligence: Mengupas Rekayasa Kecerdasan Tiruan*. Andi Offset. <https://books.google.co.id/books?id=O28SEAAAQBAJ>.

Rochani, Oleh :, Urip Salami, I Ketut, Karmi Nurjaya, and Dan Krisnhoe Kartika. 2008. "Penerapan Pasal 4 Undang-Undang No.8 Tahun 1999 Tentang Perlindungan Konsumen Pada Jasa Pengiriman Dokumen Di

- Pt. Kerta Gaya Pusaka Perwakilan Purwokerto.” *Jurnal Dinamika Hukum* 8 (2): 146–53.
- Shevila Kristiyenda, Yoan, Jasmine Faradila, and Christina Basanova. 2025. “Pencegahan Kejahatan Deepfake: Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang.” *ALADALAH : Jurnal Politik, Sosial, Hukum Dan Humaniora* 3 (2): 149–64. <https://doi.org/10.59246/aladalah.v2i4>.
- Stivens Situmeang, Bramcov, Inggrid Yolanda Silitonga, Reskina Felida Silaen, Tiurmaida Siringo-ringo, and Ester Esari Sipayung. 2024. “Pengaruh Artificial Intelligence Terhadap Tingkat Kasus Deep Fake Pada Selebritas Di Twitter.” *JURNAL DEVICE* 14 (1): 80–91.
- Syahirah, Sabrina Nur, Bayu Prasetyo, Universitas Muhammadiyah, and Kalimantan Timur. 2025. “Tinjauan Yuridis Terhadap Penggunaan Teknologi Deepfake Untuk Pornografi Melalui Artificial Intelligence (Ai) Di Indonesia.” *Jurnal Inovasi Hukum Dan Kebijakan* 6 (1): 191–212. <https://ejournals.com/ojs/index.php/jihk>.
- Widiarty, Wiwik Sri. 2024. *Buku Ajar: Metode Penelitian Hukum*. Yogyakarta: Wiwik Sri Widiarty.
- Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2021 Tentang Perubahan Atas Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat.
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.