

## **Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia**

**Asri Gresmelian Eurike Hailitik, Wiwik Afifah**

Universitas 17 Agustus 1945 Surabaya, Indonesia

E-mail : [hailitik@gmail.com](mailto:hailitik@gmail.com), [wiwikafifah@untag-sby.ac.id](mailto:wiwikafifah@untag-sby.ac.id)

---

### **KEYWORDS**

artificial intelligence,  
deepfake, Subject Of Law

### **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. Human beings are always trying to create something that will further their activities. Therefore, the development of technology has produced many tools that facilitate human activities and replace human roles 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 and Christy Giovanni 2021).

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 and Habibullah 2019). Artificial intelligence transforms big data and the Internet of Things (IoT) into new wisdom that improves humans' ability to live more meaningful lives (Niru Anita Sinaga and Atmoko, 2023).

The birth of AI 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 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 axioms. 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 human-created technology or system that can mimic human activities and think like a human when performing tasks. Some people translate AI as artificial intelligence, artificial intelligence, artificial intelligence, or artificial intelligence. The purpose of creating artificial intelligence is to support and facilitate human activities. Artificial intelligence work processes can be interpreted as devices or tools that support the work of people 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. For machines to be intelligent and behave like humans, they need knowledge and reasoning abilities. (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 2022). 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 2022).

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 2019). 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 key technologies and recognizes 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 (Kusumawardani 2019). 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 and Adi 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 (Sulaiman and Christy Giovanni 2021).

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 2016).

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 their applications, deepfakes have received a lot of 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. 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 (Ariq and others 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 legal research using legal, conceptual, and comparative approaches. The legal materials used are primary legal materials and secondary legal materials, which are collected, researched and used to analyze related topics, namely the regulation of artificial intelligence as a perpetrator of deepfake crimes. The analytical methods used are prescriptive methods that provide guidelines for implementation or regulation according to the laws applicable to the legal problem.

## **Results and Discussions**

### **Legal Subjects in the Indonesian Criminal Law System**

Theoretically, the legal subjects and entities that can perform legal acts or legal acts under Indonesian positive law are human beings and legal entities. All people are legal subjects and can perform legal acts and enter into legal relationships that require legal capacity and authority. The criminal laws that are still valid today are based on the knowledge that crimes can only be committed by humans. Article 59 of the Penal Code states, "If a violation against a manager, member or committee member of a management organization is deemed punishable, the manager, member or committee member of a management organization clearly did not intervene." Persons involved in the violation

shall not be punished." This clause can be interpreted to mean that the criminal act was not committed by the corporation, but by the manager or the individual. Criminal law only regulates crimes committed by individuals or persons performing their duties (Rahman and Habibulah 2019).

There is a clear reason why these rules are only intended for humans. Because only humans have mental states, are responsible for their actions, and can be influenced by criminal law rules. First, since only humans have the capacity for situational awareness and the ability to intentionally possess, only humans can commit crimes intentionally, negligently, or negligently. Second, in order to punish an agent who commits a crime, that agent must be held criminally responsible. Only humans have the level of reasoning required to incur criminal liability. Third, because criminal law aims to prevent undesirable conduct, it presupposes that affected parties may be subject to court orders and associated sanctions. Because non-human beings are unable to assess the meaning of norms and sanctions, or the social significance of undesirable acts, their creative behavior and engagement cannot be regulated by criminal norms.

Any person, no matter who he or she is, can be a legal subject and be subject to current laws for illegal activities. This is a case in which the defendant is accused by the prosecutor of having committed a crime, and the defendant confessed to the prosecutor that he is physically and mentally healthy and is able to answer any questions. This is based on the facts revealed. His questions were aimed at allowing the defendant to legally explain his actions. Companies can also be actors in this situation. This is based on his Law No.31 of 1999 on the eradication of criminal acts of corruption. Article 1(1) states that a corporation is a collection of persons and/or assets organized both as a legal person and as an unincorporated person. This means that the company has become a legal entity and therefore can be prosecuted. In addition to the Anti-Corruption Law, which recognizes legal entities as legal entities, Article 1, Paragraph 1 of Law No. 40 of 2007 on Limited Liability Companies also provides that a limited liability company (hereinafter referred to as a "company") may A capital company established, whose business activities are carried out by dividing the authorized capital of the company into shares, meeting the requirements established by this Law and its implementing regulations (Puspita Sari and Harwika 2022).

The determination of the enterprise as an actor and as one responsible for its motives must pay attention to the development of the enterprise itself. Companies can only take action through administrator intervention. Therefore, external factors (*auctus reus*) in a company depend on the relationship between the company and its stakeholders. Illegal conduct by a company is always a criminal offense. In this case, the company will also be complicit in the criminal offense. Although a corporation is an entity, it is not an entity with the power to appoint persons such as directors and managers, so it tends to violate the law (Rahman and Habibulah 2019).

Criminal law embodies modern civilization's most powerful legal social control. The concern about AI entities is that many cases are based on the fact that AI entities are not thought to have a claim on the law, especially criminal law. If a crime is committed because of a lack of mental capacity, such as a child or an animal, the perpetrator can be considered innocent because he clearly lacks the mental capacity to commit the crime. But if, for example, an innocent person receives orders from another person and the owner of the animal orders the animal to attack someone, the owner may be punished. This is similar to AI, which has no legal subject matter, but if a criminal act is committed by the AI, programmers and AI users can be prosecuted. If an AI is activated by someone to

commit a crime, such as turning a robot into a murderer, then the robot commits the crime of murder and the AI maker must be held responsible for it, making the act *autus reus*. This means that the elements are met. Indonesia's criminal law has the legal principle "*actus non facit reum nisi men sit re*", which means that an act is guilty unless there is a reason for it to be guilty.

AI crimes can be said to be legally relevant in a legal system if the legal system decides to specifically regulate AI crimes. Regulating AI crimes can impose duties and responsibilities on humans or AI systems. There are two approaches that can be used to explain AI-driven crimes. According to the first approach, the relevance of AI criminal law does not mean that AI systems are subject to criminal law. People as users, developers, and disseminators remain the sole recipients of criminal law norms and sanctions. If an AI system contributes to a criminal act, it can be prosecuted. In connection with the prohibition of implementation, the obligation to deactivate or reprogram components, payment of damages and fines, as well as restrictions on the further use of his AI system, may be required. In the second approach, AI systems are subject to criminal law and are therefore directly affected by legal responses to crimes committed. Legal responses may take the form of sanctions-like actions against people (e.g., fines) or other forms of sanctions (e.g., reprogramming harmful AI systems). This second approach of his represents AI as a legal entity (Lagioia and Sartor 2020).

Under the Electronic Information Transactions Act, AI is classified as electronic systems and electronic agents. An electronic agent is a part of an electronic system designed to perform actions on electronic information automatically stored by individuals. The obligations of operators of electronic systems also apply *mutatis mutandis* to operators of electronic agents. It is understood that the Electronic Information and Transactions Act states that an electronic agent or system is a tool. Based on legal doctrine, objects cannot have the rights and duties that humans have. This can be interpreted to mean that the Electronic Information and Transactions Act views electronic agents or electronic systems not as legal subjects in their own right, but as tools to be controlled by humans. An electronic agent is a part of an electronic system that is considered a device. Article 6a of the Electronic Information and Transactions Act states that an electronic system shall be used by individuals, state administrators, economic organizations and It stipulates that it is organized by the community. Based on PP No. 71 of 2019, a distinction is made between operators of electronic systems in the public and private sectors. The public sector consists of government agencies, while the private sector consists of people, businesses, and communities.

Under Indonesia's current criminal law system, AI cannot be criminally executed. It is still necessary for a natural or legal person to be liable for the resulting crime. This responsibility must be borne by both the user and the legal entity, and the person responsible for the legal entity is the company's managing director or the head of the foundation. Users of electronic systems are all individuals, government operators, businesses, and communities that use the goods, services, facilities, or information provided by operators of electronic systems. However, the person responsible for AI is not limited to its use; there is still an important entity, the creator of AI, that must not be excluded. This AI creator is someone who provides artificial intelligence to AI users. Creators of AI will also need to be involved to be held accountable for legal actions taken by the AI they create. AI users who are new to AI science are at a disadvantage. In this case, in order to ensure legal certainty regarding accountability for legal actions taken by AI, governments should regulate and establish the rights and obligations of the

parties. AI users and their AI creators, in specific AI-related May adopt and promulgate regulations. Set party limits on AI liability (Lodder and others, 2022).

Humans can manipulate AI to follow their commands to carry out specific crimes. In cases like this, the obvious solution is to hold those operating the AI accountable. This could result in a programmer successfully injecting his algorithm into the AI software, or an operator instructing the AI software to harm others. After all, AI cannot be imagined as anything other than a tool in human hands. However, responsibility may vary depending on the level of accuracy of the AI tool. Like a hammer, when you use a tool, the movement of the tool is immediately understood as a human action. Animals are also often legally considered to be things that can be manipulated by their masters (although they cannot be completely controlled like tools). In the case of animals, we legally consider them to be manipulated by their masters, even though they cannot be completely controlled like tools.

In both cases, we can assume that people are the perpetrators of the crime. Things begin to change when one human being is faced with the possibility of using another human being as an instrument of evil. For example, suppose a nurse is tricked into giving a patient a poison, and the nurse is only concerned about doing her job. This approach requires the presence of an intermediary who understands the person, what is going on, etc. For this theory to make sense in the context of AI, we need to understand what is going on and properly understand whether the AI ends up being tricked by behind-the-scenes actors into achieving the desired goal. AI needs to become more sophisticated to be able to make decisions. 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 (Lina and Lima 2018).

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 is having a devastating impact on society. Artificial intelligence systems differ from other ordinary computer algorithms (programs) due to their uniqueness. AI can learn independently, gain experience, generate different solutions based on the analysis of different situations, and can act independently, regardless of the will of the programmer (Ravizki and Lintang Yudhantaka 2022). AI is a computer program that can perform intelligent actions similar to a typical human. The wise move for now is to make a decision. Therefore, if AI has human-like intelligence and can think like humans, the question arises: can AI be held accountable for its actions under the law.

Indonesia's criminal law sets limits on the scope of criminal liability and covers not only aspects of criminal law, but also aspects of decency and justice. Criminal responsibility in Indonesia refers to dualism, an understanding that separates the criminal act and its responsibility. The flow of criminal law is the rules established and enforced in a country for the purpose of regulating acts prohibited by criminal law and acts other than prohibited acts. On the other hand, the concept of criminal liability regulation is intended as a factor in determining whether a legal entity can impose a crime. Not all acts can be classified as criminal offenses. An act can be called a crime if it is of an illegal nature and the act contains elements of guilt consisting of intentionality (*dolus*) and negligence (*culpa*) (Widiartana and 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. Conceptually, determining whether AI is subject to law requires several criteria. That is, something that has the right or authority to do a legal act in accordance with the law, or that has the right and capacity to act legally, it is the defender of rights who is authorized or authorized by the law to act as the defender of rights, and all who have rights and obligations according to the law.

Regarding criminal liability in the event that artificial intelligence commits a crime, it is first necessary to clarify the issue of criminal liability. The concept of criminal

liability actually concerns not only legal issues, but also questions of the moral values and common sense adopted by an organization, community, or group of society. This is done to fulfill criminal responsibility through the fulfillment of justice. Criminal liability is a form of determining whether a suspect or defendant is responsible for a crime committed. In other words, criminal liability is the form that determines whether a person can be convicted of a crime. The principle of liability in criminal law (*geen straf zonder guilty, actus non facit reum nisi men sir rea*) does not apply in cases where there is no fault. It should be noted that the subjects of the criminal law enforced in Indonesia are individuals, and as the scope of the criminal law expands, legal entities may become subjects of the criminal law in Indonesia. In Indonesia, regulations regarding artificial intelligence are not specifically regulated and developed. Therefore, interpretation is required to determine whether artificial intelligence is subject to Indonesian law (Kurniawan 2023).

Chairman Koda said that while the basis of criminal acts is the principle of legality, criminals can be sentenced based on their guilt, meaning that if they commit an illegal and violation act, they will not be held criminally responsible. I explained that I would be exposed. Misconduct is an important part of 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 *actus reus* (action) and *mens rea* (condition) (Hallevy 2018). Hallevy further classified it as follows :

1. *Actus 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 *perpetration-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 acts or omissions of an employer or its employees may lead to criminal liability, and vicarious liability, where an operator who takes advantage of an innocent party to commit a crime is primarily responsible. It is the principle of innocence. According to this characterization of *Auctus*

Reus, both AI systems responsible for controlling physical objects (such as robots) and systems that are not physically present (software) can meet the operational requirements of Auctus Reus. This is true not only when the performance in question is the result of internal calculations by the AI system, but also when the AI system carries out instructions from a human operator.

In the case of willful violation, the realm of men consists of two elements: knowledge and will. Perception is an agent's perception of actual reality and includes all elements of auctus reus. Will consists of the intention to perform an action and achieve a result, and it never exists alone and is always accompanied by consciousness. Criminal intent basically refers to a psychological process that is under the perpetrator's control and can be made conscious. To determine whether an AI system has intent, we need to focus on its internal structure and functionality. We need to consider whether an entity has both internal epistemic states (beliefs) and positive states (desires, goals, intentions). If an entity has such internal conditions, it can be said to have a goal of achieving a result. Intention is more difficult to prove than consciousness because consciousness deals with current or past situations, whereas intention involves the prediction of future states (planned actions from which intentions and expected outcomes can be inferred) is.

The criminal liability of AI that can be enforced through Indonesian criminal law is the Alternative Offender Model (PVM) and the Naturally Occurring Consequential Liability Model (NPCLM). The first model, Perpetration – than the alternative model (PVM), considers artificial intelligence to be an innocent actor. The law assumes that machines are machines and never humans. Based on this model, that functionality is not sufficient to consider AI as the perpetrator of a violation. This ability is not sufficient to recognize an AI as the perpetrator of a violation. His abilities are similar to the parallel abilities of people with similar limitations, children, or those who are mentally incompetent or do not have criminal thoughts. According to the law, if an innocent person commits a crime, such as when a child, a mentally unstable person, or a person without criminal thoughts commits a crime, that person may be held criminally responsible: There is a possibility that the He becomes the perpetrator. He has two candidates who will be held criminally responsible if an AI commits a crime. One is the programmer of the device and the other is the user. This model assumes that programmers and users commit violations through the instrumental use of AI.

AI device programmers can use AI to design programs that commit violations. The second most problematic perpetrator is the user. The user does not program the software, but uses his AI for his own benefit and advantage. By engaging in malicious activities that create a dangerous risk through the AI system, even when no harm or injury occurs, he or she intentionally or negligently authorizes the AI system to commit criminal acts. I will punish you. This result can be achieved by widening the scope of negligence so that it can be described as opaque negligence. This is a situation in which the defendant knows that his or her actions are dangerous, but does not realize or consciously ignores the dangers of that action. In this model, the user or programmer of an AI system is aware that the system may be involved in certain crimes and may be held criminally responsible for crimes committed by the AI system. .

The second criminal liability model, the Naturally Occurring Consequences Liability Model (NPCLM), assumes that there is no intent to commit a crime through the AI, and that there is strong programmer or user involvement in the AI's daily activities. The programmer or user had no knowledge of, did not intend to commit, or participated in the violation. For example, if you have a robot or AI software that acts as an autopilot.

AI is programmed to help planes fly. During flight, a human pilot activates the autopilot. At some point after the autopilot activated, the human pilot noticed a storm approaching and attempted 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 Internet threats and protect computer systems. After a few days of activating your device, you learn that the best way to detect such threats is to visit websites that have been classified as malicious and destroy any software that is detected as a threat. It is being When software does this, a computer compromise occurs, even if Permogram did not intend this to happen. In the second model, a person can be held responsible for a violation if the violation is a natural and possible consequence of that person's actions. In this approach, the AI commits violations without the knowledge, intention, or participation of the programmer or user. However, it assumes that the programmer or user is careless. Programmers and users do not need to be aware of all impending crimes due to AI activity, but they should be aware that such violations are a natural consequence of possible AI activity.

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 lack of awareness about AI. In general, self-awareness refers to the ability to think and make moral judgments, such as judgments of right and wrong. From an ethical and legal perspective, AI is not aware of the consequences of its actions and therefore cannot be directly held criminally responsible.

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 and Zhang 2023).

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 crime deterrence also applies to AI systems, we need to consider whether the AI is capable of recognizing its interests (or those of its owners or users) and how criminal sanctions affect these interests. You need to consider whether to give. 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. To determine whether crime deterrence also applies to AI systems, we need to consider whether the AI is capable of recognizing its interests (or those of its owners or users) and how criminal sanctions affect these interests. You need to consider whether to give.

#### **Smart Compliance and Violations**

AI needs to respond to morals and laws, taking into account legal values and norms. Therefore, AI also requires a normative agent that can express, reason about, and follow norms and values. Normative actors have the ability to recognize and derive norms (learning), transmit norms to other actors (communication), and impose laws on other actors who do not comply with applicable norms. He has two approaches to the design of normative agents. In the first approach, norms are formed statically as constraints at the time of creation, so they cannot be violated to achieve a particular goal. In the second approach, more flexible authors enable intelligent violations of norms. For example, a self-driving car that must avoid pedestrians crossing the street. Suppose the car is too slow to come to a complete stop, and the car ends up crossing the double line in the road and turning into oncoming traffic. Although this is prohibited by traffic rules, it is a wiser choice than hitting a pedestrian. A truly intelligent normative agent must be able to recognize that a norm exists, take that norm into account when deciding to act, and then decide whether to follow that norm in her own cases and actions not. The development of AI that has the potential to violate norms must be done with great care and designed in such a way that existing norms can only be applied 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. A deepfake programmer or user who creates or manipulates grammatical, audio, or video content that closely resembles a person, object, place, or entity that is already false and appears false to a human being is a deepfake. You must disclose that it has been manipulated.

The characteristics of AI that make it comparable to electronic systems and agents make electronic information and transactions law clearly applicable to AI. The Electronic Information and Business Act provides that the operator of an electronic agent is the operator of the electronic system, and 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 Transactions Act states that the operation of electronic systems as a form of use may only be carried out by individuals, government operators, businesses, and communities (Salsabila and others 2023). Regarding responsibilities in the operation of electronic systems, Article 15 of the Electronic Information and Transactions Law stipulates as follows:

1. Each electronic system operator must operate the electronic system responsibly to ensure 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) shall not apply if force majeure, negligence or negligence on the part of the operator of the electronic system part of the electronic system user is proven.

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.

Article 38, Paragraph 1 of the Electronic Information Transaction Law provides that any person may file a lawsuit against a party who has organized an electronic system or used information technology to cause a loss. Therefore, the victim can claim compensation for damages, and someone (the perpetrator) may also be held civilly liable. Electronic system operators must be able to assume responsibility for the operation of the electronic system. However, this provision shall not apply in cases where force majeure, errors or omissions on the part of the user of the electronic system can be proven. Additionally, the Electronic Information Transactions Act applies unless otherwise provided by another law. 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 arising from electronic transactions are borne by the person executing the transaction.
2. When conducting electronic transactions, all legal consequences of performing electronic transactions are the responsibility of the organizer of the electronic media.
3. If the loss in an electronic transaction is caused by a malfunction of the electronic agent due to the actions of a third party directly aimed at the electronic system, all legal proceedings are carried out at the expense of the operator of the electronic means .

However, if the electronic agent is unable to function due to the service user's negligence and the electronic transaction is lost as a result, the service user will bear all legal responsibility. This provision shall not apply in cases where force majeure, negligence or negligence on the part of the user of the electronic system can be proven (Salsabila and others 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 the registered electronic system operator are fulfilled before the electronic system user starts using the electronic system.
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. Operators of electronic systems are obliged to provide guidelines to 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 for deepfake crimes other than PVM is the Natural-Probable-Consequence Liability Model (NPCLM). According to this model, there is a link between AI violations and the actions of programmers or deepfake users. Even if a programmer or user did not intend to commit a violation, he or she may be held liable if there is evidence that he or she could have taken corrective action to prevent the violation and failed to do so. Criminal liability based on negligence is based on the assumption that neither the programmer nor the user intended to harm others. Therefore, liability arises due to a lack of testing and thoroughness when creating or using deepfake applications. This is similar to the



relationship between an owner and a pet. Therefore, just as pet owners are responsible for the negligence caused by their pets, deepfake programmers or users must also be held liable for the negligence associated with deepfakes. In this case, a programmer or user commits a criminal offense if he or she fails to warn of a foreseeable risk or to provide sufficient instructions to prevent damage.

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 models for criminal liability when committing a crime: the Prepertration-via-other Model (PVM), the Natural Probable Consequential Liability Model (NPCLM), and the Direct Liability Model (DLM). The criminal liability of AIs who commit deepfake crimes applicable in Indonesia are Prevention by Alternative Model (PVM) and Naturally Occurring 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 liability requires that a legal entity must have the capacity and intention for their actions, but AIs do not have the capacity to be responsible for the actions they commit, and They also do not have the ability to commit criminal acts. As such, humans are absolute legal subjects in criminal law, and since there is an element of consciousness and guilt for acts committed by AI, AI programmers and users can be held responsible for their acts from a criminal law perspective. Criminal liability for AI under the PVM and NPCLM models is not regulated by Indonesian laws and regulations. Regulation in Indonesia remains limited by Law No. 19 of 2016 amending Law No. 11 of 2008 on Electronic Information and Electronic Transactions.

## References

- Ariq, Muhammad, Abir Jufri, and ; Akbar Kurnia. 2021. 'Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi', *Journal of International Law*, 2.1: 31–57
- Budhi, I Gusti Kade. 2022. *ARTIFICIAL INTELLIGENCE : KONSEP, POTENSI MASALAH, HINGGA PERTANGGUNGJAWABAN PIDANA* (Depok: PT Rajagrafindo Persada)
- Fahrudin, Naiman. 2018. *PENERAPAN METODE FINITE STATE MACHINE PADA GAME ADVENTURE 'FRANCO'*, *Jurnal Mahasiswa Teknik Informatika*, II
- Halleve, Prof. Gabriel. 2018. 'Dangerous Robots Artificial Intelligence vs. Human Intelligence', *SSRN Electronic Journal* (Elsevier BV) <<https://doi.org/10.2139/ssrn.3121905>>
- Hern, Alex. 2018. 'Google's Solution to Accidental Algorithmic Racism: Ban Gorillas', *The Guardian* <<https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people>> [accessed 1 August 2023]
- Kominfo. 2016. 'Selama 2016, 300 Akun Medsos Penyebar Hoax Diblokir Polisi', *Kementerian Komunikasi Dan Informatika* <[https://www.kominfo.go.id/content/detail/8640/selama-2016-300-akun-medsos-penyebar-hoax-diblokir-polisi/0/sorotan\\_media](https://www.kominfo.go.id/content/detail/8640/selama-2016-300-akun-medsos-penyebar-hoax-diblokir-polisi/0/sorotan_media)> [accessed 1 August 2023]
- Kristo, Fino Yurio. 2016. 'Tay, Robot Twitter Rasis Yang Bikin Malu Microsoft', *Detikinet* <<https://inet.detik.com/cyberlife/d-3174763/tay-robot-twitter-rasis-yang-bikin-malu-microsoft>> [accessed 2 August 2023]
- Kurniawan, Itok Dwi. 2023. *Analisis Terhadap Artificial Intelligence Sebagai Subjek Hukum Pidana*, *Mutiara Jurnal Ilmiah Multidisiplin Indonesia*, 1 <<https://jurnal.tiga-mutiara.com/index.php/jimi/index>>
- Kusumawardani, Qur'ani Dewi. 2019. 'HUKUM PROGRESIF DAN PERKEMBANGAN TEKNOLOGI KECERDASAN BUATAN', *Veritas et Justitia*, 5.1 (Veritas et Justitia): 166–90 <<https://doi.org/10.25123/vej.3270>>
- Lagioia, Francesca, and Giovanni Sartor. 2020. 'AI Systems Under Criminal Law: A Legal Analysis and a Regulatory Perspective', *Philosophy and Technology*, 33.3 (Springer): 433–65 <<https://doi.org/10.1007/s13347-019-00362-x>>
- Lina, Dafni, and Dafni Lima. 2018. *Could AI Agents Be Held Criminally Liable: Artificial Intelligence Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law and the Challenges for Criminal Law COULD AT AGENTS BE HELD CRIMINALLY LIABLE? ARTIFICIAL INTELLIGENCE AND THE CHALLENGES FOR CRIMINAL LAW*, *South Carolina Law Review*, LXIX <<https://scholarcommons.sc.edu/sclr>>
- Liu, Min, and Xijin Zhang. 2023. '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), pp. 1308–14 <[https://doi.org/10.2991/978-94-6463-040-4\\_194](https://doi.org/10.2991/978-94-6463-040-4_194)>
- Lodder, Arno R, Anja Oskamp, and Marius J A Duker. 2022. *AI & Criminal Law : Past, Present & Future* <<http://www.rechten.vu.nl/~lodder>>
- Niru Anita Sinaga, and Dwi Atmoko. 2023. 'Kesiapan Sistem Hukum Indonesia Dalam Transformasi Masyarakat Dari 4.0 Menuju 5.0', *KRTHA BHAYANGKARA*, 17.1 (Universitas Bhayangkara Jakarta Raya): 119–26 <<https://doi.org/10.31599/krtha.v17i1.2111>>

- Puspita Sari, Amelia, and Dara Manista Harwika. 2022. 'Legal Liability of Artificial Intelligence in Perspective of Civil Law in Indonesia', *International Journal of Social Science Research and Review*, 5.2 (International Journal of Social Science Research and Review): 57–60 <<https://doi.org/10.47814/ijssrr.v5i2.191>>
- Rahman, Rofi Aulia, and Rizki Habibulah. 2019. 'The Criminal Liability Of Artificial Intelligence : Is It Plausible To Hitherto Indonesian Criminal System?', *Legality : Jurnal Ilmiah Hukum*, 27.2: 147 <<https://doi.org/10.22219/jihl.v27i2.10153>>
- Ravizki, Eka Nanda, and Lintang Yudhantaka. 2022. 'Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual Dan Tantangan Pengaturan Di Indonesia', *Notaire*, 5.3 (Universitas Airlangga): 351–76 <<https://doi.org/10.20473/ntr.v5i3.39063>>
- Salsabila, Nathania, Marikar Sahib, Soesi Idayanti, and Kanti Rahayu. 2023. *Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia Article*
- Sihombing, Eka NAM, and Muhammad Yusrizal Adi Syaputra. 2020. 'Implementasi Penggunaan Kecerdasan Buatan Dalam Pembentukan Peraturan Daerah', *Jurnal Ilmiah Kebijakan Hukum*, 14.3 (Badan Penelitian dan Pengembangan Hukum dan HAM): 419 <<https://doi.org/10.30641/kebijakan.2020.v14.419-434>>
- SindoNews.Com. 2023. 'Awat, Penipuan Suara Dengan Kecerdasan Buatan Mengintai, Kenali Bahayanya' <<https://tekno.sindonews.com/read/1086049/207/awat-penipuan-suara-dengan-kecerdasan-buatan-mengintai-kenali-bahayanya-1682996724>> [accessed 14 September 2023]
- Sulaiman, Robintan, and Christy Giovanni. 2021. *Hukum Di Era Artificial Intelligence*, 1st edn (Robin Sulaiman & Partners)
- Suyanto. 2021. *Artificial Intelligence*, 3rd edn (Bandung: Infomatika)
- Taniady, Vicko. 2019. 'Revolusi Industri 4.0 Dalam Sistem Peradilan: Tanpa Hakim Dan Advokat?', *KawanHukum.Id* <<https://kawanhukum.id/sistem-peradilan-tanpa-hakim-dan-advokat/>> [accessed 1 August 2023]
- The Jakarta Post. 2020. 'UGM Receives Orders for GeNoSe Covid-19 Detector', *The Jakarta Post* <<https://www.thejakartapost.com/news/2020/12/29/ugm-receives-orders-for-genose-covid-19-detector.html>> [accessed 1 August 2023]
- Widiartana, Gregorius, and Vincentius Patria Setyawan. 2023. 'Prospects of Artificial Intelligence Criminal Liability Regulations in Indonesian Criminal Law', *Jurnal Kewarganegaraan*, 7.1
- Zou, Mimi. 2020. 'Smart Courts' in China and the Future of Personal Injury Litigation <<https://ssrn.com/abstract=3552895>>