The Existence of Deepfake Artificial Intelligence As a Means Of Crime In The Perspective Of Indonesia's Positive Law

Gede Sariasa[1], Ni Luh Made Madhusodani[2], Dewa Ayu Diah Ambarawati A.P[3]
Ni Putu Ega Parwati[4]

sariasa@undiksha.ac.id[1], madhusodani@undiksha.ac.id[2], ayu.diah.ambarawati@undiksha.ac.id[3], ni.putu.ega.parwati@undiksha.ac.id[4]

Universitas Pendidikan Ganesha, Indonesia[1,2,3,4]

Abstract. Indonesia and the world have entered the era of Social Revolution 5.0, where humans and machines are expected to work together to address various challenges arising from the Industrial Revolution 4.0. Artificial intelligence (AI), especially deepfake technology, is one of the biggest innovations of our day. Careless people have used deepfake technology to conduct a number of offenses, including fraud, defamation, and attacks of privacy. Deepfake technology is capable of manipulating videos and audio to create content that appears real, posing a threat to personal data security and public trust. This research use a normative legal research method to examine the legal vacuum concerning deepfake technology in Indonesia's positive law system. The findings reveal that there are currently no specific legal regulations that address the protection against the misuse of deepfake technology, either in civil or criminal law. This regulatory gap creates opportunities for widespread abuse of deepfake technology, potentially harming individuals and society at large. To prevent the widespread negative use of deepfake technology, there is a need for the formulation of legal substance synchronization (ius constituendum) that specifically governs deepfake in Indonesia's legal system. The necessary efforts include drafting more specific regulations related to this technology, enhancing the capacity of law enforcement to deal with deepfake-related crimes, and raising public awareness about the dangers and negative impacts of the technology. Additionally, it is crucial to strengthen internal management in the legal structure and legal culture, as well as provide support for digital facilities that can prevent the misuse of deepfake AI. With comprehensive regulation and appropriate preventive measures, Indonesia is expected to more effectively anticipate the development of deepfake technology and protect its citizens from the potential crimes it may cause.

Keywords: Deepfake Artificial Intellegence, Cybercrime, Ius Constituendum

1 Introduction

Indonesia and the world have now entered the era of the social revolution 5.0 and have gone through 4 industrial revolutions. In the era of society 5.0, society is expected to be able to solve problems that arise in the 4.0 era by making humans and machines coexist with each other [1]. The existence of technology and information that has developed very rapidly provides a new interaction space for humans where this interaction space is very easy for humans to interact with each other because there are no restrictions on interaction. The internet as a computer network system is a medium that supports the ease of interaction without space and time limits.

ICLSSE 2024, October 17, Singaraja, Indonesia

DOI 10.4108/eai.17-10-2024.2353690

Interaction can be done anywhere because of technological developments that are able to provide convenience in interacting anywhere and anytime. The era of digitalization has a positive and negative impact on the process of constitutional life, the nation and the state and of course the future policy direction (ius constituendum). The development of a precise and methodical population data collection process by the government for the community is one of the benefits of the digital age. This process ensures that the public service process is conducted in a responsible and transparent manner. Judging from its negative impact, the digital era provides opportunities for the threat of cybercrime by targeting victims individually, groups or the security of a country through cyberspace.

One of the things that makes human work patterns change to an all-automatic and digital pattern is the existence of artificial intelligence or commonly known as Artificial Intelligence (hereinafter referred to as AI). Poole and Mackworth define AI as a field that combines and analyzes a computing agent that runs intelligently[2] . Meanwhile, Andreas Kaplan and Michael Haenline [3] define AI as the ability of a system to interpret an external data which is then studied, then based on the learning from the data is used to carry out tasks to achieve certain goals with flexible adaptation patterns. Additionally, the science and engineering of creating intelligent robots is what John McCarthy [4] regarded as the father of artificial intelligence, characterized as AI. Minsky [5] provided another definition of artificial intelligence, defining it as the scientific study of how to make computers perform tasks that people can.

The existence of AI in technological development is certainly inseparable from a legal regulation that applies in a country. Naturally, a number of legal issues pertaining to the activities and/or deeds AI performs can arise from the technological advancements that allow it to perform human tasks. Artificial intelligence that is limited by the programming that drives its operations is known as AI. Since AI is judged in this instance by its capacity to carry out actions and deeds, it is not an exception to the rule that it can carry out legal actions just like a person, such as committing a crime that causes harm to other people. One of the problems caused by AI based on data from the Ministry of Communication and Information Technology occurs in women. It was revealed that women are often the target of the abuse of artificial intelligence technology or Artificial Intelligence (AI) in the form of pornographic-themed deepfakes. Nezar Patria, Deputy Minister of Communication and Informatics, said there are three impacts and victimizations that may occur as a result of AI misuse. One of them is the targeting of women's groups. "Women are the target of pornography content that is deliberately created through deepfake technology [6].

One example of a case that occurred recently is the spread of a hoax video similar to celebrity Syahrini. A syur video similar to Syahrini has gone viral on social media since May 12, 2020. The culprit, a woman with the initials MS, was apprehended by the police in Kediri, East Java. MS spread a hoax of Syahrini's syur video on her Instagram account. The police revealed the background of the pornographic video that profited from Syahrini's name. Every day, women with the initials MS have the status of housewives. But in his daily life, MS does spend more time playing social media. Another reason for the video's spread is because MS is a fan of other celebrities. MS was involved in legal trouble after being caught spreading pornographic videos by profiteering Syahrini's name[7].

In addition to the case involving several names of Indonesia celebrities, well-known figures such as the Chairman of PDIP, Megawati Soekarnoputri have also been victims related to the misuse of deepfake applications. On Facebook, Welly (Chairman of FPI Galang District, North Sumatra) posted a fake image of PDIP Chairman Megawati Soekarnoputri holding President Joko Widodo. Welly was proven to have posted a photo of Megawati Soekarnoputri holding President Joko Widodo through her Facebook social media account. Welly must face the investigation process at the Directorate of Special Criminal Investigation (Ditreskrimsus) of the North Sumatra Police and has been designated as a suspect[8] .

In addition, the threat of using deepfakes has been proven through various phenomena in recent years. For instance, a video of President Joe Biden performing the children's song "Baby Shark" as the national anthem at one of his public speeches toward the end of 2022 startled the American audience [9]. It was later discovered that a UK citizen had used deepfake technology to modify the video. Another example of causing financial losses occurred in 2019, where a CEO of a subsidiary in the United Kingdom transferred a sum of $243,000 at the request of someone whose voice sounded very similar to his boss at a Germany parent company[10] . The call turned out to be carried out by criminals who used AI technology to imitate the voice of company executives to commit fraud. In Indonesia, in October 2023, a video showing President Joko Widodo speaking fluently in Mandarin in a state of the nation speech went viral[11] . After investigation, the video was proven to be based on false information. With the increasing awareness and use of deepfakes in Indonesia, it is important to be aware of the potential for their abuse, which without adequate regulation and restrictions, can have significant negative consequences.

The emergence of deepfakes from well-known figures can have a real impact on social conditions in society ranging from hate speech, conflict, disintegration, intolerance that is increasingly accommodated, and even criminal acts. As time goes by and this technology becomes more sophisticated, the spread of hoaxes, fake news, and deepfake-based pornography is increasingly rampant. The ease with which the video is spread through social media threatens the privacy of someone who does not even participate in using it. In addition, in the past time there was a case, namely Indonesia entered the top 10 with the number of ChatGPT accounts stolen by malware over the past year. According to a report by Singaporean cyber intelligence company Group-IB, more than 101,000 Chat GPT user accounts were compromised.The leaked data is then uploaded on the dark site, Details of the leaked data include email accounts, credit card data, cryptocurrency wallet information, and other types of target data. The data was obtained because many ChatGPT users come from the business world.

Deepfake AI is very vulnerable to being used as a medium to commit crimes because of its sophisticated ability to fake visual and voice identities, which are often difficult to distinguish from the original. The use of deepfakes for criminal purposes, such as fraud, defamation, and the spread of hoaxes, has shown significant impact in various countries, including Indonesia. For example, the case of fake videos featuring celebrities or political figures, such as President Joe Biden or Megawati Soekarnoputri, shows how deepfakes can be used to damage reputations and manipulate public opinion. Additionally, deepfakes are often a tool for gender-based crimes, such as the spread of fake pornographic content targeting women.

Some nations that have implemented AI technology in a variety of industries have positioned AI as a legal subject with rights and obligations; however, this is not the case in Indonesia, as positive law in that country does not recognize AI as a legal topic. Naturally, if AI technology in the future does legal acts that go against Indonesia's favorable legal rules, this will become a legal issue. The author claims that it is clear from the background data above that the rapid development of science and technology is always followed or accompanied by the appearance of criminal activities that are more intricate and sophisticated. This is demonstrated by the rapid evolution of their tools and ways of crime (modus operandi). Therefore, more information regarding the Crime of Using Deepfake Artificial Intelligence and the rules that law enforcement officers utilize as countermeasures is required. Based on this, the author is interested in studying more deeply the existence of Deepfake Artificial Intelligence as a means of criminal acts in the perspective of positive law in Indonesia.

2 Method

Marzuki (2017) [12] stated that finding the truth of coherence that is, whether the rule of law and norms in the form of orders or prohibitions are consistent with the principle of law as well as whether an individual's actions (acts) are consistent with legal norms (rather than just legal rules) or legal principles is the goal of legal research On essence, legal research is a scientific endeavor grounded on certain methodologies, systematics, and ideas that seeks to analyze and examine one or more particular legal occurrences. The legal research process requires a research method that will support the results of the research. The research methods used in this legal research are as follows.

2.1 Type of Research

Normative legal research, which is study conducted by analyzing a body of rules and regulations that apply or are utilized in a particular legal issue, is the form of research used in this work. Not only legislation but also data collection with this type of normative research can use other library material [13]. Legal research contributes to preserving the essential elements of legal science as a sui generis normative science by providing juridical arguments in situations involving emptiness, ambiguity, and normative disagreement [14]. This study will investigate the legal void surrounding the existence of deepfake artificial intelligence in Indonesian positive law by examining a number of current legal regulations that have not been able to support the security of people's personal data. As a result, the Indonesian government must work to prevent criminal acts that use deepfake artificial intelligence as a means of committing crimes.

2.2 Types of Approaches

Approach is a perspective in choosing a language that is expected to be able to provide clarity in the description of the substance of a scientific work. In general, the approach in normative legal research consists of a statue approach, a conceptual approach, a historical approach, a case approach[15] . There is a continuity between the type of research and the type of approach, where this type of normative research uses a type of legislative approach (statue approach) and a case approach (case approach). With the guidance of this approach, what is

done is to study, research, and analyze a legal system that applies in a particular case, conceptualized, and also structured regarding the existence of deepfake artificial intelligence in Indonesia's positive law as well as the efforts that must be made by the Indonesian state in preventing criminal acts that utilize Deepfake Artificial Intelligence as ius constituendum.

a. The statute approach is a technique that involves looking at the laws and rules pertaining to the issues (legal difficulties) at hand.In this study, regulations related to the existence of deepfake artificial intelligence in Indonesia's positive law will be examined as well as efforts that must be made by the Indonesian state in preventing criminal acts that utilize Deepfake Artificial Intelligence.
b. The case approach is carried out to build a legal argument from the perspective of concrete cases that occur in the field and usually aims to find the value of truth and solutions to legal events in accordance with the principles of justice[16] . In the research, criminal cases involving the use of Deepfake Artificial Intelligence were used.
c. A conceptual approach is one that begins with the theories and opinions that emerge in legal science. Researchers will discover notions that give rise to legal understandings, legal concepts, and legal principles that are pertinent to the circumstances at hand by examining the opinions of legal science theories. The conceptual study here is used to examine the formulation of articles in several regulations in Indonesia that regulate personal data security or crimes in the cyber world whether they are able to accommodate the existence of Deepfake Artificial Intelligence which is used illegally.

2.3 Source of Legal Materials

The source of legal material is material that can be used for the purpose of analyzing the applicable law. In normative law research, data sources are only obtained from secondary data sources. Secondary data sources are data obtained from literature or literature that is related to the research object [13]. The sources of legal materials obtained, processed, and used to analyze in this study are:

a. Primary legal materials are legal materials that are authoritative and binding on the issues to be studied. In this study, the primary sources of law are from Law Number 1 of 1946 concerning the Criminal Code (KUHP), Law Number 1 of 2023 concerning the Criminal Code (KUHP), Law Number 27 of 2022 concerning Personal Data Protection, and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.
b. Secondary legal material is a legal material that can be interpreted as non-binding legal material, and which will provide an explanation of the primary legal material, which provides the results of research and assessment from an existing legal source in the form of :
    1 Books or reading materials related to the existence of deepfake artificial intelligence in Indonesia's positive law and the efforts that must be made by the Indonesian state in preventing criminal acts that utilize Deepfake Artificial Intelligence as ius constituendum.

2 Expert opinions that have a relationship with the existence of deepfake artificial intelligence in Indonesia's positive law and the efforts that must be made by the Indonesian state in preventing criminal acts that utilize Deepfake Artificial Intelligence as ius constituendum.

c. Tertiary Legal Materials, namely supporting materials used to explain primary legal materials and secondary legal materials. This legal material can be in the form of the Great Dictionary of Indonesian Language (KBBI) and legal dictionaries.

2.4 Legal Materials Collection Techniques

A literature review of legal materials, including primary, secondary, and tertiary legal resources, is the method used to gather legal materials for normative research. [16] Legal materials are gathered via inventory processes, laws and regulations are identified, and legal materials are categorized and organized based on research issues.

As a result, the method of gathering legal materials for this study is literature review. Reading, analyzing, taking notes, and reviewing literature pertaining to the existence of deepfake artificial intelligence in Indonesian positive law as well as the steps the Indonesian government must take to stop criminal acts that use deepfake artificial intelligence as a ius constituendum are the methods used in literature studies.

2.5 Legal Material Analysis Techniques

Legal material analysis techniques include descriptive, comparative, evaluative, and argumentative methods. The process of analyzing legal materials involves gathering the materials, then analyzing them to arrive at the final argument in the form of solutions to research problems. [14]

The legal material analysis technique used in this study is a descriptive technique which is a research method by describing and interpreting objects or phenomena according to what they are obtained from literature research which later the presentation of the research results aims to obtain a comprehensive but still systematic picture, especially regarding facts related to the problems that will be aimed at this research. Following the collection of primary and secondary legal sources, they are reviewed, interpreted, and arguments are then presented. This argument seeks to offer an evaluation that needs to be supported by legal reasoning, whether it be about what is right or wrong or what the law requires in light of the incident that took place. This led to the drawing of conclusions and the conducting of descriptive talks.

3 Result and Discussion

3.1 The Existence of Deedfake Artificial Intelligence in Indonesia's Positive Law

Rapid technological developments throughout time are a hallmark of the globalization phenomenon. This technological advancement, in addition to bringing changes in a positive direction in helping to make human life easier, is intersecting with negative impacts in the form of the emergence of new types of crimes. One of the new types of crimes that is currently still being sought to solve and minimize the possibilities and impacts caused is cyber crime.

Cybercrime is defined as any illegal act that involves the use of computer technology as a tool or media for criminal activity.

Technological advancement innovations in the form of Artificial Intelligence (AI) are one of the new forms of threats in cyber crime. Examples of problems that arise due to the misuse of Artificial Intelligence technology are deepfake pornography and theft of personal data. This deepfake crime is carried out in the form of fake video or audio manipulation, usually found in the form of fake pornographic videos and sometimes difficult to distinguish the authenticity. Deepfake crimes typically affect public personalities, including artists and political figure. In committing this deepfake technology crime, the perpetrator steals the victim's personal data and steals individual personal information. The results of the video that have gone through the deepfake process will be spread by the perpetrator through social media with the aim of defamation, terror to the victim, and exploitation of the victim in the form of wealth.

In addition, there are other losses that must be felt by victims of Deepfake Artificial Intelligence technology crimes which are described as follows:

1) Psychological and Social Harm

   The psychological and social losses resulting from the abuse of Deepfake AI technology include those related to anxiety, depression, and other mental health conditions. Victims will begin to withdraw and isolate themselves from their social life until the most fatal impact is in the form of victims committing suicide which is considered a way out of the problems they face.

2) Economic Losses

   Some victims of deepfake technology abuse cases frequently suffer financial losses, such as losing their sources of income or getting fired from their job because their employer views it as a disgrace and because they are unable to perform their duties because of mental health issues.

3) Mobility Limitations

   Victims of deepfake abuse will feel that their moving space, both online and offline, will feel scary. The victim will assume that he is of low value from other humans because of what he has experienced, so he will begin to lose his freedom and confidence. Then self-censorship will occur to the victim because they feel unsafe in using technology, and decide never to use technology again as they should because they feel that technology is not safe to use and threatens their lives.

Considering the adverse impact caused by Deepfake Artificial Intelligence, other countries have implemented that Artificial Intelligence (AI) is a legal subject so that there are regulations that specifically regulate individual responsibility for using or abusing deepfake technology. However, in Indonesia, artificial intelligence (AI) has not been regarded as a legal topic, hence there hasn't been any comprehensive legislation that addresses AI abuse up to this point. In fact, with the absence of norms that specifically regulate crimes using Deepfake Artificial Intelligence, there are limitations that have an impact on enforcement in the field, with the existence of special regulations governing Deepfake Artificial Intelligence, clear limits are

created on how individuals must responsibly use technology, creating wisdom in society to positively use AI technology so that it can minimize the occurrence of crimes using this AI.

In criminal law, the criminal liability of perpetrators of Deepfake Artificial Intelligence abuse is categorized into complaint offenses based on the form of criminal acts committed. On the other hand, crimes that occur in Indonesia due to the misuse of deepfake technology can be charged with several articles in the Criminal Code (KUHP) and with other laws such as deepfake pornography to public figures on social media is classified as a cyber crime, pornography, harassment, defamation, theft of personal information, and the perpetrator will be subject to the ITE law. This is considered in accordance with the special legal realm (lex specialis) which specifically regulates issues related to electronic transactions. For example, regulations that are often used in cases of Deepfake Artificial Intelligence technology abuse are as follows:

a. Electronic Information and Transaction Law or *Undang-Undang Informasi dan Teknologi* (UU ITE);
    1. Article 27 paragraph (3) regulates the prohibition of distributing, transmitting, or making accessible an electronic information and/or electronic document that has insulting and/or defamatory content.
    2. Article 28 paragraph (1) regulates the prohibition of spreading false and misleading news (hoax) that causes consumer losses in electronic transactions.
    3. Article 29 regulates the prohibition of disseminating electronic information and/or electronic documents that have content that threatens violence or gives fear to consumers.
b. Criminal Code or *Kitab Undang-Undang Hukum Pidana* (KUHP);
    1. Articles 310 and 311 that regulate defamation.
    2. Article 378 regulates fraud.
    3. Article 335 regulates the act of a pleasant act to deceive or threaten to use deepfake.
c. Law No. 44 of 2008 concerning Pornography;
    1. Article 29 regulates the prohibition of creating, disseminating, and/or utilizing pornographic content. If deepfakes are used to create prono content without the consent of the parties in the video, it can be charged with the Pornography Law.
d. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions which is related to sanctions against the misuse of information and electronic technology.

Although there is no grammatical regulation of the act of pornography that collaborates with AI technology. So from this description, it can be concluded that there are no regulations or laws that fully accommodate the complexity and speed of the development of Artificial Intelligence (AI) technology in Indonesia. In criminal law, there are several forms of legal protection that can be received by victims of the crime of misusing Deepfake Artificial Intelligence, namely[17]:

3.2 Preventive and Repressive Legal Protection

The preventive legal protection in question is laws and regulations related to such as the crime of misuse of Deepfake Artificial Intelligence technology such as the ITE Law, as well as

other special laws (lex specialis) connected to the crime of the perpetrator. Then repressive protection in the form of fines, imprisonment, and other forms of sanctions that aim to make the perpetrator get a reward for the losses experienced by the victim. One example of repressive protection against the abuse of Deepfake Artificial Intelligence is take down. Takedown applications can be submitted by the community, ministries or institutions, law enforcement officials, and/or judicial institutions. The application can be submitted through the website, application, non-electronic mail, and/or e-mail. Another repressive legal protection is the "right to be forgotten" adopted from European countries called the term "Right to be Forgotten (RTBF)" which is regulated in Article 26 paragraphs (3) and (4) of the ITE Law.

There is a difference between the "right to be forgotten" and the concept of "Right to be Forgotten" with the fundamental difference lies in the result of fulfilling these rights. The following are other differences between "right to be forgotten" and "Right to be Forgotten":

a. In "Right to be Forgotten" the personal information to be deleted will disappear from the search engine results but can still be found on the original link where the data information is located, so "Right to be Forgotten" is known as a step that can make it difficult for a person to access information on the search engine site about a person who makes an application for RTBF.
b. The concept of "right to be forgotten" has a different procedure by deleting the data so that it is not only deleted from the search engine site results but also done on the original link of the data source.

From these two things, there are also obstacles to using personal data to avoid the threat of deepfake techniques in the future for victims of the crime of misusing Deepfake Artificial Intelligence. Before carrying out the procedure, there are several requirements that must be met in order for the application to be granted, namely:

a. *"Right to be Forgotten" refers to the Court of Justice of the European Union (CJEU) ruling in the Gonzalez case, the public information is inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes*.
b. The "Right to be forgotten" provides a condition that the information must be irrelevant.
    1. Compensation

        Compensation is usually given to victims of crimes of abuse of Deepfake Artificial Intelligence is the provision of convicts' assets as a form of compensation for victims' losses. The victim, his family, or his lawyer can apply for compensation through the Witness and Victim Protection Institution (LPSK) in accordance with an inkracht court ruling. Then, The state budget and victim relief money from charities, society, people, corporate social responsibility, and environmental responsibility, among other legal and non-binding sources, are used to pay the compensation.
    2. Restitution

        Restitution is a form of compensation given to the victim or his family by the perpetrator or a third party. This restitution aims to compensate the victim for the loss of wealth or source of income, the victim's suffering caused by the perpetrator's actions, compensation for medical and psychological expenses from the victim. Restitution can

be filed before the inkracht court decision, and through the public prosecutor when drafting the letter of demand.

3. Handling, Protection, and Rehabilitation for Victims of Sexual Harassment
   a. Right to handle
      Victims of the crime of misusing Deepfake Artificial Intelligence can find out all information and access to documents resulting from case handling, legal services, the right to psychological rehabilitation, the right to medical treatment, and the right to delete sexually contentious content for cases of sexual violence with electronic media.
   b. Protection rights
      Victims of the crime of misusing Deepfake Artificial Intelligence have the right to know information about protection facilities, the right to receive protection against the threat of perpetrators, protection by maintaining the confidentiality of the victim's identity, protection from job loss, education, political access to be able to restore the dignity and dignity of the victim.
   c. Right to recovery or rehabilitation
      Restitution and/or compensation, social reintegration, medical rehabilitation, mental rehabilitation, and social empowerment are all rights of victims of the crime of Deepfake Artificial Intelligence abuse.

Then, proving the crime of misuse of Deepfake Artificial Intelligence technology as one of the parts of the procedure that must be passed in criminal case courts in accordance with the provisions of the criminal procedure law needs to involve the use of technology in detecting and verifying deepfake crimes which must always pay attention to privacy and ethical aspects, so that law enforcers must ensure that in the process of proving there is not a single violation of human rights Human and Individual Privacy [18].

The lack of official and informal educational opportunities that give people a general understanding of artificial intelligence (AI), especially deepfake technology, so they can use it responsibly to make their lives simpler in the future and avoid the problems that come with it, also has an impact on this. Because behind the rapid advancement of technology over time, it needs to be balanced with the wisdom of the individual himself in using the technology to use it effectively. People who have a good understanding of AI technology can minimize the emergence of legal cases related to the misuse of AI in the future [19].

3.3 Efforts to be Done by the State of Indonesia in Preventing Crimes of Deepfake Artificial Intelligence Misuse

One of the many attempts to control the advancement of the times is the creation of artificial intelligence (AI) technology, such as Deepfake AI technology. Prevention of crimes that can be caused by Deepfake Artificial Intelligence can start with the development of comprehensive regulations. The Indonesia government needs to consider the establishment of specific regulations governing the use of artificial intelligence (AI) technology. This regulation must include various basic things related to AI, starting from a clear definition of what Deepfake Artificial Intelligence is, prohibition of its use that can harm or cause criminal acts, as well as

strict sanctions for violators. To address new risks brought about by the advancement of modern technology, the Electronic Information and Transaction Law (ITE Law) must also be revised. International cooperation should also be enhanced given the cross-border nature of many of the crimes of Deepfake Artificial Intelligence. By integrating various preventive measures, Indonesia can build a strong legal and social framework to prevent and deal with crimes involving Deepfake Artificial Intelligence.

Efforts that must be made by the State of Indonesia in preventing crimes that utilize deepfake technology as ius constituendum (a law that is idealized to be applied) covers various aspects, ranging from regulations, increasing the capacity of law enforcement, to public education. The steps that can be taken to deal with deepfake technology as ius constituendum are as follows:

1. Regulatory Development and Enforcement
   Indonesia needs to consider the formation of regulations in the form of laws that specifically regulate the application or use of Deepfake Artificial Intelligence technology. The lack of specific and comprehensive regulations makes it difficult for authorities to effectively crack down on AI abusers and impose appropriate sanctions [20]. This regulation must include definitions, prohibitions, and sanctions for violations. Meanwhile, there is the Electronic Information and Transaction Law (UU ITE) which can be revised or updated to cover technology more broadly, including Deepfake Artificial Intelligence, considering the scope of the ITE Law which currently only focuses on information technology-based crimes only.
2. Increasing the Capacity of Law Enforcement
   Law enforcers such as police and prosecutors need to be trained to deepen their knowledge in the field of deepfake technology and how to detect it. This knowledge is fundamental to identifying and investigating various cases involving Deepfake Artificial Intelligence. In addition, the development and adoption of various technologies capable of detecting and identifying content related to Deepfake Artificial Intelligence should also be considered. This can include software that can detect AI that is capable of analyzing metadata or patterns in video and audio.
3. Public Education and Social Awareness
   Socialization related to awareness of the use of AI can foster public awareness about the dangers and characteristics of Deepfake Artificial Intelligence. Where through this socialization it is hoped that it will be able to educate the public so that they can use AI for positive things. This is important so that the public is more aware of the information they receive and disseminate. In addition, efforts can be made to encourage social media platforms to develop stricter policies and tools to detect and flag various content related to the misuse of Deepfake Artificial Intelligence. People who have a good understanding of AI technology can minimize the emergence of legal cases related to the misuse of AI in the future [19].
4. Research and Development
   To be able to reach and regulate AI, of course, a fundamental deepening related to AI information is needed. To achieve this, the government can fund various research related to

Deepfake Artificial Intelligence and other AI technologies to understand the social and legal impacts caused, as well as find ways to mitigate the risks. For example, the use of digital forensic analysis, machine learning, and artificial intelligence to recognize unusual anomalies in video and audio [18]. This automatic detection technology can be applied on social media platforms and internet service providers to monitor and remove deepfake content before it spreads widely. With this integration, deepfake content can be identified and removed quickly, preventing the massive spread of false information.

4 Conclusion

The use of deepfake AI has caused significant legal problems in Indonesia, such as fraud, defamation, and the spread of hoaxes, so that the leakage and use of personal data in violation of the law is one of the government's biggest responsibilities in today's digital era. The existence of Deepfake Artificial Intelligence as a means of crime has begun to be detected in Indonesia, but the law has not been able to provide civil or criminal protection. To prevent the massive negative use of Deepfake Artificial Intelligence, it is necessary to formulate and collect data on the synchronization of legal substance that specifically regulates Deepfake Artificial Intelligence, internal management at the level of legal structure, socialization and monitoring of legal culture, and support for digital facilities in preventing the misuse of deepfake AI.

References

[1] Hamdan Mustameer, "Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0," *J. Yustika Media Huk. Dan Keadilan*, vol. 25, no. 01, pp. 40–53, 2022, doi: 10.24123/yustika.v25i01.5090.

[2] W.-V. B. Li -Shanghai H, "Wang WW. AI, Governance and Ethics: Global Perspectives 1," blog.google rechnology AI primciples. [Online]. Available: https://www.blog.google/technology/ai/ai-principles/

[3] M. H. Andreas M. Kaplan, "Users of the world, unite! The challenges and opportunities of Social Media," *Sci. Direct*, vol. 53, no. 1, pp. 59–68, 2010, [Online]. Available: https://doi.org/10.1016/j.bushor.2009.09.003

[4] John McCarthy, *Defending AI research : a collection of essays and reviews*, Distribute. CSLI Publication, 1996. [Online]. Available: https://press.uchicago.edu/ucp/books/book/distributed/D/bo3613109.html

[5] James A. Anderson, *Neurocomputing, Volume 1: Foundations of Research*. The MIT Press, 1988. [Online]. Available: https://direct.mit.edu/books/edited-volume/5431/Neurocomputing-Volume-1Foundations-of-Research

[6] Kominfo, "Kikis Ketimpangan Gender, Menteri Budi Arie Dorong Perempuan Memanfaatkan AI," *kominfo.go.id*, 2024.

[7] M. Flora, "5 Fakta Kasus Video Syur Mirip Syahrini, Motif hingga Pelaku Ditangkap," *liputan6.com*, 2020.

[8] Tim Detik.com, "5 Fakta Geger Ketua FPI di Sumut Unggah Foto Hoax Mega Gendong Jokowi," *www.detik.com*, 2020.

[9] Goldin, "Video of Biden singing 'Baby Shark' is a deepfake," *APnews.com*, 2022.

[10] Stupp, "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case," *WSJ.com*, 2019.

[11] Fransisca Lahur, "Konten Jokowi Pidato "Bahasa Mandarin," *Tekno.Tempo.co*, 2023.

[12] D. & I. I. Marzuki, Utami Widiati, Diyenti Rusdin, "The impact of AI writing tools on the content and organization of students' writing: EFL teachers' perspective," *cogent Educ.*, vol. 10,

no. 2, 2017, [Online]. Available: https://www.tandfonline.com/doi/epdf/10.1080/2331186X.2023.2236469?needAccess=true
[13] Ishaq H, *Metode Penelitian Hukum Dan Penulisan Skripsi, Tesis, Serta Disertasi*. Bandung: Alfabeta, 2017.
[14] Diantha, *Metodologi Penelitian Hukum Normatif Dalam Justilikasi Teori Hukum*. Jakarta: Prenadamedia Grup, 2016.
[15] Ali. Z, *Metode Penelitian Hukum*. Jakarta: Sinar Grafika, 2016.
[16] A. Y. Fajar. Mukti, *Dualisme Penelitian Hukum Normatif dan Empiris*. Yogyakarta: Pustaka Pelajar, 2015.
[17] H. L. A. Yolanda Frisky Amelia, Arfan Kaimuddin, "Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia," *JIM UNISMA*, vol. 30, no. 1, 2024.
[18] N. A. . Respati AA, Dewi Setyarini A, Parlagutan D, Rafli M, Mahendra RS, "No Title," *Media Huk. Indones. Publ. by Yayasan Daarul Huda Krueng Mane*, vol. 2, no. 2, pp. 586–592, 2024, [Online]. Available: https://ojs.daarulhuda.or.id/index.php/MHI/article/view/573/600
[19] W. H. Rizki Kurniarullah M, Nabila T, Khalidy A, Juniarti Tan V, "Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi dan Pencurian Data Pribadi," *J. Ilm. Wahana Pendidik.*, vol. 10, no. 10, pp. 534–547, 2024, [Online]. Available: https://doi.org/10.5281/zenodo.1144881
[20] A. F. D. Raisa Safina, Khalda Alifia Azzahra, "Kajian Yuridis Penggunaan Kecerdasan Artifisial pada Pembuatan dan Penyebaran Konten Pornografi di Media Sosial dalam Hukum Positif Indonesia.," *J. Polit. Sos. Huk. dan Hum.*, vol. 2, no. 2, 2024.

Regulatory sources

Law of Republic Indonesia Number 19 of 2016 concerning Electronic Information and Transactions.
Law of Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions.
Criminal Code (KUHP).
Article 29 of Republic Indonesia Law Number 44 of 2008 concerning Pornography.
Article 14 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 the Implementation of Private Electronic Systems.
Article 14 Paragraph (2) of the 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 Electronic System Organizers.