

Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia

Asri Gresmelian Eurike Hailtik, Wiwik Afifah

Universitas 17 Agustus 1945 Surabaya, Indonesia

E-mail: hailitika@gmail.com, wiwikafifah@untag-sby.ac.id

*Correspondence: hailitika@gmail.com

KEYWORDS

artificial intelligence;
deepfake; Legal subjects

ABSTRACT

The development of technology that continues to evolve has given birth to an innovation called artificial intelligence or artificial intelligence which is usually called "AI". The development of AI has sparked an algorithm called deepfake technology. Deepfakes use machine learning and neural network technology, which are methods in AI that teach computers to process data in a way inspired by the human brain. This study aims to determine the regulation of AI as perpetrators of deepfake crimes and to determine the criminal responsibility of AI who commit criminal acts in Indonesia. The research method used is normative legal research using a statutory approach (statue approach), conceptual approach (conceptual approach), and comparative approach (comparative approach). AI is classified as an electronic system and electronic agent which when viewed to the characteristics of AI that has a match with the definition of electronic systems and electronic agents. If AI commits deepfake crimes, it can violate several articles in Law No. 19 of 2016 concerning Electronic Information and Transactions. In California, legislation has been passed to address deepfakes related to pornography, fraud, and defamation: Calif AB-602 and Calif AB-730. There are three AI criminal liability models that commit criminal acts, namely Perpetration-via another model (PVM), Natural-Probable-Consequence Liability Model (NPCLM), and Direct Liability Model (DLM). In Indonesia, AI has not been recognized as a legal subject so that if you commit a criminal act, the person who must be responsible is the creator of AI or AI users

Attribution- ShareAlike 4.0 International (CC BY-SA 4.0)



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. Humans always try to create something that can facilitate their activities so technological developments have produced many tools to facilitate human

activities, even replacing the role of humans in certain functions. The development of technology that continues to evolve has given birth to an innovation called artificial intelligence or artificial intelligence which is usually called "AI". This AI technology has been used to help human work in almost every field such as transportation, education, health, industry, and security (Sulaiman, Robintan, 2021).

Artificial Intelligence (AI) or artificial intelligence is one of the inventions that has changed the face of the world. AI technology allows machines to have autonomous algorithms that can evolve according to their initiatives. AI is able to produce new inputs to carry out tasks like humans, including in processing data and recognizing massive and structured data processing patterns (Rahman & Habibulah, 2019). Artificial intelligence will transform big data and the internet of things (IoT) into a new wisdom, which will be dedicated to improving the ability of humans to live a more meaningful life (Sinaga & Atmoko, 2023).

The beginning of the birth of AI technology began in 1941 with the invention of information storage and processing tools. The invention is called an electronic computer developed in the USA 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 leading to AI. Then in 1956, John McCarthy along with Minsky, Claude Shannon and Nathaniel Rochester conducted research in automata, neural networks and intelligent learning. The result of their research was a program capable of non-numerical thinking and solving thought problems, called Principia Mathematica. McCarthy assumed that every aspect of human intelligence could be precisely defined and simulated by machines. In the first years of AI's development, a program called General Problem Solver was created. This program is designed to initiate humane problem solving. After that, a program called Program with Common Sense was created. This program is designed to use knowledge in finding solutions. In 1959 Prover's Geometry Theorem program was developed, 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. From 1966 to 1974, the development of AI slowed down. In 1980, AI became a large industry with very rapid development. Many large-scale industries are investing heavily in AI (Suyanto, 2021).

Artificial Intelligence (AI) is a technology or system made by humans that can imitate human activities and has a human-like frame of mind in carrying out a job. Some people translate AI as artificial intelligence, artificial intelligence, artificial intelligence, or artificial intelligence. The purpose of creating artificial intelligence is to support human activities to make it easier. The work process of artificial intelligence can be interpreted as equipment or tools to support the work of humans who have the ability to think and reason like humans. According to McCarthy, AI was created to know and model human thought processes and design human behavior. Smart means having knowledge accompanied by experience. There is reasoning where able to make decisions and take action and have good morals. Humans are intelligent because they have knowledge and experience. The more knowledge you have, the wiser you are in solving a problem. In addition, humans also have the common sense to reason based on experience and knowledge possessed. In order for machines to be intelligent and act as well as humans, they must be equipped with knowledge and have the ability to reason (Fahrudin, 2018).

Until now, there has been no single universally accepted definition of what AI is. So it does not rule out the possibility that other AI definitions will appear in the future along with the development of AI capabilities.

The development of hardware and software, making various AI products successfully developed and used in everyday life. AI is divided into three categories based on the ability to process and receive information, namely Artificial Narrow Intelligence (ANI), Artificial General Intelligence (AGI) and Artificial Super Intelligence (ASI). At present, the level of development of artificial intelligence is still in the stage of ANI, and is heading towards the process of developing and realizing AGI, while ASI is still categorized as a future technology. Ray Kurzweil estimates that AGI can be achieved in 2029 while ASI can be achieved in 2045 which will then be followed by a transformation of thinking in society and the economic sector (Kusumawardani, 2019) With the existence of high-level technology that is increasingly developing in society, making AI more real and continues to develop.

The implementation of AI capabilities has been adopted in various fields of work including in the fields of medical, education, and legal services. In the medical field, AI is assumed to be able to help health workers and provide more quality and efficient services. In America, more than 90 percent of prostate cancer surgeries have used robot-based assistance (Budhi et al., 2021). In 2020, AI technology was used to create a Covid-19 detection tool. How to detect viruses with rapid serology methods, antigens, to PCR swabs. Indonesia has succeeded in developing Gadjah Mada Electronic Nose (GeNoSe), a tool that can detect Covid-19 infection through human breath and produce results in minutes with the help of AI The Jakarta Post 2020.

In the field of education, the use of technology has actually begun since the computer era then switched to the era of internet-based technology until now an AI-based education system. Technologies that are closely related to education are machine learning, learning analytics, and data meeping. The application of Intelligent Tutoring Systems (ITS), for example, is able to provide assessment of student tasks. Another example, the turnitin program is able to check the plagiarism rate of student assignments. AI also provides virtual reality programs that help students to explain or practice teaching materials. Teachers can also take advantage of AI technology in the form of web-based platforms, robotics, video conferencing, audiovisual, and 3D technology (Budhi et al., 2021).

The absorption of AI technology is an innovation in various fields of work, including service or law enforcement work. Collaboration between technological sophistication and work patterns in the legal field has the potential to improve the quality and range of legal service provision. AI in legal services is defined as the use of computer operating systems that function to perform tasks such as search, research, legal analysis, decision making and legal prediction. Some countries are already using artificial intelligence in legal practices organized by those countries. In the United States, artificial intelligence has been used as a tool to make legal decisions like a judge, but there are also developments in predictive analytics technology that allows making predictions about the outcome of litigation. Next there is DoNotPay chat in the UK, which currently covers more than 1,000 (one thousand) legal fields. This artificial intelligence has been able to solve legal problems to more than 160,000 people. The UK formed an artificial intelligence committee in the House of Lords to review issues and rules related to artificial intelligence (Taniady et al., 2020). China's Supreme Court in 2015 proposed the establishment of a smart court aimed at creating a transparent, effective, and efficient

judicial system. Smart courts are used to educate the public about applicable laws and legal steps available to parties (Zou, 2020).

Russia's Sberbank company launched a robot lawyer that can file a lawsuit against individuals, and GlavstrahControl launched a robot to help resolve insurance disputes. Saudi Arabia granted citizenship status to the robot Sophia. Japan also granted residence permits to the Shibuya Mirai robot based on special regulations. The European Union has identified robotics and AI as cornerstone technologies, and has recognized the need for significant investment in these areas. A new EU task force was also established to examine barriers related to the adoption of big data and digital technology in various fields. In Indonesia, the Hukum Online website provides the LIA (Legal Intelligence Assistant) platform which is the first legal chatbot in Indonesia to help people get education about marriage law, divorce law, and inheritance law. The use of LIA is enough to ask questions related to the problems experienced and then will be answered directly by LIA automatically (Sihombing & Syaputra, 2020).

Like a double-edged sword, the existence of AI technology in addition to having a positive impact has a negative side as well. The positive impact of using AI itself is related to efficiency where AI can help perform tasks appropriately and efficiently, help make decisions and provide more accurate information, and can increase productivity and facilitate work. AI also has some negative impacts, such as reducing the demand for certain jobs due to the many tasks that machines can perform. This has the impact of making human labor less needed and making people lose their jobs because they are replaced by machines or robots. AI can also discriminate when programmed with inappropriate data and can compromise privacy and security if personal information is misused or data is spread.

AI has the potential to create advanced technology crimes due to the characteristics of autonomous algorithms that cannot be predicted and controlled by humans. No human being can know and control the mindset or algorithm of AI, so the issue arises of criminal liability related to crimes that arise or are committed by AI. 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 addition to robots killing humans, AI can also trigger racism issues. Google has been criticised over an image recognition algorithm scandal that labelled photos of a group of African-Americans as "gorillas". Google confirms that "automatic photo labeling is a new and far from perfect technology" (Hern, 2018). In addition to Google, there is a chatbot called Tay, uploading posts on Twitter that are offensive, racist, and proactive against Adolf Hitler. Tay is a project of Microsoft Technology. Tay was created with the aim to interact with internet users all over the world. Microsoft did not create Tay to do so, so the company eventually deleted Tay's account (Kristo, 2016). In 2016, the Criminal Investigation Directorate of Polda Metro Jaya detected thousands of bot accounts that spread hoaxes, provocations and SARA. The police proposed blocking to Kominfo for 300 provocative robotic or bot accounts on cyber networks (Kominfo, 2023).

The development of AI has sparked an algorithm called 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 way to manipulate videography that can be used to manipulate a person's face into someone else's face in the form of a video. In its application, deepfakes have attracted widespread attention due to the use of the technology in celebrity porn videos, fake news, hoaxes, and financial fraud. This also invites responses from industry or government to detect and limit its use. Deepfake technology utilizes data in the form of faces from individuals who are part of personal data and have the potential to be misused, be it for crimes such as propaganda, identity theft or other related privacy issues (Jufri & Putra, 2021).

Deepfakes have entered Indonesia, marked by Indonesian people who have used applications such as My Heritage where applications are able to animate old photos as if they were alive again. Then there is also, FaceApp which is also able to change a person's photo to be older in an instant. There is Deepfake Studio which has a faceset feature that can manipulate other people's faces by loading up to 500 images to create other people's faces from various angles. The public is increasingly gullible with voice-based fraud attempts. More and more days we can't tell the difference between the voice of AI and the real voice of humans. Even some artificial intelligence applications not only imitate but also enhance it with other capabilities. For example, foreign singers who can skillfully sing Indonesian songs. This has even been done by local Indonesian content creator Octavianus Kalistus, successfully juggling foreign singers, namely Ariana Grande and Jungkok who are good at singing Indonesian songs uploaded on Instagram and TikTok platforms SindoNews.Com 2023.

Indonesia has laws and regulations related to information technology, namely Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. AI in the Electronic Information and Transactions Law is classified as an electronic system. However, the law does not yet contain a clear description of AI and deepfake crimes. 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. Based on the description that has been described, it is seen that the criminal responsibility of AI who commits deepfake crimes in Indonesia has not been specifically regulated in a regulation or law. Therefore, in this study the formulation of the problem to be discussed is related to the criminal responsibility of artificial intelligence that commits deepfake crimes in Indonesia.

Research Methods

This type of research uses normative juridical research that uses a statutory approach, a conceptual approach, and a comparative approach. The legal materials used are primary legal materials and secondary legal materials that are collected, studied, used to analyze related matters, namely the regulation of artificial intelligence as perpetrators of deepfake crimes. The analysis technique used is prescriptive, which provides guidelines on how to conduct or regulate according to the law that applies to the legal problems faced.

Results and Discussions

Legal Subjects in the Indonesian Criminal Law System

Theoretically, legal subjects who can make legal acts or legal acts and legal subjects contained in Indonesian positive law are humans and legal entities. Every human being is a subject of law and is able to perform legal acts or enter into legal relations that

must be followed by legal capacity and legal authority. The Criminal Code used today still adheres to the understanding that a criminal act can only be committed by humans. Article 59 of the Criminal Code states that "in cases where it is determined that it is criminal to be a violation against the management, members of the governing body or commissioners, the administrator, member of the governing body or commissioner who apparently did not interfere in the violation, shall not be criminalized". The article can be interpreted that criminal acts have never been committed by corporations but are committed by administrators or persons. The Criminal Code only regulates criminal acts committed by people whose responsibilities are also carried out individually (Rahman & Habibulah, 2019).

The fact that these rules are only directed at human beings has a clear reason because only humans can have a mental state, take responsibility for their actions, and be influenced by criminal rules. First of all, only humans have situational awareness and the capacity to possess intentionally and consequently only humans can act deliberately, carelessly, negligently to commit crimes. Second, the punishment of the agent who committed the crime requires that the agent be criminally responsible. Only human beings have the level of reasoning responsiveness necessary to be criminally responsible. Third, since criminal law is intended to prevent undesirable acts, its application presupposes that the intended party may be affected by legal orders and associated sanctions. Since non-human entities cannot appreciate the importance of norms and sanctions, nor the social significance of an undesirable act, their creative behavior, and contention cannot be governed by criminal norms.

Whoever, every person becomes a subject of the law to whom he can be affected by existing laws because of his unlawful acts. That based on the facts revealed in the trial that the defendant as a person who has been charged by the public prosecutor with committing a criminal offense and the confession of the defendant before the public prosecutor that he is physically and mentally healthy and can answer and listen to every question asked to him so that legally the defendant is able to account for his actions. Corporate entities can also be actors in this situation. This is in accordance with Law No. 31 of 1999 concerning the Eradication of Criminal Acts of Corruption, in article 1 paragraph 1 states that a corporation is a collection of people and / or wealth organized both as legal entities and non-legal entities. That is, the corporation has become a subject of law and can therefore be subject to criminal charges. In addition to the anti-corruption law that recognizes legal entities as legal subjects, it is also mentioned in article 1 point 1 of Law Number 40 of 2007 concerning Limited Liability Companies states that a Limited Liability Company hereinafter referred to as the Company is a legal entity that is a capital partnership, established based on an agreement, to carry out business activities with the company's authorized capital which is divided into shares and which meets the requirements as stipulated in this law and its implementing regulations (Sari & Harwika, 2022).

The determination of the corporation as a subject as well as responsible for its motivation must pay attention to the development of the corporation itself. Corporations can only perform acts through the intervention of administrators. Thus, external factors (*auctus reus*) in corporations depend on the relationship between the corporation and its stakeholders. Unlawful acts committed by corporations are always punishable inclusions. In this case the corporation becomes part of the entry of crime. Corporations can be actors but cannot be subjects who have the authority to appoint and tend to violate the law who

should be people such as directors, administrators and so on (Rahman & Habibulah, 2019).

Criminal law embodies the most powerful legal social control in modern civilization. The fear of AI entities is that many cases are based on the fact that AI entities are considered undemanding to the law, especially in criminal law. If the crime is committed because it has no mental capacity, children, animals, then the offender can be presumed innocent because it does not have the mental ability to expressly commit the crime. However, for example, if an innocent person receives an order from someone else, if the owner of the animal orders to attack someone, then the owner can be punished. This can also be analogous to AI that does not have mens rea to be a subject of law but programmers or AI users can be subject to criminal liability if there is a criminal act committed by AI. If AI is activated by someone to commit a crime, for example making a robot a murderer, then the act has fulfilled the element of *auctus reus* because the robot committed the crime of murder and the AI maker must be responsible. There is a legal principle known in the Indonesian penal system, namely *actus non facit reum nisi mens sit re*, meaning that an act becomes guilty, except for guilty reason.

If the legal system chooses to regulate AI crimes specifically, then it can be said that in the legal system, AI crimes are legally relevant. AI crime regulation can impose obligations and responsibilities on humans or on humans as well as AI systems. There are two approaches that can be used to consider crimes committed by AI. According to the first approach, the relevance of AI crime law does not mean that AI systems are subject to criminal law. Humans as users, developers, and disseminators will remain the sole recipients of criminal norms and sanctions. They can be subject to criminal sanctions if they contribute to the criminal behavior of AI systems. They may be required to pay compensation and fines and limit further use of AI systems in connection with bans on implementation, obligations to disable them, or reprogram their components. In the second approach, AI systems will be subject to criminal law, that is, they will be directly affected by legal reactions to crimes committed. The legal reaction can be in the form of actions similar to sanctions against humans (e.g. fines) or in other forms of sanctions (e.g. reprogramming harmful AI systems). This second approach places AI as a legal entity (Lagioia & Sartor, 2020).

In the Electronic Information and Transaction law, AI can be categorized as an electronic system and an electronic agent. An electronic agent is a part of an electronic system created to perform actions on electronic information automatically held by people. The obligations of electronic system operators apply *mutatis mutandis* to electronic agent operators. It can be understood that the law on electronic information and transactions is that an electronic agent or electronic system is a tool. Based on the legal doctrine, an object cannot have the rights and obligations that humans have. This can be interpreted to mean that the electronic information and transaction law sees electronic agents or electronic systems as a tool controlled by humans rather than seeing them as independent legal subjects. An electronic agent is a part of an electronic system that is viewed as a device. Article 6a of the Electronic Information and Transactions Law states that electronic systems are organized by every person, state administrator, business entity, and community that provides, manages, or operates electronic systems either individually or jointly to users of electronic systems for their own needs and the needs of other parties. Based on PP No.71 of 2019, electronic system operators are distinguished in the public sphere and the private sphere. In the public sphere it consists of state administration

agencies while in the private sphere it consists of people, business entities and the community.

In Indonesia's current penal system, AI cannot be executed using criminal law. It is still necessary for a person or legal entity to be responsible in the event of a criminal act that results from it. This responsibility must be borne by the user as well as a legal entity whose responsibility is the director of the company or the head of the foundation. Electronic system users are any person, state operator, business entity and community who utilize goods, services, facilities, or information provided by electronic system operators. However, the person in charge of AI is not limited to its use but there is still an important party that should not be ruled out, namely the creator of AI. This AI creator is the one who makes artificial intelligence used by AI users. The creator of the AI must also be included to be responsible for the legal actions carried out by the AI he created. AI users who are unfamiliar with AI science will be disadvantaged. In this case, in order for there to be legal certainty regarding the accountability of legal actions carried out by AI, the government can form and issue special regulations related to AI that regulate the rights and obligations of the parties, namely AI users and AI creators, and provide limits for parties to AI liability (Lodder et al., 2018).

Humans can manipulate AI to do their bidding with the intention of committing a certain crime. In cases like these, the obvious solution is to hold accountable the person manipulating the AI. This could be a programmer successfully inserting an algorithm designed to shut down into the AI software or an operator instructing the AI software so that it will harm others. After all, AI cannot be thought of as anything other than a tool in the hands of humans. However, the way to take responsibility may differ according to the degree of rigor of the tools the AI has. Like a hammer, by using the tool, the movement of the tool is immediately understood as a human action. Animals, too, are often equated in legal terms with things, which can be manipulated by their masters (although they can never be controlled absolutely like a tool). In the case of animals, we often equate in law that they are manipulated by their masters even though they can never be controlled absolutely, like a tool.

In both instances, it can be considered that humans are perpetrators of criminal acts. Things begin to change when we face the possibility of one human being using another human being as a means to commit evil. For example, when a nurse is tricked into giving poison to a patient and the nurse only thinks about doing her job. In this approach, there is required to be an intermediary where the person understands what is happening or anything. For this theory to make sense into the context of AI, AI must be more sophisticated to have the ability to understand what is going on and choose accordingly if in the end AI is tricked into achieving the desired goals by the actors behind the scenes. Some argue that autonomous vehicles programmed to walk the streets and hit people is a different scenario with drivers manipulating AI cars into thinking of certain people only as objects they can safely hit. Ultimately, it all comes down to whether or not technological advances allow us AI to be human-like enough. At this point, there are also possible cases when the AI performs actions that go beyond its original purpose. For example, autonomous vehicles are programmed to injure humans, but instead kill those humans. In such cases, the end result is something different from what is desired by human beings, and the theory of assigning responsibility based on estimates and the possibility of the actual crime being committed as a consequence of the intended criminal act may prove useful, Criminal liability in these cases comes from accomplices or

instigators when they can and should have predicted the different consequences arising as a possible result of the act which was originally intended (Lima, 2017)

Offenses and crimes are threatened with law which is suffering or torture for the person concerned, in addition to the perpetrator himself, there is also one or several people who participate in the criminal event. Articles 55 of the Criminal Code and 56 of the Criminal Code are rules that regulate the participation of one or more people when others commit a crime. So that someone participates when committing a criminal act can also be responsible, not only someone who commits a criminal act is convicted. From the two articles (Article 55 of the Criminal Code and Article 56 of the Criminal Code), it can be seen that according to the Criminal Code the division of the group of participants for the criminal act of participation, namely those who commit (Pleger Implementers), those who order to do (Influence Makers; Doen Pleger), those who participated in doing (Participating Makers; Medepleger), people who deliberately advocate (Organizer Maker: Uitolkker), and Helper (Medeplichtige). The definition of deelneming is all forms of interference by people together with others in doing actions that result in offense or are prohibited by law. In the case of humans as perpetrators of crimes that use artificial intelligence to commit criminal acts, it can be categorized as a pleger. In that article it is not explained what is included with the intruder, but in memorie van toelichting (explanatory memory) of the Dutch Criminal Code it is stated as follows: "The intruder of criminal acts (doen pleger) is also he who commits criminal acts but not personally, but with the intercession of others, as an instrument in his hands, when the other person acts unintentionally, negligence or responsibility due to circumstances that know, are misled or are subject to violence". So the person who is used as a "tool" in the hands of the perpetrator (doen pleger), must meet certain requirements, namely people without "willfulness, negligence, or responsibility". The person who is legally ordered cannot be blamed or cannot be accounted for.

Criminal Liability of Artificial Intelligence that Commits Deepfake Crimes

The existence of AI has caused a disruptive effect on society. Artificial intelligence systems differ from other ordinary computer algorithms (programs) because of their uniqueness. AI can learn independently, accumulate experience and produce different solutions based on the analysis of various situations independently of the will of the programmer, which is able to operate independently (Ravizki & Yudhantaka, 2022). AI is a computer program that can perform intelligent actions like humans in general. The smart action that comes in is to make decisions and make choices. So, if AI has intelligence like humans and can think like humans, then questions arise such as whether AI can account for its actions in the eyes of the law.

Indonesian criminal law provides limits on the scope of criminal liability not only covering aspects of criminal law but also covering aspects of decency and justice. Criminal responsibility in Indonesia refers to the flow of dualism, which is the understanding that separates criminal acts and their responsibility. The flow of criminal rules is a rule formed and enforced in a country where the rule aims to regulate actions prohibited in criminal law and other acts outside the prohibited act. While the concept of criminal liability regulation is intended as a determinant of whether or not a legal subject is appropriate in imposing a crime against him. Not all acts can be categorized as criminal acts, an act and act that can be said to be a criminal act can be said to be so if it contains unlawful nature and the act contains elements of guilt consisting of intentionality (dolus) and negligence (culpa) (Widiartana & Setyawan, 2023). Crime is the only legal basis for criminal liability. In order for a criminal act to be charged to a person or legal entity, there

must be certain elements such as criminal acts, being able to be responsible, with willfulness or negligence, and the absence of excuse of excuse. The provisions of criminal responsibility in the Indonesian Criminal Code (KUHP) still adhere to the fact that criminal responsibility can only be given to humans (natuurlijke person) and legal entities (rechtspersoon).

AI has helped human life a lot from all aspects. Even the current state of AI has a broad legal impact on society, especially related to legal responsibility, considering that the world today still does not regulate much firmly about who should be responsible if AI commits a crime. To overcome this, there are several things to consider, especially when talking about legal liability. The topic of legal liability becomes quite difficult to discuss because one of them discusses the capacity of legal subjects in being responsible. To find out whether AI is a subject of law or not, conceptually several criteria, namely something that according to law has the right or authority to do legal acts or who has the right and ability to act in law, something that is a supporter of rights who according to law is authorized or has the power to act as a supporter of rights and everything that according to law has rights and obligations.

With regard to criminal liability for artificial intelligence when committing criminal acts, it is necessary to discuss criminal liability first. The concept of criminal responsibility actually does not only concern legal issues, but also concerns issues of moral values or general decency adopted by an organization, community or group in society, this is done so that criminal responsibility is achieved by fulfilling justice. Criminal liability is a form of determining whether a suspect or defendant is held accountable for a criminal act that occurred. In other words, criminal liability is a form that determines whether a person can be convicted or not. The principle of liability in criminal law (geen straf zonder schuld; actus non facit reum nisi mens sir rea) a criminal offence does not apply if there is no fault. Please note that the subject of criminal law applicable in Indonesia is a person and in accordance with the expansion of the subject of criminal law, a legal entity can become a subject of criminal law in Indonesia. Regulations regarding artificial intelligence in Indonesia have not been specifically regulated and formed, therefore interpretation is needed to determine whether artificial intelligence is a legal subject or not in Indonesia (Kurniawan, 2023).

Chairul Huda stated that the basis of a criminal act is the principle of legality while a criminal can be convicted on the basis of guilt, which means that a person will have criminal responsibility if he has committed a wrong act and contrary to the law. Wrongdoing is a major element in criminal liability. When AI commits a criminal act, in this case AI does not understand the meaning of the consequences of the actions it does and AI cannot determine its own will to do an act and AI also has no awareness in taking legal actions.

Humans as legal subjects have absolute consciousness when doing a legal act while AI is a tool created by humans with technology so that consciousness is not contained in AI. Therefore, AI does not have the ability to be a legal subject that can be given responsibility in criminal law. Negligence is the most appropriate model used to assume criminal liability for unintentional actions that occur in the context of programming or use commonly performed by AI, that is, when the agent performs its duties without malfunctioning. Here, the focus turns to the designer or operator to take appropriate action to prevent unintended results that can occur in the usual performance of the AI and that should have been predicted by the programmer or user.

Some experts have developed certain scenarios regarding AI criminal liability. One that is quite widely discussed is the idea of Gabriel Hallevy. The Israeli criminal law professor formulated an AI criminal liability scenario based on elements of *auctus reus* (action) and *mens rea* (condition) (Hallevy, 2018). Hallevy further classified it as follows:

1. *Auctus reus* means that the subject of the law commits an act that is against the law or does not perform an act required by law.
2. *Mens rea* can mean a legal subject who knows or is aware; or those who simply do not know, are unaware, or accidentally.

Based on the classification above, it can be understood that criminal acts committed by AI can appear in three possibilities. First, criminal acts that arise due to the purpose or deliberate purpose of legal subjects in utilizing AI to fight the law. Second, criminal acts that arise due to the purpose or deliberate purpose of legal subjects in utilizing AI not to carry out something required by law. Third, criminal acts that arise due to the negligence of legal subjects in utilizing AI. Hallevy then provided three models of accountability in criminal acts committed by artificial intelligence, namely *preperation-via another model* (PVM), *natural-probable consequence liability model* (NPCLM), and *direct liability model* (DLM).

Perpetration-via another model (PVM)

In this model, AI is considered an agent that does not have the ability to commit criminal acts. In this case, AI is only an instrument, while the parties involved in making and utilizing AI resulting in criminal acts are the real perpetrators. They are the ones who are held accountable for the crime. In this context, the perpetrator could be a programmer who deliberately designed the AI to perform an offensive action in certain situations. Perpetrators can also be owners or users who deliberately use AI for criminal purposes. This approach to accountability is strict liability. That is, criminal liability is assigned without having to assess the existence of elements of guilt or negligence. This is because the perpetrator's deliberate in creating and utilizing AI for unlawful purposes can be considered dangerous to society.

Natural-Probable-Consequence Liability Model (NPCLM)

The NPCLM model focuses on criminal acts that occur due to errors or AI systems that do not work properly. When a robot killed an employee at a motorcycle factory in Japan in 1981. The robot identifies the employee as something that hinders his task, finally the AI system embedded in the robot calculates the action that needs to be done, which is to get rid of the employee by pushing him to the machine that is operating. In relation to such cases, direct criminal liability can be assigned to all parties (owners, designers, or supervisors) if they know about the risks that may arise. They can also be held accountable if they are not aware of the weaknesses of the AI system they use. Proportional liability can also be used if in a criminal act there is a cause and effect that varies from maker to maker.

Direct Liability Model (DLM)

This model treats AI like humans in criminal liability. That is, AI is not considered an innocent agent, but has a certain awareness or mental condition in the occurrence of criminal acts. In short, AI has the ability to be responsible. At first glance, this DLM model seems hard to imagine. Assigning mental attributes to AI is a real challenge in many cases. For example, if a self-driving car travels at a speed faster than the maximum speed requirement required by national law, then AI technology is found to have violated its responsibility. The truth about this approach is a lot of debate. For example, what about violations of responsibility due to errors in software or mistakes made by AI as a result

of self-defense will also be equated with the theory of forgiving reasons based on criminal law. Indeed, giving AI status as a legal subject means involving all parties who have involvement in the planning, manufacturing process, implementation, or owner of the technology who will be held criminally liable regardless of the proportion of the share given.

To be able to impose criminal liability, it is necessary to meet two cumulative components, namely *auctus reus* and *mens rea*. *Auctus reus* is usually understood as a component of an external goal, namely the execution of a violation. It consists of essential elements, the criminal act itself, and circumstances and consequences. *Auctus reus* identifies what to do or not to do. Recent legal doctrines have criticized the traditional view of *auctus reus* as a deliberate body movement. First of all, it has been observed that in fact the nature of *auctus reus* relates to a particular evil in which the act consists of a particular circumstance. In certain circumstances, the defendant may be liable for the actions of third parties.

Two examples of liability are vicarious liability where the employer can be held criminally liable or the acts or omissions of its workers and the doctrine of agency innocence in which primary liability is imposed on manipulators who use innocent parties to commit crimes. According to this *auctus reus* characterization, both AI systems in charge of controlling physical objects (such as robots) or systems that do not have a physical presence (software) can meet the behavioral requirements of *auctus reus*. This is true not only when the performance in question is the result of internal calculations performed by the AI system, but also when the AI system executes instructions given by a human operator.

In deliberate transgression, *mens rea* has two components: cognition and willpower. Cognition is the agent's awareness of factual reality and involves all components of the *auctus reus*. The will consists of the intention to perform actions and achieve results and can never stand alone, always accompanied by awareness. Criminal intent consists of mental processes that are in principle under the control of the offender and can be made conscious. To determine whether an AI system has the intention, it must be focused on its internal structure and function. It should be considered whether the entity has both an internal epistemic state (belief) and a conative state (desire, goal, intention). It can be said that an entity has a goal to realize a result when the entity has such internal conditions. It is more difficult to prove intention than consciousness, because consciousness deals with current or past circumstances, whereas intention includes projections of future states (planned actions from which to have intentions and expected results).

AI criminal liability that can be enforced by Indonesian criminal law is the Perpetration-via another model (PVM) criminal liability model and the Natural-Probable-Consequence Liability Model (NPCLM). The first model, Perpetration-via another model (PVM), artificial intelligence is considered an innocent agent. The law assumes that a machine is a machine and has never been a human being. Based on this model, its capabilities are not enough to consider AI as a perpetrator of violations. This is not enough ability to perceive AI as a perpetrator of violations. His abilities resemble the parallel abilities of people who have parallel limitations, children, or someone who is mentally incompetent or who does not have criminal thoughts. By law, when an offence is committed by an innocent person, such as when a person causes a child, a person who is mentally unstable, or has no criminal thoughts, to commit an offence then that person can be criminally liable as the offender. There are two candidates who can be held criminally liable when AI commits a criminal offense is the device programmer and the second is

the user. This model assumes the *auctus rea* and *mens rea* of programmers and users to commit violations through the instrumental use of AI.

An AI device programmer might design a program to commit a breach through AI. The second person who may be considered the perpetrator is the user. The user does not program the software, but uses AI for his own benefit and benefit. Punish users or creators who intentionally or negligently allow AI systems to develop criminal behavior even when no damage or injury has occurred, for carrying out malicious activities through AI systems that pose a dangerous risk. This result can be obtained by broadening the scope of carelessness so that it can be called opaque carelessness, which is a situation in which the defendant knows that his actions are risky but fails to realize or consciously ignore the risks of the act. In this model, users or programmers of AI systems with awareness that the system may be involved in certain criminal acts and bear criminal responsibility for crimes committed by the AI system.

The second criminal liability model, the Natural-Probable-Consequence Liability Model (NPCLM), assumes deep involvement of programmers or users in the daily activities of AI, but without any intent to commit any offense through AI. The programmer or user had no knowledge of the violation, they did not plan to commit any violation, and they did not participate in any of the violations. For example, when there is a robot or AI software designed to function as an automatic pilot. AI is programmed to help fly planes. During the flight, the human pilot activates autopilot. At some point after autopilot activation, human pilots saw a storm approaching and tried to abort the flight. However, AI considers the actions of human pilots a threat and takes action to eliminate the threat. Perhaps by cutting off the pilot's air supply or activating his ejection seat so as to get the human pilot killed. Of course, the programmers didn't intend to kill anyone but human pilots were killed by AI.

Another example is software designed to detect threats from the internet and protect computer systems. A few days after the device is activated, it is known that the best way to detect such threats is to enter websites that are considered malicious and destroy any software that is recognized as a threat. When the software does this, a computer breach occurs even though the program does not intend to do so. According to the second model, a person may be held liable for a violation, if the violation is a natural and likely consequence of the person's behavior. In this approach, the AI commits a breach while the programmer or user does not know it, does not intend or participate in it. However, it requires that the programmer or user be in a state of negligence. Programmers or users are not required to be aware of every impending criminal act as a result of AI activities, but are required to be aware that such violations are a natural consequence of possible AI actions.

The Direct Liability Model (DLM) model is still not applicable in Indonesia because in criminal law, to impose criminal liability must meet *auctus reus* and *mens rea*. In this case, artificial intelligence has not been able to meet these requirements. Especially in the determination of *mens rea* elements. How the law is able to explain the intention of the AI in doing its wrong. This will be very difficult due to the lack of awareness of AI. In general, self-awareness represents a person's ability to think and make moral judgments, for example judging good and evil. So from an ethical and legal perspective, AI cannot be directly criminally responsible because they are not aware of the consequences of their actions.

The development of AI technologies such as machine learning and deep learning provides new opportunities for criminals to commit new crimes. Deepfake is a genetic

technique of human image using AI technology thinking algorithms. With the help of deepfakes we can rely on data sources consisting of images or videos that are very much processed and studied by AI algorithms to develop and produce new images or videos by mimicking real things. With this explanation, it can be said that the use of deepfakes is a form of use and utilization of a legal object that is controlled or carried out by someone as a legal subject. If deepfake technology is used to portray someone with something bad then this will affect other people's perception of that person.

Deepfakes are a smart cybercrime model where the more digital content and its reproduction, the higher the level of forgery. These deepfakes are used in pornography, the spread of fake news, fraud, manipulation of facts or circumstances, and defamation. Society will increasingly find it difficult to distinguish what is real and what is produced for a crime. If a video spread on the internet is proven to be fake and removed from the internet, it does not rule out the possibility that the video has been downloaded first by someone else without valid consent so that it can violate the law. The highlight of deepfake use is "who" is responsible. There are several groups that can be affected by deepfake abuse, namely deepfake technology providers, platforms that distribute deepfakes, individuals who create deepfakes, people who are harmed, and people who see deepfakes (Liu & Zhang, 2022).

High manipulation of digital content makes deepfakes a real challenge also in criminal justice agencies. The difficult thing here is to determine who is criminally responsible for digital content manipulation behavior, especially if the crime is committed by AI without human intervention and difficult evidence. This deepfake technology is actually just a tool where the ethics of its use depend on who is in control. However, in this case there are several reasons stating that AI can not only engage in deepfake crimes by being aware of the *auctus reus* and *mens rea* required to commit the crime but can also be held responsible for the crime, by having an adequate level of apprehensiveness, namely:

Responsive Reasons

Criminal responsibility presupposes that the perpetrator concerned has adequate responsiveness, i.e. an adequate understanding of relevant knowledge and practices. Criminal law aims to prevent the occurrence of unwanted behavior. To determine whether criminal deterrence also applies to AI systems, it is necessary to consider whether AI can be aware of its interests (or the interests of its owners and users) and how criminal sanctions affect those interests. So, AI that is responsive to criminals must have instrumental rationality, namely having a purpose and the ability to adapt its actions to its objectives by considering the possible consequences of the actions carried out including criminal penalties. AI that has only instrumental rationality is geared towards maximizing its usefulness and to avoid the undesirable. For AI to be sensitive to reason for criminal law purposes, there are three relevant capacities. The first capacity is the ability of AI to gain awareness of their behavior and the resulting impact. The second capacity is AI's ability to identify and understand applicable norms and associated sanctions. The third capacity is AI's moral motivation to comply, which usually results from the ability to internalize a criminal act and emotionally know its guilt.

Smart Compliance and Violations

AI must be responsive to morals and laws while having the capacity to consider legal values and norms. Therefore, AI must also have normative agents who have the ability to represent norms and values, reason, and obey. Normative agents have capacities such as recognizing and inferring norms (learning), conveying norms to other agents

(communication) and imposing laws on other agents if they fail to comply with applicable norms. There are two approaches to normative agent design. In the first approach, norms are statically formed as limitations in their creation so that they cannot violate norms to achieve certain goals. In the second approach, a more flexible creator allows for intelligent violations of norms. For example, a self-driving car that must avoid pedestrians who are crossing. Assume that it is too late for the car to come to a complete stop and eventually the car turns into the opposite lane by crossing the double line of the road. Although this is prohibited in traffic rules, it is a more reasonable option than having to hit pedestrians. A truly intelligent normative agent must have the ability to know that a norm exists, consider this norm in the decision-making of its behavior, and then decide whether to follow that norm in its case and behavior. The development of AI capable of violating norms must be done with extreme caution, it must be designed to allow the application of existing norms only in very limited circumstances.

Currently, Indonesia does not have a specific regulation governing the use of AI in deepfake crimes. Deepfake crimes are considered criminal acts in the realm of the corpse world or cybercrime and its parent is cyberspace. Cyberspace is seen as a world of communication based on computers. Deepfake is a form of illegal content, where the content violates the law and disturbs public order. AI as a perpetrator of deepfake crimes requires a special response under the law because this system is very dangerous not only on the gap of responsibility but the social consequences of AI itself.

In deepfake crimes, the AI criminal liability that can be used is Perpetration-Via another model (PVM). When a crime is committed by an AI it should be considered an innocent agent. So in this case, criminal charges will lead to deepfake technology providers, people who distribute deepfakes, and individuals who create deepfakes. Deepfake programmers or users who produce or manipulate gambar, audio, or video content that closely resembles a person, object, place or entity that is already and appears false to a person must disclose that the content was artificially created or manipulated.

The characteristics of AI that can be likened to electronic systems and electronic agents explicitly make electronic information and transaction laws applicable to AI. In the electronic information and transaction law, it is said that the operator of an electronic agent is the operator of an electronic system, where all rights and obligations of the operator of the electronic system apply *mutatis mutandis* to the operator of the electronic agent. The Electronic Information and Transaction Law also explains that electronic system operators as a form of electronic system utilization can only be carried out by people, state operators, business entities, and the community (Salsabila and others 2023). Regarding accountability by the operation of electronic systems, it is stated in Article 15 of the law on electronic information and transactions which states that: :

1. Each Electronic System Operator must carry out the Electronic System responsibly for the proper operation of the Electronic System,
2. The Electronic System Operator is responsible for the Operation of the Electronic System
3. The provisions referred to in paragraph (2) do not apply in the event that it can be proven that force majeure, error, and/or negligence on the part of the Electronic System user.

Article 15 explains that in order for the electronic system to be carried out correctly, all operators have the obligation to be responsible for every operation of the electronic system they have, so that it can operate smoothly and safely. Electronic system operators also have an obligation to operate each of their Electronic Systems, namely by having to

meet the minimum requirements listed in Article 16, namely a) every information, data, and document presented must be complete without lacking in the slightest, and must also have a period of time as stipulated in the legislation, b) the operator has an obligation to protect authenticity, the integrity and confidentiality of any information contained in their electronic systems, c) able to operate as stated in the procedures and instructions in the electronic system operator, d) facilitate guidance and guidance by completing language, symbols, information that is commonly heard, so that the parties can understand it, e) so that the procedure remains clear and responsible, it must have a continuous mechanism.

In the provisions of Article 38 paragraph (1) of the law on information and electronic transactions which states that anyone can file a lawsuit against the party that organizes the Electronic System or uses information technology that causes losses. Therefore, a person who is a victim can file a claim for compensation, therefore someone (perpetrator) can also be held civilly liable. The operator of the electronic system must be able to take responsibility for the operation of the electronic system. Although this provision does not apply if force majeure, errors or omissions committed by the user of the electronic system can be proven. The law on electronic information and transactions also governs, as long as there is no separate law that provides otherwise. Every party involved in an electronic transaction, is a sender and receiver who can carry out electronic transactions themselves, or by conducting electronic transactions through authorized parties or electronic agents. Thus, the party responsible for all legal disputes from the implementation of electronics is :

1. All legal consequences that occur in electronic transactions will be borne by the party making the transaction
2. If done through a power of attorney, all legal consequences during the implementation of the electronic transaction shall be borne by the power of attorney
3. If carried out through electronic media, all legal consequences of conducting electronic transactions are the responsibility of the organizer of the electronic media
4. If the loss of electronic transactions is caused by the malfunction of the electronic agent due to the actions of third parties who directly target the electronic system, all legal actions are borne by the operator of the electronic agent.

However, if the electronic agent cannot operate due to the negligence of the service user resulting in the loss of electronic transactions, then all legal consequences shall be borne by the service user. This provision does not apply in the event that force majeure, errors or negligence on the part of electronic system users can be proven (Sahib et al., 2023). In Government Regulation No.71 of 2019 concerning Electronic System and Transaction Operators, several obligations and/or requirements must be met by electronic system operators, including: :

1. Electronic system operators have obligations and responsibilities in operating their electronic systems, so that they can operate normally, safely, and reliably.
2. Electronic system operators must be able to guarantee that their electronic systems contain information or documents that are not prohibited by law.
3. The obligations of registered electronic system operators are fulfilled before electronic system users start using electronic systems.
4. Electronic system operators are required to have management practices, operational work methods, and mechanisms to review electronic systems periodically.
5. Require system operators to apply the principles of personal data protection in processing personal data.

6. Electronic system operators are required to provide a guide for users of electronic systems.
7. Electronic system operators are required to provide a guide for users of electronic systems.
8. Electronic system operators are required to provide commensurate functions, in order to match the character of the electronic system used later, expected functions include maintenance and cancellation of orders.

Electronic system operators should obtain permission to operate electronic systems through the issuance of decisions (*beschikking*). This is because in the implementation of the electronic system, permits are needed as a means of control from the government for legal protection for electronic system users, including the public, against violations or crimes related to the use of electronic systems such as cybercrime which covers deepfake crimes.

An artificial intelligence criminal liability model that can be used in deepfake crimes other than PVM is the Natural-Probable-Consequence Liability Model (NPCLM). According to this model, there is a relationship between AI violations and the actions of programmers or users of deepfakes. Even if the programmer or user did not intend to commit the violation, if there is evidence that they could have taken corrective action to prevent the violation but did not do so then they should be held responsible. Criminal liability based on negligence is based on the assumption that none of the programmers or users intended to harm others, so liability arises due to lack of audit and thoroughness in the creation or use of the deepfake application. This is similar to the relationship between the owner and his pet. So deepfake programmers or users must be responsible for negligence related to deepfakes, just as animal owners are responsible for negligence caused by their pets. In this case programmers or users are criminally liable if they fail to warn of foreseeable risks or fail to provide adequate instructions to avoid harm.

In order to effectively enforce law in the future that can anticipate the development of society characterized by the use of AI-based technology, it is necessary to design that can anticipate crime, damage or loss caused by the use or misuse of AI-based technology or due to negligence and error systems that cause losses and victims so that the law can be present in the community. The establishment of specific or specific regulations of AI-based technology, such as on development and application, ethical feasibility, to criminal liability and sanctions, is also needed so that the legal system built can be anticipatory, effective, and responsive so that the law can be present in the midst of developments, dynamics and needs of society.

Conclusion

There are three AI criminal liability models that commit crimes, namely prepetration-via another model (PVM), natural-probable consequence liability model (NPCLM), and direct liability model (DLM). The criminal liability of AI that commits deepfake crimes that can be applied in Indonesia is prepetration-via another model (PVM) and natural-probable consequence liability model (NPCLM). In the PVM model, AI is considered to have no ability to be a violator. So that criminal liability must be carried out by programmers and users. The programmer might design a program to commit infringement through AI whereas the user uses the AI for his own benefit. In the NPCLM model, it focuses on criminal liability involving negligence on the part of the party operating the machine (user) or AI machine that is under the supervision of one party. In Indonesia's current criminal system, AI cannot be processed in criminal law. Criminal

Criminal Liability of Artificial Intelligence That Commits Deepfake Crimes in Indonesia

liability requires that legal subjects must have the ability to be responsible and can willed their actions while AI does not have the ability to be responsible for the actions they commit and also AI cannot expect the possibility of criminal acts committed, so that in the perspective of criminal law AI programmers and users can be held accountable or actions committed because humans are absolute legal subjects in criminal law that has awareness and elements of guilt against actions committed by AI. AI criminal liability from PVM and NPCLM models has not been regulated in Indonesian laws and regulations. Regulation in Indonesia is still limited in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

References

- Budhi, B. J. P. D. I. G. K., Harryarsana, S. I. K., & SH, M. (2021). *Filsafat Hukum*. PT. RajaGrafindo Persada-Rajawali Pers.
- Fahrudin, N. (2018). Penerapan Metode Finite State Machine Pada Game Adventure “Franco”. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 2(1), 446–453.
- Halleve, P. (2018). Dangerous robots–Artificial intelligence vs. human intelligence. *Dangerous Robots–Artificial Intelligence vs. Human Intelligence (February 11, 2018)*.
- Hern, A. (2018). Google’s solution to accidental algorithmic racism: ban gorillas. *The Guardian*, 12.
- Jufri, M. A. A., & Putra, A. K. (2021). Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi. *Uti Possidetis: Journal of International Law*, 2(1), 31–57.
- Kominfo, B. H. K. (2023). Kementerian Komunikasi dan Informatika. *Website Resmi Kementerian Komunikasi dan Informatika RI*. Accessed February, 17.
- Kristo, F. Y. (2016). Menelusuri Asal Usul Lazada. Retrieved Februari, 25, 2018.
- Kurniawan, I. (2023). Analisis Terhadap Artificial Intelligence Sebagai Subjek Hukum Pidana. *Mutiara: Jurnal Ilmiah Multidisiplin Indonesia*, 1(1), 35–44.
- Kusumawardani, Q. D. (2019). *Hukum Progresif Dan Perkembangan Teknologi Kecerdasan Buatan*. *Veritas et Justitia*, 5 (1), 166–190.
- Lagioia, F., & Sartor, G. (2020). Ai systems under criminal law: a legal analysis and a regulatory perspective. *Philosophy & Technology*, 33(3), 433–465.
- Lima, D. (2017). Could AI agents be held criminally liable: artificial intelligence and the challenges for criminal law. *SCL Rev.*, 69, 677.
- Liu, M., & Zhang, X. (2022). Deepfake Technology and Current Legal Status of It. 2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022), 1308–1314.
- Lodder, A. R., Oskamp, A., & Duker, M. J. A. (2018). AI & Criminal Law: Past, Present & Future. *JURIX*.
- Rahman, R. A., & Habibulah, R. (2019). The criminal liability of artificial intelligence: is it plausible to Hitherto Indonesian criminal system? *Legality: Jurnal Ilmiah Hukum*, 27(2), 147–160.
- Ravizki, E. N., & Yudhantaka, L. (2022). Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia. *Notaire*, 5(3).
- Sahib, N. S. M., Idayanti, S., & Rahayu, K. (2023). Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia. *Pancasakti Law Journal (PLJ)*, 1(1), 61–74.
- Sari, A. P., & Harwika, D. M. (2022). Legal Liability of Artificial Intelligence in Perspective of Civil Law in Indonesia. *International Journal of Social Science Research and Review*, 5(2), 57–60.
- Sihombing, E. N. A. M., & Syaputra, M. Y. A. (2020). Implementasi penggunaan kecerdasan buatan dalam pembentukan peraturan daerah. *Jurnal Ilmiah Kebijakan Hukum*, 14(3), 419–434.
- Sinaga, N. A., & Atmoko, D. (2023). Kesiapan Sistem Hukum Indonesia Dalam Transformasi Masyarakat Dari 4.0 Menuju 5.0. *KRTHA BHAYANGKARA*, 17(1), 119–126.
- Sulaiman, Robintan, C. G. (2021). *Hukum Di Era Artificial Intelligence*.
- Suyanto. (2021). *Artificial Intelligence, 3rd edn (Bandung: Infomatika)*.
- Taniady, V., Riwayanti, N. W., Anggraeni, R. P., Ananda, A. A. S., & Disemadi, H. S.

Criminal Liability of Artificial Intelligence That Commits Deepfake Crimes in Indonesia

- (2020). PHK Dan Pandemi Covid-19: Suatu Tinjauan Hukum Berdasarkan Undang-Undang Tentang Ketenagakerjaan Di Indonesia. *Jurnal Yustisiabel*, 4(2), 97–117.
- Widiartana, G., & Setyawan, V. P. (2023). Prospects of Artificial Intelligence Criminal Liability Regulations in Indonesian Criminal Law. *Jurnal Kewarganegaraan*, 7(1), 325–331.
- Zou, M. (2020). ‘Smart Courts’ in China and the Future of Personal Injury Litigation. *China and the Future of Personal Injury Litigation (March 11, 2020)*. *Journal of Personal Injury Law* (forthcoming).