REGULATING ARTIFICIAL INTELLIGENCE AS A PERPETRATOR OF DEEPFAKE CRIMES IN INDONESIA

Asri Gresmelian Eurike Hailitik[1],, Wiwik Afifah[2],

1Faculty Of Law, University of 17 August 1945, Surabaya

2Faculty Of Law, University of 17 August 1945 Surabaya

Corresponding author: hailitika@gmail.com, wiwikafifah@untag-sby.ac.id

ABSTRACT

Artificial intelligence and Deepfake are the fruits of technological development which can make deepfake a deadly and threatening weapon. The purpose of this study is to determine the regulation of artificial intelligence as a deepfake criminal in Indonesia.The research method used is normative legal research using a statutory approach, conceptual approach, and comparative approach. Artificial Intelligence as a perpetrator based on Indonesian positive law has not been specifically regulated until now only recognized as an object of law not a subject of law. The use of artificial intelligence in deepfake technology is often used to commit crimes such as spreading hoaxes, fraud, defamation, pornography, and manipulation of facts or circumstances. These crimes may violate the provisions of the Criminal Code, Law No.19 of 2016 on Electronic Information and Transactions and Law No.44 of 2008 on Pornography. In California, legislation has been passed to address deepfake crimes but only focuses on preventing nonconsensual sexual activity and relates to the election of candidates for office. Artificial Intelligence is only classified as an electronic system and electronic agent which in its implementation is organized by humans so that if a criminal offense is committed, the electronic system organizer will act as a legal subject to be responsible.

Key words: Artificial Intelligence, Deepfake, Legal Subject

INTRODUCTION

The industrial revolution 4.0 is a convergence of innovation from science and technology that opens opportunities for the world community to revitalize technology and digital transformation. Human beings are always trying to create something that will further their activities. Therefore, the development of technology has created many tools that facilitate human activities and replace human roles in certain functions. Technological developments that continue to evolve have given birth to an innovation called Artificial intelligence or artificial intelligence which is usually called "AI". Technology artificial intelligence It has been used to aid human employment in almost every field such as transportation, education, health, industry, and security [1].

Artificial Intelligence (AI) is one of the inventions that has changed the face of the world. Technology artificial intelligence Allows the machine to have autonomous algorithms that can evolve according to its initiative. Artificial intelligence Able to produce new inputs to carry out tasks like humans, including in processing data and recognizing patterns of data processing in a massive and structured manner [2] . Artificial intelligence will transform big data and the internet of things (IoT) will be the new wisdom to improve people’s ability to live more meaningful lives [3] .

The birth of artificial intelligence technology began in 1941 with the invention of tools for storing and processing information. The invention is an electronic computer developed in America and Germany. Back then computers involved configuring thousands of cables to run a program. In 1949, a computer was successfully created that was able to store programs, making the job of entering programs easier. This discovery became the basis for the development of programs the led to artificial intelligence. Then in 1956, John McCarthy along with Minsky, Claude Shannon and Nathaniel Rochester conducted research in the field of automatic, neural networks and intelligent learning. The result of their research is a program that is able to think non-numerically and solve thinking problems, called Principia Mathematica [4] . McCarthy assumed that every aspect of human intelligence could be precisely defined and simulated by machines. In the first years of development artificial intelligence, successfully created a program called General Problem Solver. This program is designed to initiate humane problem solving. After that, a program called Program with Common Sense. This program is designed to use knowledge in finding solutions. In 1959 the program was developed Geometry Theorm Prover designed to prove a theorem using existing axiomas. Then in 1963, James Slagle created a program capable of solving closed integral problems for calculus. Then in 1968, there was an analogy program made by Tom Evan that was able to solve geometric analogy problems that existed on IQ tests. The period from 1966 to 1974, development artificial intelligence Slowed down. In 1980, artificial intelligence developed very rapidly and became a large-scale industry. Many large companies are investing heavily in the field of artificial intelligence [5].

Realizing the use of artificial intelligence Adopted in various fields of work including medical, educational, and legal services. In 2020, technology artificial intelligence used to make Covid-19 detection tools. Indonesia successfully developed Gadjah Mada Electronic Nose (GeNoSe), a tool that can detect the presence of viruses Covid-19 through human breath and emit accurate results within minutes. In the field of education, the most closely related to artificial intelligence Was machine learning, learning analyticand data meepining. Additionally, in the legal field, artificial intelligence will improve the quality and delivery of legal services. Some countries use artificial intelligence to conduct domestic legal practices. In the UK he has DoNotPay Chat, which currently provides legal aid to over 1,000 people. Saudi Arabia granted citizenship status to the robot Sophia. Japan also granted a residence permit to the Shibuya Mirai robot based on special regulations, In Indonesia, the Online Law website provides an LIA platform (Legal Intelligence Assistant) that help the public to get education about the law [6] .

Like a double-edged sword, artificial intelligence It has the potential to create high-level crimes due to the unpredictable and controllable characteristics of autonomous algorithms. Robert William was the first person to die in a robot accident. William was killed after a robotic arm punched him as he was about to climb up to a shelf to retrieve equipment. The equipment should have been taken by the robot because it was his daily task. However, the robot received the wrong information in the input. This incident comes because of the lack of safety precautions that should be a priority before operating this robot. The judges judged that this was not the robot's fault. In 2016, the Criminal Investigation Directorate of Polda Metro Jaya detected thousands of bot accounts that spread hoaxes, provocations and SARA. The police filed a block to the Ministry of Information and Information for 300 provocative robotic or bot accounts.

Artificial Intelligence The ever-evolving has triggered an algorithm called with Deepfake Technology. In other words deepfake is a term given to an algorithm where the algorithm allows users to change faces from one actor to another in the form of images or videos. Deepfake technology is a new method of videography and photo manipulation that allows one person's face to be transformed into another person's face in the form of a video [7. Deepfake applications have received widespread attention as the technology has been used in celebrity porn videos, fake news, misinformation, and financial fraud. This also leads to industry and government exposing and restricting its use .Technology deepfake Utilizing data in the form of faces from individuals who are part of personal data and have the potential to be misused, be it for criminal acts such as propaganda, identity theft or other related privacy issues.

Indonesia currently has laws and regulations related to information technology, in particular Law No. 19 of 2016 amending Law No. 11 of 2008 on Electronic Information and Transactions . Artificial Intelligence in the ITE Law it is classified as an electronic system. However, the law does not yet provide for artificial intelligence in detail and forms of crime deepfake. Regulatory conditions that have not been regulated optimally certainly have the potential to cause legal problems so that if left unchecked it can provide legal uncertainty in the community. Use artificial intelligence in crime deepfake is an action that needs to be regulated regarding its regulation. Therefore, this study will discuss related to regulation artificial intelligence as a perpetrator of evil deepfake.

MAIN RESULTS

Deepfake Crimes

Deepfake is a technique for creating an intense human image based on artificial intelligence, where an image or video can be combined with certain methods so that the results appear real. Use of technology deepfake It was originally introduced professionally to feature films or television shows. Deepfake technology is currently being used in photo and video recordings to alter one person's face to look like another person's face. Fake content is nothing new, but deepfakes use powerful machine learning techniques to create visual and audio content that is likely to be deceptive.

Deepfake has a positive impact when used properly in everyday life. One of the positives of deepfakes is reflected in an application created by Microsoft called "seeing AI", where technology deepfake designed to help people with disabilities. This application reads text in document formats, scans products and barcodes, recognizes people and their emotions, describes nearby places, helps identify currency and banknotes, and adjusts voice volume and tone. You can communicate in multiple languages based on: Products are tailored to the environment [9]. In the entertainment industry, there is technology deepfake CGI (Computer Generated Imagery) which can create three-dimensional animated images or videos entirely using the help of computer graphics. The use of CGI technology helps the film production crew and actors to relax the shooting process. With CGI, a filming process can be done in the studio by adding media green screen, without going to the original location. Deepfake It is also useful in helping retail indstrial sales. This makes it easier for customers to try on a product virtually such as clothes, shoes to hairstyles.

Developing this technology is like a double-edged sword. Although it is undeniable that technological advances provide convenience for humans, on the other hand it raises new problems. Deepfake even if it's just a fake audio or visual made using artificial intelligence This does not mean that deepfakes can be easily seen as fakes with the naked eye. Quite the opposite, deepfake can look very real and original depending on its use. More and more data in the form of voice samples and facial images from source subject (the individual whose face or voice is used) the better deepfake the result.

This deepfake technology has the potential to be a tool for crime. The technologies that provide this convenience are often misused without the consent of the data owner, or source subject, with negative consequences. The harm caused occurs because whatever happens in a deepfake always refers to and is considered the work of the individual featured in it. This becomes very vulnerable for the source subject as the owner of the data because he must be responsible for the consequences caused by the deepfake. If the use is for purposes in the film, advertising, broadcasting industries, then the use of one's personal data must still be protected because it involves the right to privacy for the individual concerned, so it requires permission before use [10]. Depending on the application, deepfakes could be used to destroy personal privacy or interfere in a country's economic and political situation. There are four types of creators who use deepfakes : deepfake for entertainment porposes only, deepfake user communities, political actors such as governments and activists, political actors such as scammers, and legitimate actors such as corporate television. only.The negative effects of deepfakes may also be caused by people's tendency to react to false news online [11].

Deepfakes have the potential to erode people's trust, especially when it comes to big, well-known people. Not only about fake videos, one's reputation can also be damaged easily with this technology. Many people spread negative content with deepfake applications, such as the spread of hoax news or data manipulation. Large-scale fake videos, high or low quality, still fuel misinformation and disinformation in society because people often don't pay attention to the source, veracity, or purpose of news. There is a possibility. The emergence of deepfake applications can lead to disinformation that has adverse effects, not only on society but also on democracy. In 2019, video footage emerged of President Obama swearing while giving a public service announcement. Then there is also a video of Mark Zuckerberg who says about his power to control all data on Facebook. In its use, deepfakes are divided into several types, namely [12]:

1) Photo Deepfake

In this type, the use of deepfakes is to make changes to the face, replace or blend the face or body of another person. Examples of its use in FaceApp applications that can change a person's appearance or face. The use of deepfake photos helps people to be able to try cosmetics, fashion, hairstyles and so on virtually.

2) Audio Deepfake

Deepfake audio can change the voice or mimic the voice of others. The development of deepfake audio was demonstrated by OpenAI which is a non-profit AI company funded by one of Elon Musk. Through its new system called Jukebox, OpenAI creates an artificial neural network capable of producing musical compositions including vocals in various musical genres and styles of singers. Armed with a dataset of 1.2 million songs obtained by the OpenAI team, they linked songs with lyrics and recorded them from LyricWiki until they were able to train the system to create its own musical compositions.

3) Deepfake Videos

Deepfake video is a technology that allows the face of a person in a video to be replaced with the face of another person.This technology can manipulate videos to make it appear that the people in the video are acting or acting.The main purpose of this video is to influence the way people think through the concept of "seeing is believing." The human brain can convince itself of fake or fake events even if the quality of the resulting video is not perfect.

4) Generative Text

By using computers, artificial intelligence can produce artificial text but look real. On september 8, 2020, the guardian published an article entitled "a robot wrote this entire article. are you scare yet, human" the news is connected using a language generator, generative pre-trained transformer-3 (gpt-3) developed by openai. gpt-3 is trained based on data from commoncrawal, webtext, wikipedia, and book sets.

Deepfake Can be misused to create negative content, most of the targets are aimed at public figures to make people more interested in reviewing their content. These cases can occur repeatedly and continuously if there is no prevention and treatment, then people will continue to freely edit videos or photos without any restrictions. Therefore, there is a need for legal arrangements that can regulate clearly and provide strict sanctions so that there is no repetition of the same crime, it is also intended to reduce the impact and losses caused by abuse deepfake aforementioned. Hence the abuse deepfake that meets the criteria for criminalization may be classified as a criminal offence. Criminal misuse of the application deepfake can be analyzed based on the laws governing cybercrime attributed to app abuse deepfake namely Law No.19 of 2016 concerning Amendments to Law No.11 of 2008 concerning Electronic Information and Transactions, Law No.44 of 2008 concerning Pornography, can also use the Criminal Code which regulates related to fraud, decency, and defamation.

Use and utilization deepfake This is done by a person as a subject of law. This relates to the usage implemented in various application features such as: MyHeritage, FaceAppand Deepfake Studio which is used by users from all over the world including in Indonesia. From use deepfake, has problems resulting from its use. This act can be classified as a form of cyber crime. In the evil of the virtual world (cybercrime), the perpetrator or someone who has violated the law must certainly be responsible for the losses he committed. The implementation of a legal right and obligation always requires the implementation of a form of legal responsibility [13 .

The emergence of deepfakes from well-known political figures can have effects that significantly affect social conditions in society ranging from hate speech, disintegration, conflict, criminal acts, and intolerant acts that are increasingly accommodated. From various literature sources from The Guardian, CNN, Business Insider, and the BBC, here are some things that can be caused by deepfakes [14] :

a. Deepfake videos can spark great social unrest

Deepfake technology can create convincing videos of public figures. The risk is public safety, with such adoption encouraging "false conspiracies". The circulation of deepfakes can be a physical mobilization under false pretenses, starting a public safety crisis and triggering outbreaks of violence. This can be seen from a row of fake conspiracies that proliferate through whatsapp as an example of how fake messages and media have fueled violence. From these cases, it can be predicted that deepfakes have the ability to spread violence and spread propaganda in society.

b. Deepfakes can spread hate

Deepfakes are used to expand the spread of LGBT, antiracial, white supremacist, and radical ideas. Videos that are shared can on behalf of anyone to speak out of accordance with reality to sharpen these sentiments.

c. Deepfakes can be a propaganda tool

This technology allows people to create propaganda by utilizing images of public figures. This condition can be dangerous for countries that are experiencing conflicts between groups. Manipulative propaganda can cause physical mass movement that allows friction to occur. As time progresses, the quality of deepfake videos will be more perfect and it is very difficult to identify whether the video is real or fake. Especially if the person in the video is a well-known public figure who has a lot of followers.

d. Deepfakes can be a political tool

The emergence of deepfake videos from political figures in the United States has proven that deepfakes are becoming a political tool. Donald Trump is one of the political figures who spread a deepfake video of Nancy Pelosi and triggered various responses from netizens. Deepfake videos can be material for politicians to attack other politicians in order to achieve their political goals. Deepfakes can make noise in political years, especially for public opinion agitation, and attacks between camps.

Deepfakes can used to defame, impersonate, and spread disinformation. The main pitfalls This deepfake is that humanity could be in an age where it can no longer determine whether media content conforms to the truth. Consequences of deepfakes Not significant enough to shake the entire system of government. But deepfake has the ability to corrupt individual entities tremendously. This is because: deepfake It is often aimed at one individual and his relationship to another in hopes of creating a narrative strong enough to influence public opinion or belief. Application usage deepfake has an impact on the tendency of malicious behavior from people who abuse the application deepfake.

Artificial Intelligence as Perpetrators of Deepfake Crimes

Artificial Intelligence is the result of technology created by humans that aims to facilitate work so that it is more efficient and effective. Artificial intelligence is designed to be intelligent so that it has exactly the same ability as the human brain, which has the ability to reason, think, process knowledge, and even make decisions in solving problems. Through human commands, artificial intelligence can gain knowledge, and by simulating thought processes, artificial intelligence can use knowledge and think like humans to solve existing problems. Although artificial intelligence cannot accept researchers, experience, and knowledge like humans, it can obtain the necessary knowledge through human efforts [15] .

The rapid progress of digitalization has provided a solution to a social problem. If a machine can think, decide, and act of its own accord, shouldn't it also be recognized as an entity? The more intelligent a system is, the more likely it is to perform actions that give rise to legal consequences [16]. Of course, the existence of artificial intelligence as a result of technological development cannot be separated forom the existence of national legal regulations in the form positive lawa the development and advancement of technology embedded in artificial intelligence that can perform human tasks may give rise to a variety of legal issues related to the acts it performs.

The development of artificial intelligence currently has not reached a level equivalent to humans, namely in the types of Artificial General Intelligence (AGI) and Artificial Super

Intelligence (ASI). With increasingly complex developments, efforts to create a legal umbrella for artificial intelligence must be prepared early. This is important to prevent negative impacts from AGI and breast milk levels. The application of deviant artificial intelligence technology is not a matter that can be considered trivial, the threats posed can be in the form of digital, physical and political threats [17] . This deviation in the application of artificial intelligence is believed to cause chaos in global, targeted and very efficient attacks. The development of deviations from artificial intelligence technology that are not followed by defense against it produces 3 (three) high-level implications for the threat landscape that make artificial intelligence crimes will: [18]

a. Expanding existing threats

The use of an efficient artificial intelligence system that can increase the number of perpetrators who carry out certain attacks, if artificial intelligence can be calculated the perpetrator will create a much higher attack ability because the perpetrator already has resources. Advances in artificial intelligence technology can also expand threats by increasing the intent and desire of perpetrators to plan an attack. Artificial intelligence makes the perpetrator not participate in a threatening act where the perpetrator can act anonymously and does not need to see the victim directly which causes the perpetrator's post-trauma.

b. Introducing new threats

The nature of artificial intelligence that is not tied to humans indicates that artificial intelligence systems can carry out attacks that humans cannot do. For example, humans cannot realistically imitate other human voices or make them in real audio resembling recordings of human speech but the development of artificial intelligence actually shows the opposite where this technology can imitate real human speech. This system will in opportunity be able to open up new crimes to spread ambiguous information and imitate other things. Artificial intelligence technology that is still not in the perfect stage there are weaknesses and vulnerabilities that still surround this technology so that actors and by exploiting these weaknesses to be used as threat opportunities.

c. Change the typical character of a threat

Attacks that utilize artificial intelligence technology and exploit the weaknesses of artificial intelligence generate a new threat and make it highly effective, targeted and difficult to overcome turning the target into a distinctive or distinctive threat.

Legal regulations on artificial intelligence can be analyzed through the civil code. The Civil Code indirectly provides the option that artificial intelligence is analogous to a worker. This can be seen in the relationship between workers and employers regulated in Article 1367 paragraphs (1) and (3) of the Civil Code which states as follows:

(1) A person is liable not only be for damages caused by his own actions, but also for damage caused by the actions of those for whom he is responsible or caused by goods under his control.
(3) Employers and persons who appoint others to represent their affairs shall be liable for losses incurred by their servants or subordinates in the performance of the work for which these persons are used".

The article can be analogous to that artificial intelligence This as a worker by looking at the characteristics of the "worker" inherent in the system artificial intelligence. If artificial intelligence It is as a worker that he has a legal relationship with the employer. Of course, he is also responsible to his employer if he breaks the law. But in practice this is very difficult, so it still requires humans to be responsible. In addition to being analogous to a worker, artificial intelligence can be analogous to animals . It is solely looking at the resemblance between animals and animals. [19] artificial intelligence as an entity that can move and behave independently. In this case, the Civil Code regulates if the animal causes harm then the owner will be responsible. This is also based on Article 1368 of the Civil Code which states that:

"The owner of an animal, or who wears it, is, so long as the animal is clothed, responsible for the harm in his custody, or lost or detached from his care"

The article means that the owner of the animal will be responsible for the harm caused by the animal, whether it is under his supervision or the animal is lost or escaped from his supervision. But the analogy of artificial intelligence categorized as animals is still under long debate that still has to be studied more deeply both from a philosophical and theoretical side.

Technology artifificial intelligence Can carry out actions and actions like humans, of course, this is what underlies a legal arrangement in a country to have special arrangements related to artificial intelligence. At this time, the status and standing of artificial intelligence both the laws of other countries and Indonesian law are still a problem. Legal position of artificial intelligence It is not yet known with certainty so that if there is a loss or unlawful act caused by artificial intelligence It will be very difficult to know who will be responsible for the loss. However, that does not mean there are no alternatives that can be used [20] . Based on the law applicable to Indonesia with respect to technology regulation, namely Law No.19 of 2016 on the amendment of Law No.11 of 2008 on electronic information and transactions, this regulation, as a form of government, regulates the rapid development of technology in Indonesia.It corresponds to Indonesia.The purpose of this Information Law and Electronic Transactions is to resolve all technology and information system issues in Indonesia, provide legal certainty, and bring benefits to the resolution of technical issues [21] .

Although the Information Electronic Transactions Act is an administrative law, but legislators include some provisions on criminal acts. This is inseparable from the birth of the information technology revolution which also brought the potential for crime. In the information electronic transactions act, the anatomy of crimes classified as criminal offenses is broadly divided into two groups. First, crimes that target the internet, computers, and related technologies. Under the information electronic transactions act, there are seven types of crimes classified as crimes targeting the internet, computers, and related technologies. These crimes are considered contemporary crimes that produce new forms of crime, namely Hacking (Article 30), Intersepsis Ilegal (Article 31), Data Interference (Article 32 paragraphs 1 and 3), Electronic Theft (Article 32 paragraph 2), Interference with electronic systems (Article 33), Misuse of Devices (Article 34), and Fraud and counterfeiting related to computers (Article 35). The second group Is related to the publication and distribution of illegal content using the internet, computers, or technology. This second group is considered an old evil, but technological developments have created a new medium for these acts to emerge or arise. These crimes include pornography (Article 27(1) of the Act), gambling (Article 27(2) of the Act), defamation (Article 27(3) of the Act), and extortion (Article 27(4)). and consumption. These include fraud endangering people (Article 28(1)), hate speech (Article 28(2)) and threats of violence against others (Article 29).

When artificial intelligence In contact with crime, it is necessary to know that crime can occur due to negligence (auctus reus) and intent to commit a crime (mens rea). If the robot artificial intelligence Proven to have sufficient awareness, then they can be responsible as direct perpetrators of criminal acts or responsible for crimes of negligence. If it has been recognized that the robot artificial intelligence Having a mind of its own, endowed with man-like free will, autonomy or a sense of morality, then the entire legal system must be drastically changed.

The Information and Electronic Transactions Law takes into account the characteristics of artificial intelligence and classifies it into electronic systems and electronic agents according to the definitions of electronic systems and electronic core. This is stipulated in Article 1, Section 5 of the Law on Information and Electronic Transactions:

"An electronic system is a set of electronic devices and processes designed to prepare, collect, process, analyze, store, display, report, transmit, and distribute electronic information."
While electronic agents are regulated in Clause 1, Article 8 of the Law on Information and Electronic Transactions, which stipulates:

"An electronic agent is a device in an electronic system that is designed to automatically perform actions on specific electronic information in the possession of a human being."

For the purposes of Article 1, an electronic system is described as a set of electronic devices and processes for the purpose of preparing, collecting, processing, analyzing, storing, displaying, publishing, transmitting and distributing electronic information. An electronic agent is a part of an electronic system created to automatically perform actions on electronic information stored by humans.The obligations of the operator of an electronic system also apply mutatis mutandis to the organizer of an electronic facility.The Electronic Information and Transactions Act also stipulates that the operation of electronic systems can only be carried out by individuals, public operators, commercial organizations and the general public.Who can be called a legal subject in information law and electronic transactions, specifically state organizations, individuals, economic organizations and communities.

Artificial intelligence is based on positive law, Indonesia has so far only functioned as a subject of law and has not been recognized as a subject of law. Increasing similarities between humans and artificial intelligence indirectly proves that now a confession is needed stating that artificial intelligence is a subject of law. It must be admitted that it is difficult to categorize or equate artificial intelligence as an organism like humans. This raises the debate like a corporation that is considered a subject of law. The debate that arose at that time was that corporations were not organisms but there was a need to recognize corporations as subjects of law. Artificial intelligence is considered a computer product operated by humans and it cannot perform its work at will [22] .

Artificial intelligence is a human-operated technology in its implementation, combined with positive law and artificial intelligence operated by electronic system operators in accordance with Government Regulation No.71 of 2019 on the Implementation of Electronic Systems and Transactions.In this case, the operator of the electronic system as a legal entity is responsible for the operation of the electronic system, except in mandatory cases.

Deepfakes and artificial intelligence are the result of technological developments, artificial intelligence is the gift of technological innovation that can eventually turn deepfakes into deadly and threatening weapons. Deepfakes use machine learning and neural networks.
Neural networks are an artificial intelligence technique that teaches computers to process data

in a way inspired by the human brain.The main characteristic of deepfakes is that the software used must be based on artificial intelligence (AI) in order to exchange the face of a subject as a source with another subject in the form of a video or image as an external target. GAN (Generative Adversarial Network) technology is the foundation of deepfake.The central idea comes from the zero-sum game between two people in game theory. Traditional deep learning is a single-level process, but GANs introduce an “adversarial” mechanism based on repeatedly retrieving and detecting internal arrhythmia data. GAN is implemented bidirectionally by two deep dynamic convolutional neural network training sets, including a generator and a discriminator [11] .

Artificial intelligence through computer programs can also be realized in hardware that solves tasks related to people, knowledge, and communication, as it can think a set of binary codes of programming logic on behalf of the human brain and body. Artificial intelligence has many unique capabilities, including the ability to integrate into many different applications, adapt to technological advances based on the Internet of Things, and be used by public services to improve national military resilience. There is a function. For example, the US used facial recognition algorithms to punch terrorist suspects in the face during the conflicts in Syria and Afghanistan, and they can also be used for population control to create ID cards. Cargo transportation in Indonesia. Using artificial intelligence in deepfake technology, developers can easily superimpose one person's face onto another person's body in a series of images that become a video.
[10].

Deepfake technology is vulnerable to being used as a means of committing crimes such as the spread of fake news, fraud, defamation, pornography, and manipulation of facts or circumstances [23] .

a) Spread of Fake News (Hoax)

Hoaxes are news or information that is spread containing things that are uncertain or not facts that happen. The spread of hoaxes is most widely circulated through social media. Hoaxes in Indonesia have sowed doubts about the information received and caused confusion among the public.Many irresponsible parties are taking advantage of this situation to spread slander and hate. In information and electronic transaction law, spreading hateful feelings or reporting false information is an intentional crime. Article 28, Paragraph 1 of the Electronic Information Transaction Law stipulates that ``any person shall knowingly and without authority disseminate false information in electronic transactions, causing confusion and causing damage to consumers. Risk of crime is defined in Article 45A(1) of the Electronic Information Transactions Act.The penalty is up to six years in prison or a fine of up to Rp1 billion.

b) Fraud

Deepfake audio is often used in psychological manipulation scams, making people believe they are receiving instructions from trusted individuals.In 2019, the CEO of a British company was scammed over the phone when someone asked him to transfer 220,000 euros to a Hungarian bank account using deepfake audio technology to imitate the voice of the parent company's CEO. Fraud is included as a criminal offense in the Penal Code. Article 378 of the Penal Code stipulates that a person who aims to gain benefits for himself or others by using a false name, false rank, using false words, inciting others to give something or incur debt and cancel claim compensation, are threatened fraud received 4 years in prison.

Fraud that occurs today uses a variety of methods, such as sending fake news or illegally impersonating someone else and committing fraud over the Internet. Fraudulent acts that cause damage to victims of losses in electronic transactions are stipulated in Article 28, Paragraph 1 of the Electronic Information Transactions Act, and are acts that intentionally or unintentionally disseminate false and misleading information to harm consumers provides for losses suffered in electronic transactions transaction transaction. The elements of the crime stipulated in Article 28, Paragraph 1 of the Electronic Information Transaction Law have certain similarities with the crime of fraud stipulated in Article 378 of the Penal Code.

c) Defamation

Deepfake application This increases the difficulty in classifying whether a video is original or not. Alex Champandard says that everyone should know how quickly things can be destroyed by deepfake technology and that the problem is not a technical one but one that needs to be solved with trust in information and newspapers. Deepfake technology It is possible to create convincing videos of public figures.The risk is related to public safety, as such an application would encourage “wrongful conspiracies”. Circulation of deepfake This may involve material mobilization under false pretenses, causing a public security crisis and triggering an outbreak of violence.Deepfake abuse can damage a person's reputation as that person is negatively impacted by the results of the image or video created by the deepfake itself.Defamation is an act intended to harm a person's honor and dignity. Defamation consists in conveying a speech by accusing certain acts aimed at a person's honor and reputation, leading to humiliation and degradation of a person's self-esteem.

Defamation using information technology is carried out by creating images or creating electronic documents to defame another person.Contempt in the Penal Code has been revised from Article 310 of the Penal Code to Article 321 of the Penal Code. At the same time, the Electronic Information Transaction Law is in accordance with Article 27, Section 3, which prohibits the transmission, distribution or provision of electronic information or documents containing offensive or defamatory content. The injunction carries a maximum penalty of four years in prison and a maximum fine of Rp 750,000,000.

d) Pornography

Influence deepfake In the victim is the manipulation of images and videos using malicious artificial intelligence. Like pornography deepfake aims to humiliate his target. Moreover deepfake Also used for target deception and revenge. Deepfake It can also threaten a person's reputation, image and credibility. Especially if deepfake The resulting one looks real and similar to the original. Deepfake What is already scattered can threaten a person's position and job. Crime deepfake continues to expand and cause harm to many people, not only celebrities, but politicians and also famous figures. During the Covid-19 pandemic, deepfake There is concern because of the use of this technology in videos of celebrities or public figures.

The offense of obscenity is regulated by Law No. 44 of 2008 on pornography. Article 4(1) of the Pornography Act states that the creation, manufacture, copying, reproduction, distribution, dissemination, importation, offer, exchange, rental or supply of pornographic content, including sex, sexual violence, masturbation or masturbation, nudity, genitalia. It stipulates that everyone who does And child pornography. The ban carries a penalty of up to 12 years in prison or a fine of at least Rp250 million and up to Rp6 billion. Pornography can also be attributed to the Information and Electronic Transactions Act, in particular Article 27(1).This law stipulates as follows: “Send, download, and/or create accessible electronic information and/or electronic documents”

e) Manipulation of facts or circumstances

North Korean leader Kim Jong-Un and Russian President Vladimir Putin have become targets of deepfake technology manipulation by the non-partisan advocacy group “RepresentUs”. The event was intended to be broadcast publicly as an advertisement to convey the idea that executive interference in U.S elections would be detrimental to American democracy.This ad is also intended to shock Americans into realizing the fragility of democracy and how media and information can significantly influence the path of the country, regardless of its credibility. At the end of the video, he also issued a statement clarifying that the images were fictional. However, the final ad was not released to the public to avoid negative reaction from the American public. In Indonesia, the National Police's Cyber Crime Directorate arrested a man with the initials MS for spreading content insulting tribes and editing photos of President Joko Widodo.The suspect intentionally showed hatred by practicing racism. This case of hate propaganda is regulated by Article 28, Paragraph 2 of the Law on Information and Electronic Transactions, which states: Ethnicity, religion, race, and intergroup foundations

This technology allows people to create propaganda by utilizing images of public figures. This condition can be dangerous for countries that are experiencing conflicts between groups. Manipulative propaganda can cause physical mass movement that allows friction to occur. As time progresses, video quality deepfake It will be more perfect and very difficult to identify whether videos containing propaganda are increasingly easy to spread and accepted or believed.

When artificial intelligence commits a crime, in this case the artificial intelligence does not understand the meaning of the consequences of the action it performs and the artificial intelligence cannot determine its own desire to perform the action. it and the artificial intelligence are not aware of that behavior execution legal action. With regard to consciousness, humans as absolute legal subjects in criminal law are not always free from negligence for the actions they do. Therefore, artificial intelligence does not have the ability to be a legal subject that can be given responsibility in criminal law.

Comparison of Artificial Intelligence Settings that Commit Deepfake Crimes in California and Indonesia

a. California

Lawmaker ini the U.S have been working for years to combat online sexual harassment, and many jurisdiction have criminalized revenge porn. Some lawmakes have proporsed specifically banning deepfake depicting lewd sexual acts. America has 50 states. These states each have their own legislative laws, which are part of the United States Code or the general constitutional law of the United States. In December 2018, the United States congress passed the Malicious Deepfake Prohibition Act Of 2018 as the law defining deepfakes. However, this is opposed by the public because of its vague definition and potential conflict with the first amendment of the United States constitution [24] .

Several states responded quickly to the inappropriate use of deepfakes, passing laws inclu ding California, Texas, and Virginia. California has passed two laws to tackle deepfakes: Calif.AB-602 and Calif.AB-730. Texas passed a deepfake law known as Tex.SB 751. Virginia legalizes "unlawful dissemintaion or sale of image of another person" [11] . In the United States, 30 states recognize a variety of publicity rights, known as rights of publicity. California has a high level of national celebrity and well-known entertainment industry that has infuluenced laws and legislative decision in this area. Currently, California is one of five states that allow advertising under both statutory and common law.

b. Indonesia

Indonesia until now the discussion about artificial intelligence and its influence on law has not developed much. Indonesia does not yet have a definite legal rule regarding the existence of these smart robots. To date, the use of artificial intelligence in various fields has been made public only by Law No.11 of 2008 on Electronic Infromation and Transactions and Law No.19 of 2016 on Amedments to Law No.11 of 2008 on Electronic Information and Transastions is regulated and Government Regulation No.71 of 2019 on Inpementation of Electronis Trading Systems. With the development of artificial intelligence, actually cyber crimes regulated by the ITE Law still do not cover several important aspects such as how artificial intelligence is accountable, data security from artificial intelligence users, and others. Because artificial intelligence in the aspect of cyber law is very large and complex, there is an urgency for the public and law enforcement to know the development of artificial intelligence technology, at least be able to predict the possibilities that will occur that may be caused by this artificial intelligence and how to accommodate these issues when they occur in the future.

Table1. Comparison of the Regulation of Artificial Intelligence Committing the Crime of Deepfake in California and Indonesia

No	Types of Crimes committed by AI	California	Indonesia
1.	Pornography	AB 602 provides that the person depicted has a cause of action against: ``[E] (1) Create sexually explicit material that the person depicted knows, or reasonably should have known, that the person depicted is doing so. or (2) that the person depicted does not consent to its creation or disclosure; A person who knowingly discloses sexually explicit material.	Article 27 Paragraph (1) Law on Information and Electronic Transactions: "Any person who knowingly and without authorization distributes, transmts and/or crates accessible electronic informations or documents that violate good ethics"
2.	Fraud	AB 730, this law covers "materially misleading audio or video media" such as: ``[A] visual, audio, or video recording of a candidate's appearance, speech, or behavior intentionally manipulated into an image or sound; may appear to be and cause a person to have a fundamentally different understanding or impression of the representational content of an image, sound, or video recording than if he or she had used it or seen or heard the image, the original, unaltered version of the audio and video recordings. "	Article 28, paragraph (1) Law on Information and Electronic Transactions: "Any person who intentionally and without speads false information, causes confusion in electronic transactions, and causes damage to consumers".
3.	Defamation	Section 3 of California AB 730:``(a) Except as	Article 27 paragraph (3) of the law regarding

		otherwise provided in subsection (b), no person, corporation, association, corporation, campaign committee, or organization shall conduct a campaign that: You may not produce, distribute, publish, or broadcast any material that, in actual malice, contains (1) an image or photograph of a person superimposed with the likeness of a candidate for public office, or (2) the likeness of another person. ``Campaign Materials" includes images or photographs of candidates for public office overlaid with images or photographs of candidates for public office that are displayed or superimposed on a person. or computer images, including but not limited to; For purposes of this section, "actual malice" means knowing that an image or photograph has the image of a person superimposed on it to create a false representation, or that the image or photograph has an image of a person superimposed on it to create a false representation. It means carelessly ignoring whether or not it is layered to create a misrepresentation. False representation	information and electronic transactions: “Any person who, knowingly and without authorization distributes, transmits, and/or makes available electronic information and/or accessible electronic materials that are defamatory and/or libelous in content”.

Calif-AB 602 is designed to punish anyone who impersonates one or more people who engage in nonconsensual sexual activity. Disclosure under AB 602 means "to make publicly available, available to, or distributed to the public.”Victims can file a complaint if they are depicted in videos or images without their consent or disclosure.This law excludes the liability of a person who discloses obscene material in certain circumstances.These circumstances include “reporting illegal activity” while performing law enforcement duties or as part of legal proceedings. We also exclude materials related to legitimate matters of public interest or comments, criticisms, or disclosures protected by the California Constitution or the United States Constitution. Victims are entitled to economic and non-economic damages, as well as punitive damages (limited by law to $30,000, or $150,000 if the tort was committed with malice), and punitive damages and can recover your attorney's fees. While this law is intended to protect Californians, it focuses solely on the use of deepfakes for sexual purposes. AB 602's scope is too limited to fully address the problem caused by deepfakes. While in Indonesia, with respect to the provisions of Article 27, Paragraph 1 of the Electronic Information Transactions Law, the question of whether the creator fully complied with the elements of the provisions may result in sanctions based on the provisions of the same article. Whether paragraph 45 (1) of this Act. The Information and Electronic Transactions Act can lead to imprisonment of up to 6 years and a fine of up to Rp1,000,000,000.00

California-AB 730, the law aims to reduce the impact of candidates running disinformation campaigns aimed at confusing voters. Focusing on deepfakes has had a huge impact in the political arena. This law provides a broader definition by including audio and visual manipulation. Simply put, a deepfake is any audio or visual medium in electronic format, including moving images, video recordings, or any audio recording created or altered in such a way that to the viewer, it appears to be the same as the original. Record video or audio. However, this law only applies to candidates running for election. It does not include candidates for appointed civil service positions. This data also does not include ordinary people who could be attacked or harmed by deepfakes. The law grants immunity to radio stations and websites that broadcast altered media, provided they post a label stating that the authenticity of the media can be verified. Media companies are not responsible for airing paid political advertisements that contain misleading audio or video material. In Indonesia, fraud in electronic transactions is stipulated in Article 28, Paragraph 1 of the Electronic Information Transaction Law, and those who spread fake news and cause damage to others are subject to criminal liability. Criminal intimidation against a person meeting the requirements of Article 28, Paragraph 1 is punishable by up to 6 years' imprisonment and a maximum fine of VND 1 billion under Article 45A of the Law on Electronic Information Transactions Leading to Death.

Defamation can be done in writing or orally. Under AB 730, an individual, business, business association, campaign committee or bad faith organization is prohibited from producing, distributing, publishing or broadcasting material containing images of candidates member to a public agency. A person's image superimposed on an image or photograph can create a misleading representation.Candidates for public office whose likenesses appear in prohibited images or photographs may bring civil claims against the entities that publish or produce such images or photographs. The court may award damages equal to the costs of producing, distributing, publishing or broadcasting campaign material in violation of this section, in addition to reasonable attorney's fees. In Indonesia, defamation through electronic media is stipulated in Article 27, Paragraph 3 of the Electronic Information Transaction Law, which stipulates as follows: Electronic documents containing defamatory and/or libelous content. ” Defamatory or insulting conduct using network media is regulated separately in the Information and Electronic

Transactions Law because the impact is more global than ordinary defamation. Emails can be sent anywhere in the world in a matter of seconds, social media statuses can be forwarded and shared or retweeted with ease, and the resulting impact can be complex and complex. Prohibition of insult and/or defamation using computer systems may carry criminal penalties under Section 45(3) of the Information and Electronic Transactions Act, with imprisonment of up to four years and a fine of up to be. 750 million.

Now countries need to consider laws governing artificial intelligence that commit deepfake crimes. There are several important points to consider when making laws regarding artificial intelligence that commit deepfake crimes. First, provide a broadly encompassing definition of artificial intelligence or deepfakes. A broad definition is needed to encompass as many things as artificial intelligence or deepfakes might do.Second, expand the scope of accountability of artificial intelligence or deepfakes. Third, determine the appropriate standards of accountability for artificial intelligence or deepfake makers, for example those related to intentionality, malicious intent, negligence, or other intentionality. The standard of responsibility must be reinforced. Fourth, give punishment by considering the crime committed. Fifth, be inclusive by expanding the laws that will be established to protect everyone, both children, the general public, and all citizens.

CONCLUSION

Regulations related to artificial intelligence as perpetrators of deepfake crimes until now have not been grammatically regulated in a specific legislation. The misuse of deepfakes by artificial intelligence cannot be separated from cyber crime because the spread of deepfake photo or video edits is carried out through social media which also uses the internet network in its operation, therefore the abuse of deepfake applications can be classified as cybercrime. The right rules to ensnare artificial intelligence as perpetrators of deepfake crimes include Law No.19 of 2016 concerning Amendments to Law No.11 of 2008 concerning Electronic Information and Transactions, Law No.44 of 2008 concerning Pornography, can also use the Criminal Code which regulates related to fraud, immoral crimes, and defamation crimes. Indonesia in the future needs to immediately design more specific arrangements related to artificial intelligence in Indonesia. The use and development of artificial intelligence requires law as a means of development. This is to provide legal certainty and determine limits in use and utilization to prevent the misuse of artificial intelligence in the future.

REFERENCES

[1] A. R. Lodder, A. Oskamp, and M. J. A. Duker, “AI & Criminal Law : Past, Present & Future,” 2022. [Online]. Available: http://www.rechten.vu.nl/~lodder

[2] R. A. Rahman and R. Habibulah, “The Criminal Liability Of Artificial Intelligence : Is It Plausible To Hitherto Indonesian Criminal System?,” Legality : Journal of Legal Science, vol. 27, no. 2, p. 147, Nov. 2019, doi: 10.22219/jihl.v27i2.10153.

[3] Niru Anita Sinaga and D. Atmoko, "Readiness of the Indonesian Legal System in Transforming Society from 4.0 to 5.0," KRTHA BHAYANGKARA, vol. 17, no. 1, pp. 119–126, Apr. 2023, doi: 10.31599/krtha.v17i1.2111.

[4] H. Surden, “Artificial Intelligence and Law: An Overview Recommended Citation Artificial Intelligence And Law: An Overview,” 2019. [Online]. Available: https://readingroom.law.gsu.edu/gsulrAvailableat:https://readingroom.law.gsu.edu/gsulr/vol35/iss4/8

[5] Suyanto, Artificial Intelligence, 3rd ed. Bandung: Infromatika, 2021.

[6] E. N. Sihombing and M. Y. Adi Syaputra, "Implementation of the Use of Artificial Intelligence in the Formation of Regional Regulations," Scientific Journal of Legal Policy, vol. 14, no. 3, p. 419, Nov. 2020, doi: 10.30641/Policy.2020.v14.419-434.

[7] M. Ariq, A. Jufri, and ; Akbar Kurnia, "Aspects of International Law in the Use of Deepfake Technology for

Personal Data Protection," Journal of International Law, vol. 2, no. 1, pp. 31–57, 2021.

[8] M. F. Ferraro, “Deepfake Legislation: A Nationwide Survey-State and Federal Lawmakers Consider Legislation to Regulate Manipulated Media,” 2019.

[9] R. Sulaiman and Christy Giovanni, Law in the Age of Artificial Intelligence, 1st ed. Robin Sulaiman & Partners, 2021.

[10] A. Purwadi, C. Y. Serfiyani, and C. R. Serfiyani, “Legal Landscape on National Cybersecurity Capacity in Combating Cyberterrorism Using Deep Fake Technology in Indonesia,” International Journal of Cyber Criminology, vol. 16, no. 1, pp. 123–140, Jan. 2022, doi: 10.5281/zenodo.4766560.

[11] M. Liu and X. Zhang, “Deepfake Technology and Current Legal Status of It,” in Proceedings of the 2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022), Atlantis Press International BV, 2023, pp. 1308–1314. doi: 10.2991/978-94-6463-040-4_194.

[12] J. Kietzmann, L. W. Lee, I. P. McCarthy, and T. C. Kietzmann, “Deepfakes: Trick or treat?,” Business Horizons, vol. 63, no. 2. Elsevier Ltd, pp. 135–146, Mar. 01, 2020. doi: 10.1016/J.bushor.2019.11.006.

[13] M. Faqih and E. Soerjati Priowirjanto, "Accountability Regulation for Perpetrators of Deepfakes Abuse in Artificial Intelligence Technology on Pornographic Content Based on Indonesian Positive Law," Indonesian Journal of Social Technology, vol. 3, no. 11, pp. 1156–1168, Nov 2022, doi: 10.36418/jist.v3i11.528.

[14] I. Hidayatul Khusna Sri Pangestuti, "Deepfake, A New Challenge for Netizens Deepfake, A New Challenge for Netizens," AUGUST 1945 JAKARTA 1 PROMEDIA, no. 2, pp. 1–24, 2019.

[15] I. D. Kurniawan, "Analysis of Artificial Intelligence as a Subject of Criminal Law," 2023. [Online]. Available: https://jurnal.tiga-mutiara.com/index.php/jimi/index

[16] E. N. Ravizki and Lintang Yudhantaka, "Artificial Intelligence as a Legal Subject: A Conceptual Review and Regulatory Challenges in Indonesia," Notary, vol. 5, no. 3, pp. 351–376, Oct. 2022, doi: 10.20473/ntr.v5i3.39063.

[17] T. C. Helmus, “Artificial Intelligence, Deepfakes, and Disinformation: A Primer,” 2022.

[18] D. Typhano Rachmadie, "Regulation Of Artificial Intelligence Deviations In Malware Crimes Based On Law Of The Republic Of Indonesia Number 19 Of 2016," 2020.

[19] Q. D. Kusumawardani, "Progressive Law And The Development Of Artificial Intelligence Technology," Veritas et Justitia, vol. 5, no. 1, pp. 166–190, Jun. 2019, doi: 10.25123/vej.3270.

[20] Y. P. Ambor and K. Komarhana, "The Prospect Of Artificial Intelligence As A Subject Of Civil Law In Indonesia," 2021.

[21] M. T. A. R. Haris and Tantimin, "ANALYSIS OF CRIMINAL LAW LIABILITY AGAINST," Journal of Legal Communication, vol. 8, 2022.

[22] G. Widiartana and V. P. Setyawan, “Prospects of Artificial Intelligence Criminal Liability Regulations in Indonesian Criminal Law,” Journal of Citizenship, vol. 7, no. 1, 2023.

[23] H. Novyanti and P. Astuti, "The Legal Trap Of Misuse Of Deepfake Applications In Terms Of Criminal Law," Novum : Law Journal, Dec. 2021.

[24] N. O’donnell, “have we no decency? Section 230 and the liability of social media companies for deepfake videos,” 2021. [Online]. Available: https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspa-