EAEBJOL
Ex Aequo Et Bono Journal of Law
EAEBJOL 2(2): 96-107
ISSN 3024-983X

Institute for Advanced Science, Social and Sustainable Future
MORALITY BEFORE KNOWLEDGE

Exploring the potential crimes and legal liability of artificial intelligence within the framework of Indonesian criminal law

Adria Fathan Mahmuda[1], Mahesa Cakra Gusti[1,*], Faruq Anrusfi[1]
[1] *Law Study Program, Faculty of Law, Andalas University, Padang City, West Sumatra 25163, Indonesia.*
*Correspondence: mahesacakragusti31@gmail.com

Received Date: December 9, 2024 Revised Date: January 22, 2025 Accepted Date: January 29, 2025

ABSTRACT

Background: This research examines the potential criminal offenses that can be committed by Artificial Intelligence (AI) and the implications of criminal law liability for them in the context of Indonesian law. AI, which is increasingly developing with its autonomous capabilities, has the potential to result in new criminal offenses that have not been fully anticipated by the existing legal system. Potential AI crimes, such as deepfakes and criminal offenses by autonomous vehicles, represent a significant threat to public safety and privacy. While some developed countries have begun to regulate the use of AI, Indonesia does not yet have specific regulations governing AI and its potential threats. **Method:** This research uses a juridical-normative method with conceptual, case, and statutory approaches, to analyze the concept of criminal liability in AI crimes. **Findings:** By considering legal doctrines, this research proposes that responsibility for the actions of AI, which cannot yet be considered an independent legal subject, should be transferred to humans as developers or users through the doctrines of *in loco parentis* and Vicarious Liability. Through this approach, AI is treated as a human-controlled tool, so legal liability remains with the entity that has direct control. **Conclusion:** This study expects proactive steps from the Indonesian government to develop clear regulations on AI, to ensure the protection of the public from the risks posed by AI. The regulation should be able to accommodate the rapid development of technology while educating the public on the risks of AI. **Novelty/Originality of this Study:** This research highlights the absence of specific AI regulations in Indonesia and offers a legal framework by applying the doctrines of *in loco parentis* and Vicarious Liability to AI-related offenses. It provides a new perspective on assigning liability in AI crimes, ensuring that responsibility remains with human actors while addressing the legal gaps in Indonesia's regulatory framework.

KEYWORDS: criminal act; criminal liability; artificial intelligence.

1. Introduction

In terminology, Artificial Intelligence (hereinafter referred to as AI) is a "machine" or "software" that has the ability to do everything that is considered to require intelligence or a human-like brain performance system when operating it. The existence of AI in the technological world order raises a debate that presents pros and cons. It is possible that this AI can become a double-edged coin, in one side intended to help human performance but the other side causing problem. For example, AI programmed to carry out a task can unexpectedly perform actions that violate the law or are even dangerous to society (Bostrom, 2014).

Artificial Intelligence (AI) began its presence in the early 1950s by Alan Turing and John McCarthy (Qurrahman et al., 2024). The revival of AI began in the 1990s. On February 10,

Cite This Article:
Mahmuda, A. F., Gusti, M. C., & Anrusfi, M. F. (2025). Exploring the potential crimes and legal liability of artificial intelligence within the framework of Indonesian criminal law. *Ex Aequo Et Bono Journal of Law, 2*(2), 96-107. https://doi.org/10.61511/eaebjol.v2i2.2025.1385

1996, an AI named Deepblue beat the world champion named Garry Kasparov (Pohan et al., 2023). In the 2000s, advances in AI continued to grow rapidly. AI solving the problems like natural language processing, face recognition, and computer vision. These days, AI already has various forms, such as social media algorithms, visual design, music production, problem solving, and other forms of problem solving.

The era that we live right now is the era where AI helps human life in almost every sector. Based on data from the website data.goodstats.id, Indonesia is the third-ranked country of ten countries that the most accessing AI in the world, from September 2022 to August 2023. Indonesia recorded 1.4 million visits to popular AI applications in that period. According to Goodstats that ChatGPT was the most popular AI platform used by 14 billion or 60% of the total traffic found by research analysts (Rasyid, 2024). That numbers showed us, at least, have proven how massive the use of AI is currently in Indonesia.

Referring to the dominance of AI in Indonesia, it really feels unequal with the rationalization of rule making. Untill this day, not a single regulation has been made to detail the AI phenomenon. Developed countries, which are better prepared to face global challenges, have actually prepared clear regulations as a preventive measure against the development of AI. International conention such as the United Nations Convention about the Use of Electronic Communications in International Contracts have recognized the importance of establishing the parties responsible for AI actions, which can be users, developers, or other entities involved (Carr & Goldby, 2011).

The Council of Europe's Framework Convention on Artificial Intelligence is the first legally binding international treaty that examines and establishes the types of requirements for the formulation of future AI laws within the jurisdiction of the initiating countries, such as the European Union, the United States, the United Kingdom, and others. The Convention emphasizes governance requirements with the burden of compliance placed on the developer (Sentinella, 2024).

Some countries have formulated regulations to control the use of Artificial Intelligence (AI) to protect basic rights and public safety. In the United States, the White House issued a "Blueprint for an AI Bill of Rights" in October 2022, which regulates AI privacy protection, transparency, and accountability, with California introducing the "California AI Transparency Act" for further oversight (Plotinsky & Cinelli, 2024). The UK released the "AI White Paper" in March 2023, setting out principles such as safety, fairness, and accountability, with oversight responsibilities divided among several regulators (Chamberlain, 2024). Meanwhile, the European Union pioneered by passing the "Artificial Intelligence Act" in March 2024, which prohibits the use of malicious AI and requires transparency and product testing before launch. The EU, has passed several resolutions and proposals to regulate liability for damage caused by AI, including the use of the concept of strict liability to cover legal loopholes in the event of accidents involving autonomous AI systems.

In criminal law, the discussion of AI liability focuses on determining who should be held responsible for AI actions, given that AI has no awareness or intention (mens rea). The Perpetration-by-Another liability model views AI as a tool used by humans, so criminal responsibility rests entirely with the individual or entity that programs, operates, or uses it.

Complexity arises when AI actions cannot be directly attributed to the intent or control of a specific individual because AI can make independent decisions. That situation make a difficult to determine liability, so some countries are considering a risk-based liability approach, where liability is imposed on the developer or user who commercially benefits from the AI, without considering intent or direct control over its actions (Henz, 2021).

The development of criminal act over time shows adaptation to social, economic, cultural and especially technological changes. Initially, criminal act only included conventional act, such as theft, robbery, or physical violence. However, with modernization, and especially globalization, criminal acts have experience significant changes. Crimes that were previously limited to direct interactions between perpetrators and victims have now begun to expand into more complex domains, such as economic crime, environmental crime, and cybercrime (Patel, 2015). This transformation is in line with technological

developments, which expand the scope and modus operandi of criminal acts. For example, cybercrime and AI automated attacks, where AI can be programmed to conduct automated attacks on computer networks, including massive data theft and system sabotage. Such attacks have the potential to increase the intensity and losses suffered by victims, as AI can learn and adapt to the security systems it faces. Based on the explanation above, there are two main problem formulations that are interesting to research, firstly, what is the potential criminal acts that committed by Artificial Intelligence? secondly, how is the criminal liability of Artificial Intelligence in Indonesia criminal law?

2. Methods

The type of research used to analyze the problems is normative juridical research (Soekanto & Mahmudji, 2003). The normative juridical research method is a research based on analysis of library materials as secondary data. This research is using the legal norms contained in the laws and regulations and then an assessment of the laws, regulations and the other relevant literature data studied in this paper. The approaches used in this scientific article are conceptual approach, case approach, and statute approach (Marzuki, 2011) that is related to potential crimes by AI and criminal liability carried out by AI. Library research is used to gather legal materials, and inventory is added based on the problem formulation that has to be addressed

Library research is used to acquire relevant legal materials, link them together, and assist the conversation. Criminal Code (KUHP) and Electronic Information and Transactions Law/ *Undang-Undang Informasi dan Transaksi Elektronik* (UU ITE) No. 1/2024 serve as the main legal resources used in this study. Books, journal papers, and research findings as resources a compatible theory secondary legal literature. This descriptive-analytical study aims to give a full, thorough, and organized picture of everything that has to do with criminal case resolution by outlining the relevant laws and rules, legal theories, and effective implementation strategies.

3. Results and Discussion

3.1 Discussion of potential crimes committed by artificial intelligence

In essence, the definition of a criminal offense in Indonesian laws and regulations does not have a clear and explicit definition. The definition of criminal offense understood until now is a theoretical creation of jurists. *Strafbaar feit* and *delict* are Dutch terms that are interpreted as criminal acts, criminal events, and many more (Santoso et al., 2023). *Strafbaar feit*, a dichotomy in 3 syllables, namely *straf* (translated as criminal and law), then *baar* (can or may), and *feit* (act, event, offense)(Chazawi, 2002). The usage of the term "criminal act" in Indonesia was precipitated by the adoption of Dutch criminal law based on the idea of concord. In Indonesia, the phrase criminal act is used in a variety of texts and laws, including criminal acts, criminal offenses, punishable acts, and punishable acts.

Crime is a fundamental concept in normative juridical criminal law. Crimes or criminal acts can be understood from both a juridical and criminological perspective. In the normative juridical approach, a crime is an act that, in the abstract, has fulfilled the elements of a criminal offense (Mertokusumo, 1999). Moeljatno in his book reveals that a criminal act has the meaning of an act prohibited by a rule of law, the prohibition is accompanied by a threat or sanction in the form of a certain penalty for those who violate the prohibition (Gunadi & Efendi, 2014). So it can be concluded that a criminal offense is an act or action committed by a legal subject against the law which results in criminal punishment.

Departing from this definition, of course there are elements that must be met if an act is classified as a criminal offense. The elements are divided into two perspectives, namely monistically (focusing on the requirements of nature and actions) and dualistically (focusing on actions only). According to the monistic view, the elements of a criminal offense are as follows (Ilyas, 2011):

a. The existence of an act;
b. The existence of unlawfulness;
c. There is no justification;
d. Able to take responsibility;
e. Error; and
f. There is no excuse.

Meanwhile, the elements of a dualistic criminal offense consist of:

a. The existence of acts that match the formulation of an offense;
b. There is an unlawful nature; and
c. Absence of justification.

Artificial Intelligence (AI), or artificial intelligence, is a branch of computer science that focuses on developing systems or machines capable of mimicking human intelligence to perform a variety of complex tasks that would normally require human intelligence (Qurrahman et al., 2024). In general, AI allows machines to perform activities such as reasoning, learning, decision-making, and perception of the surrounding environment. According to Russell & Norvig (2021), AI can be defined as an attempt to create intelligent agents that can understand, act, and adapt independently within their environment. AI is not just software or programs, but includes progressive adaptability and problem solving. AI is not limited to biological methods or patterns that can be observed in humans; instead, it relies on computational algorithms, machine learning, and big data to identify patterns, analyze information, and make decisions (Goodfellow et al., 2016).

AI includes various sub-disciplines such as machine learning, deep learning, natural language processing (NLP), robotics, as well as knowledge-based systems (Saini, 2023). These sub-disciplines enable AI to handle large amounts of data, analyze complex patterns, and respond effectively according to the situation at hand. The dimensions and capabilities of AI itself, according to Russell & Norvig (2021), can be divided into four main dimensions that include thought process, behavior, humanism, and rationality. Based on these dimensions, AI is classified into four categories: (1) systems that think like humans, (2) systems that act like humans, (3) systems that think rationally, and (4) systems that act rationally. This categorization focuses on AI's ability to understand problem patterns, provide accurate solutions, and think and act based on reliable calculations. In this way, AI can produce optimal solutions to various complex problems through an adaptive and data-driven approach (Tegmark, 2017).

AI is generally divided into two main types: Artificial Narrow Intelligence (ANI) and Artificial General Intelligence (AGI). ANI is a subset of AI that is especially built to perform certain functions, such as digital voice assistants or content recommendation systems. ANI relies on algorithms learned in a single area and is unable of functioning outside of its specified programming (Goodfellow et al., 2016). ANI works based on algorithms trained to recognize specific patterns in one domain, but is incapable of acting outside of its programming-defined scope. In this case, ANI has the potential to become a tool for criminal acts such as surveillance that violates privacy or manipulation of data for illegal gain.

Instead, AGI is a type of artificial intelligence that is similar to humans' ability to perceive, learn, and adapt to varied contexts. AGI is not only capable of solving various complex tasks, but also has adaptive flexibility that enables autonomous decision-making. The fast development of AI over the last few decades has brought many benefits, but it has also presented concerns, particularly in terms of potential criminal crimes and legal liability. In the future, the emergence of AGI may have major implications for criminal law, especially in terms of determining legal liability when AGI acts autonomously without human control. In this case, the potential for AGI to make autonomous decisions poses a serious risk of criminal offenses, including autonomous vehicle accidents or fatal medical errors. In these situations, it is difficult to determine the legally responsible party, given the nature of the AGI that is not fully under the control of the developer or user.

The implications of AI for criminal law require in-depth study, especially in determining legal responsibility when AI causes harm. For example, in the case of an AI-controlled autonomous vehicle that has a fatal accident, it is difficult to determine who is legally responsible. Currently, Indonesian criminal law still relies on the concept of "mens rea" or malicious intent which is only relevant for human legal subjects. The adaptable and autonomous nature of AI demands a new approach in law, including the establishment of specific regulations governing the actions and risks associated with AI.

Crime always develops one step ahead of the efforts made by law enforcement. The juridical definition of crime according to R.Soesilo is an act of behavior that is contrary to the law (Ridwan & Ediwarman, 1994). This means that a crime can be categorized as a criminal offense if it is regulated by law with the principle of legality. However, there is a criminal policy in the politics of criminal law in Indonesia in order to see the potential crimes that may arise, it is necessary to approach the law preventively administratve and repressive judiaciary. This statement is certainly in line with the massive behavior of people who always move dynamically in today's digital 5.0 era.

One of the potential crimes that are feared to occur in the future is criminal acts by artificial intelligence. Artificial intelligence will not escape the potential to commit an act of violation of the law, either due to its own autonomous capabilities or due to problems in the existing system (Bahiyaturrohmah, 2024). The sophistication of artificial intelligence can open up a series of new criminal opportunities. Based on the level of threat posed, crimes that can be committed by artificial intelligence can be categorized into mild, medium, and high (Caldwell et al., 2020).

Low-threat artificial intelligence crimes refer to the types of crimes that can be committed by artificial intelligence that tend to have relatively small or limited consequences that are easier to prevent by improving network security and authentication systems, such as misuse of biometric systems, artificial intelligence-based fraud known as snake oil, and learning-based cyber attacks. Furthermore, there is a medium threat category of artificial intelligence, which is a type of potential crime that has the same meaning as the low category, but if not prevented, it will have a great risk or impact (Leprince-Ringuet, 2020). For example, burglar bots and AI-authored fake reviews. Finally, the high-level category of artificial intelligence crimes refers to the types of crimes committed by artificial intelligence that are difficult to prevent and have a great risk, so that this artificial intelligence is considered to threaten the basic rights of everyone and even the security of the state. This high-level artificial intelligence crime is certainly different from the previous low and medium-level AI crimes. Therefore, special attention needs to be given to crimes committed by artificial intelligence at this high level. Two of these potential crimes by artificial intelligence are Deepfake and Autonomous Vehicle Crime.

First, the potential criminal offense of Deepfake. The term *deepfake* is terminologically divided into the word "*deep"* (referring to deep learning) and the word "*fake*" (Brandon, 2018). Deepfake is a visual medium in the form of video, audio, or even a combination of both that is altered to manipulate the public by using the capabilities of *Artificial Intelligence* from a machine-based or software system as propaganda and profit (Veljković et al., 2024). The technique starts by analyzing a large number of photos or videos of a person's face, teaching artificial intelligence algorithms to make changes to the face, and then using these algorithms to map the face into video, as well as audio (Dodge et al., 2018).

The purpose of creating deepfakes was originally just for entertainment and jokes. However, the irony is that in today's social media, this AI-based technology has been misused to mislead the public and spread false information or news lately. The problem of using *deepfakes* is increasingly widespread and has a variety of models. In Indonesia, PT Indonesia Digital Identity (VIDA), an Electronic Certification (PSrE) organizer registered with the Ministry of Communication and Digital (Komdigi) noted that deepfake cases are estimated to reach 1,550 in the period 2022 to 2023 (Liman & Zulaikha, 2024). For example, the case of the former President of the Republic of Indonesia appearing to make a speech using Mandarin which suddenly shocked social media, but apparently the speech was a hoax (Iradat, 2023).

Deepfake itself can also be used for pornographic content, one of which is by replacing or manipulating by attaching a person's face to the body of a pornographic content role and as if the face of the person whose face is attached to this pornographic content is carrying out sexual activities. The next example is the famous Indonesian actress Nagita Slavina in 2022 regarding a 61-second immoral video that looks like Nagita Savina, according to the Metro Jaya Police Cyber Team, it was revealed that the video was the result of Deepfake manipulation where someone else's face was replaced with Nagita Slavina's face using AI (Maharani et al., 2023).

In fact, Indonesian regulations have indeed regulated the ethics of playing social media in Law Number 1 Year 2024 concerning Electronic Information and Transactions regarding the distribution and transmission of content which is classified as a criminal offense. Criminal threats against the perpetrators are regulated in Article 45 paragraph (1) of the ITE Law which reads "Every person who intentionally and without rights broadcasts, shows, distributes, transmits, and/or makes accessible Electronic Information and / or Electronic Documents that have content that violates decency for public knowledge as referred to in Article 27 paragraph (1) shall be punished with a maximum imprisonment of 6 (six) years and / or a maximum fine of Rp l,000,000,000.00 (one billion rupiah)". Similarly, pornographic content and personal data theft are already regulated in Indonesia through law.

The issue is not about the outcome of the action, but about how these *deepfake* techniques can be prevented and overcome. Surely this deepfake technique will continue to innovate following the fast-moving AI updates. The solution from the government is questionable to move quickly in terms of this deepfake crime.

Second, Autonomous Vehicle (AV) technology, or autonomous vehicles, are innovations that allow vehicles to move and operate without human intervention, utilizing artificial intelligence and sensors for navigation and decision-making on the road. According to the National Highway Traffic Safety Administration (NHTSA), Autonomous Vehicle are able to recognize the surrounding environment and operate autonomously through a combination of sensors, AI, and machine learning algorithms (NHTSA, 2017). This technology offers many advantages in terms of efficiency and safety, but its weaknesses also create the potential for serious criminal activity, especially when these weaknesses are exploited by malicious parties or when there is a failure in the AI system.

One of the potential criminal consequences of AV is the system's limitation in recognizing and classifying objects correctly. The algorithms controlling AV's rely heavily on training data, which may not cover every situation or pattern of objects that may be encountered in the real world. In the 2018 Uber crash case, for example, the AV software failed to recognize a pedestrian as a human and considered him a static object. This prevented the system from activating brakes or maneuvering to avoid a collision, resulting in a deadly disaster. (CNN Indonesia, 2019). These failures show that limitations in object classification can create the potential for serious criminal offenses, where technological negligence has a direct impact on the safety of human lives.

In addition to failures in object classification, AVs are also vulnerable to hacking and manipulation of sensor data. Because they rely on data from sensors such as lidar, radar, and cameras, AVs can be sabotaged through external tampering or manipulation. For example, in the Jeep Cherokee hacking incident in 2015, two security experts managed to remotely access the vehicle's steering and braking systems (Greenberg, 2015).

In addition to physical threats, AVs also collect extensive user data, such as travel routes, location, and driving habits, which can be misused if they fall into the hands of irresponsible parties, as well as recording all user activities and personal data. The misuse of this data opens up opportunities for criminal acts such as identity theft or fraud, which harm individuals and potentially violate privacy (Brundage et al., 2018). An indication of this is that there is an element of fault that can be held liable to the developer as the person behind the database of the AI embedded in the AV. Overall, the weaknesses in AV technology create the potential for destructive criminal acts as they include various threats to physical safety, data security, and individual privacy.

3.2 Discussion of artificial intelligence criminal liability

Criminal liability is defined as the imposition of punishment for actions that violate prohibitions or cause prohibited conditions (Fadlian, 2020). Criminal liability is simply described as a punishment that must be applied as a result of a criminal law violation. According to Prodjodikoro (2008), a criminal act is an act whose perpetrators can be subject to criminal law. Criminal liability focuses on proving whether an action is a criminal act or not. The causality between criminal liability and the act must be seen much more specifically.

As a legal act, we should examine the elements that must be fulfilled in order for an act to be considered a criminal offense. According to Lamintang (1997), the are both subjective and objective parts to criminal act. The part of a criminal act are not limited to the two parts above. Knowledge of the part of criminal act also develops following the times and different opinion among experts. However, in general, it can be concluded that the part of a comprehensive crime include (Huda, 2010) the legal subject that is target (*addressaaat norm*), prohibited acts (*strafbaar*), either doing something (*commisssion*), or not doing something (*omission*), as well as causing consequences, and criminal threats (*strafmaat*).

Legal subjects are parties who are capable or able to carry out legal actions. Indonesia only recognizes two legal subjects that can be held criminally liable. The first is the Person (*Natuurlijke Person*), and the second is the Legal Entity (*Recht Person*). Initially, the subject of law was limited to persons only, but with the dynamics of the law that continues to develop, it gave birth to an expansion of meaning. Therefore, legal entities are also regulated as subjects of law and are considered capable of performing legal acts.

The fundamental element of a legal subject is the intention of the legal subject. Intention with its relationship to the actions taken by the perpetrator of the crime is termed *mens rea* (Joshua & Adhari, 2021). Mens rea is the psychological condition of the perpetrator of a criminal act, at the moment of committing a criminal act is a psychological state that can make a person subject to criminal sanctions (Sudarto, 2009) In this way, it can be said that intention is the basic of criminal liability, the absence of intention causes a person cannot be subject to criminal sanctions for his actions. According to Paulsen, a behavior cannot be called a crime if there is no malicious intent.

In the context of AI's existence as a legal subject, this means that AI's intent must first be proven. If AI is seen as something that can carry out legal actions, then it is not certain that AI can be held legally responsible. Due to the fact that criminal liability is only required for something that is a legal subject. This is a fundamental part of the principle of legality. So far, AI is still carried out according to human will. As long as there is no mechanism that can prove AI's natural criminal will, then imposing criminal liability on AI is wrong.

In studying AI as a legal subject, we should detach it from the framework of the principle of legality. Based on various legal sources , there are still no specific regulation regarding AI. Therefore, using analogies to overcome legal gaps is a logical thing to do. The application of basic legal logics is the best way to find the most appropriate regulation. It is hoped that the regulatory model discussed today can become the basis for future legal thinking (*ius constituendum*).

Putting AI as a single legal subject is impossible. The existence of AI cannot be separated from the human element (*natuurlijke person*) both as a users and developers. Thus, AI that commits a criminal offense will never stand alone for its actions. So far, AI can only run with human commands and cannot carry out activities for its own purposes. This means that AI does not have willpower like humans and the element of mens rea cannot be proven. As long as there is no legal mechanism that can prove that AI has a will and there is an element of intention, then making it a single legal subject is impossible.

One of the very important concepts of evidence in criminal law is the element of intent. Von Hippel explained that what is meant by intetion is the will to make an act and the will to cause consequences of that act. The formulation of willing and knowing is often referred to as *willens en wetens. Willens* means that one must will what one does and *wettens* means that one must know the consequences of what one does (Mallarangeng et al., 2023). The

element of intent and the two formulations above are clearly not fulfilled. How is it possible that an AI that does not even have consciousness to fulfill the element of intentionality to be used as a single legal subject. On the other hand, criminal acts committed by or with AI must still be held accountable. However, the paradigm of AI as a single legal subject must be shifted to humans who are involved in criminal acts committed by AI. This research aims to find out which party who should be responsible for the mistakes made by AI. Therefore, AI is considered as a partial legal subject, using the doctrine of *in loco parentis* (Amboro & Komarhana, 2021). This doctrine means "in place of parents" or instead of parents (Legal Information Institute, 2023) This doctrine views AI as a child whose responsibilities are still under parental supervision. The parents are the developers and users of that. The use of this doctrine makes sense, given that AI is considered a subject capable of legal action, but not capable of being held liable.

In proving a criminal act in AI, the first thing to do is to identify the location of fault. There are two views of AI criminal liability in terms of AI's capacity to act. The first is AI that acts semi-autonomously or still requires user commands. The liability for this action will be returned to humans or user as the government who can prove the *mens rea* element. By using the doctrine of Vicarious Liability. This doctrine essentially explains that other people can be responsible for the actions or mistakes made by other people (other entities) (Sulistio & Salsabilla, 2023). In Indonesian criminal law, this doctrine can be seen from the Criminal Code 2023, specifically in Article 37 paragraph (2). This article stipulates that a person can be held responsible for criminal acts committed by others.

The implication of the use Vicarious Liability is that criminal liability carried out by AI is returned to the user. So, AI is seen as a tool. Humans as the users becomes a substitute legal subject who will bear legal responsibility if the AI commits a criminal act at its command. This can be likened to AI as a legal firearm, and humans as its users. Firearms that is supposed to function for self-defense can be misused for criminal acts of murder. This means that the power rests with humans as the users of firearms or in this context AI. Likewise, the military should be held responsible for war crimes, and it is not arms supply companies. However, if the AI's fault lies in the programming elements that created the crime, then criminal liability will be back to the developer. For example, program errors, errors, judgment and calculations errors that have fatal consequences. Moreover, if the AI has been indicated as fully autonomous, it means that the AI has its own consciousness (Sulistio & Salsabilla, 2023). Therefore, the developer is considered to have reason to suspect that there will be criminal acts may have occured. At the end, based on the principle of material offense, developers can be criminal sanctions againts AI. Without having to wait for the effects after it reaches the user.

4. Conclusions

Based on the threat level, the potentially crimes that commited by Artificial Intelligence are divided into three categories: low, medium, and high with the highest category covering crimes that pose a significant risk to public safety and state security. Two forms of AI crime that require special attention are deepfake and autonomous vehicles (AV) crime. Deepfake uses AI to manipulate visual and audio media, creating false information that can damage reputations or spread propaganda, such as cases in Indonesia related to the spread of hoaxes and pornographic content. On the other condition, AVs, which operate without human intervention, offer efficiency but present significant risks if their AI systems fail, as in the fatal Uber crash in 2018. In addition to the risk of accidents, AVs are vulnerable to hacking, which can pose physical threats and privacy violations through misuse of user data. Overall, the development of AI brings great challenges to criminal law, requiring a proactive response from policymakers and law enforcement to anticipate and address these potential technological crimes to protect public safety and maintain the integrity of privacy.

The Criminal Liability of Artificial Intelligence in Indonesia criminal law, must be released from the framework of the principle of legality given the absence of regulations on this matter. Therefore, the use of theories, doctrines, expert opinions, basic legal logic and

analogies are the basis for proper legal formulation. The current AI does not yet have the ability to perform its own actions without human command. As a legal subject, it must have a will or mens rea element. In the will, the formulation of willing and knowing (*wettens en willens*) is known. As long as there is no legal mechanism that can prove that AI has a will and there is an element of intentionality, then making it a single legal subject is impossible. Crimes caused by AI must still be accounted for. The paradigm of criminal responsibility is shifted to the human element involved in the act. The first doctrine is to view AI as a child whose guardianship of the criminal offense committed is returned to the user and developer as parents (*in loco parentis*). The second is the doctrine of vicarious liability which emphasizes that the criminal responsibility of a person can be transferred to another person or entity in line with the Criminal Code 2023 in article 37 paragraph (2). If the element of AI fault is born due to misuse of the AI's intended function, then the liability is borne by the user. Meanwhile, if the AI fault lies in programming elements such as errors and technical errors, the developer is deemed to be able to expect that the error will occur. In such cases, it is the developer who must bear the criminal burden.

Acknowledgement
The authors would like to express their sincere gratitude to the reviewers for their valuable insights and constructive feedback, which greatly contributed to the improvement of this work. The author also extends heartfelt gratitude to the Abhinaya Fest, Faculty of Law University of Bengkulu, for their invaluable support in academic development and collaboration.

Author Contribution
All authors contributed substantially to the conception, fundamentally analysis, argumentation, data analysis, interpretation of concepts, and writing this article.

Funding
This research received no external funding.

Ethical Review Board Statement
Not available.

Informed Consent Statement
Not available

Data Availability Statement
Not available.

Conflicts of Interest
The authors declare no conflict of interest.

References

Amboro, F. Y. P., & Komarhana, K. (2021). Prospek Kecerdasan Buatan Sebagai Subjek Hukum Perdata Di Indonesia [Prospects of Artificial Intelligence as a Subject of Civil Law in Indonesia]. *Law Review*, 145-172. https://doi.org/10.19166/lr.v0i2.3513

Bahiyaturrohmah, B. (2024). *Mimpi Buruk Dunia Digital: Tindak Kejahatan yang 'Dilakukan'oleh Entitas Artificial Intelligence*. Lembaga Kajian Keilmuan Fakultas Hukum Universitas Indonesia. https://lk2fhui.law.ui.ac.id/portfolio/mimpi-buruk-dunia-digital-tindak-kejahatan-yang-dilakukan-oleh-entitas-artificial-intelligence/

Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press.

Brandon, J. (2018, February 20). *Terrifying high-tech porn: Creepy 'deepfake' videos are on the rise.* Fox News channel. https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S. J., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R., & Amodei, D. (2024). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation* (arXiv:1802.07228v2 [cs.AI]). https://doi.org/10.48550/arXiv.1802.07228

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1–13. https://doi.org/10.1186/s40163-020-00123-8

Carr, I., & Goldby, M. (2011). *International Trade Law Statutes and Conventions 2011-2013 2nd Edition*. Taylor & Francis Group.

Chamberlain, R. P. (2024, Juni 3). *The Ethics of AI - The Digital Dilemma*. RPC Legal. https://www.rpclegal.com/thinking/artificial-intelligence/ai-guide/the-ethics-of-ai-the-digital-dilemma/

Chazawi, A. (2002). *Pelajaran Hukum Pidana Bagian I: Stelsel Pidana, Teori-Teori Pemidanaan & Batas Berlakunya Hukum Pidana*. PT. Raja Grafindo Persada.

CNN Indonesia. (2019, November 8). *Kecelakaan Mobil Otonom Uber: 'Software' Tak Mengenali Objek.* CNN Indonesia. https://www.cnnindonesia.com/otomotif/20191108084518-579-446566/kecelakaan-mobil-otonom-uber-software-tak-mengenali-objek

Dodge, A., & Johnstone, E. (2018). Using Fake Video Technology to Perpetuate Intimate Partner Abuse. *Without My Consent*, 1-9. https://withoutmyconsent.org/

Fadlian, A. (2020). Pertanggungjawaban Pidana Dalam Suatu Kerangka Teoritis. *Jurnal Hukum Positum*, *5*(2), 10-19. https://journal.unsika.ac.id/index.php/positum/article/view/5556

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

Greenberg, A. (2015, July 21). *Hackers Remotely Kill a Jeep on the Highway—With Me in It.* Wired. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Gunadi, I., & Efendi, J. (2014). *Hukum Pidana*. Kencana Jakarta.

Henz, P. (2021). Ethical and legal responsibility for Artificial Intelligence. *Discover Artificial Intelligence*, *1*(1), 1–5. https://doi.org/10.1007/s44163-021-00002-4

Huda, C. (2010). *Pola Pemberatan Ancaman Pidana Dalam Hukum Pidana Khusus*. BPHN Jakarta.

Ilyas, A. (2011). *Asas-Asas Hukum Pidana*. Rangkang Education Yogyakarta & PuKAP Indonesia.

Iradat, D. (2023, October 28). *Apa Itu Deepfake Yang Bikin 'Jokowi' Jago Ngomong Mandarin?*. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20231027185650-185-1016883/apa-itu-deepfake-yang-bikin-jokowi-jago-ngomong-mandarin

Joshua, E. B., & Adhari, A. (2021). Analisis Ketiadaan Niat (Mens Rea) Dalam Pemidanaan Pada Putusan Pengadilan Negeri Jakarta Pusat Nomor 844/PID. B/2019/PN. JKT. PST. *Jurnal Hukum Adigama*, *4*(2), 3930-3952. https://www.journal.untar.ac.id/index.php/adigama/article/view/17975

Lamintang, P. A. F. (1997). *Dasar-dasar Hukum Pidana Indonesia*. Citra Aditya Bakti Bandung.

Legal Information Institute. (2023). *in loco parentis*. Cornell Law School. https://www.law.cornell.edu/wex/in_loco_parentis

Leprince-Ringuet, D. (2020, August 5). *Evil AI: These are the 20 most dangerous crimes that artificial intelligence will create.* ZD NET. https://www.zdnet.com/article/evil-ai-these-are-the-20-most-dangerous-crimes-that-artificial-intelligence-will-create/

Liman, U. S., & Zulaikha, S. (2024, November 1). *VIDA catat penipuan "deepfake" di Indonesia melonjak 1.550 persen*. Antara Kantor Berita Indonesia. https://www.antaranews.com/berita/4437365/vida-catat-penipuan-deepfake-di-indonesia-melonjak-1550-persen

Maharani, A., Sabili, A., Septia, E. W. M., Magistravia, E. G. R., & Tobing, P. (2023). *Deepfake Artificial Intelligence (AI): Metode Baru Dari Wujud Kekerasan Berbasis Gender Online (KBGO).* HopeHelps and UGM.

Mallarangeng, A. B., Mustari, Firman, & Ali, I. (2023). Pembuktian Unsur Niat Dikaitkan Dengan Unsur Mens Rea Dalam Tindak Pidana Korupsi. *Legal Journal of Law*, *2*(2), 11-24. https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/69

Marzuki, P. M. (2011). *Penelitian Hukum*. Kencana Jakarta.

Mertokusumo, S. (1999). *Mengenal Hukum*. Liberty.

NHTSA. (2017). *Automated Driving Systems: A Vision for Safety.* National Highway Traffic Safety Administration https://www.nhtsa.gov/report-a-safety-problem?gad_source=1&gclid=Cj0KCQiAx9q6BhCDARIsACwUxu4EgQmuAq4eu68EV7fkak42cvqk158Z9kQNvDP2Whjd2cyuUruyBgUaAqgMEALw_wcB&gclsrc=aw.ds#index

Patel, A. (2015). Crime in the Evolved Digital Age. *Journal of Technology Law & Policy*, *20*(1), 19–38. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2724865

Plotinsky, D., & Cinelli, G. M. (2024, April 9). *Existing and Proposed Federal AI Regulation in the United States*. Morgan Lewis. https://www.morganlewis.com/pubs/2024/04/existing-and-proposed-federal-ai-regulation-in-the-united-states

Pohan, Z. R. H., Idris, M. N., Ramli, Anwar, & Paisal, J. (2023). Sejarah Peradaban dan Masa Depan Kesadaran Manusia Pada Posisi Ontologis Kecerdasan Buatan (Artificial Intelligence) Dalam Perspektif Alquran (Kajian Tafsir Ayat-Ayat Filosofis). *Jurnal Studi Alquran dan Tafsir*, *3*(1), 29–38. https://doi.org/10.47498/bashair.v3i1.2030

Prodjodikoro, W. (2008). *Azas-Azas Hukum Pidana Indonesia*. PT Refika Aditama.

Qurrahman, S. H., Ayunil, S., & Rahim, T. A. (2024). Kedudukan dan Konsep Pertanggungjawaban Artificial Intelegence Dalam Hukum Positif Indonesia. *Unes Law Review*, *6*(4), 12687-12693. https://doi.org/10.31933/unesrev.v6i4.2108

Rasyid, N. A. (2024, Februari 22). *10 Negara Pengguna AI Terbanyak, Indonesia Salah Satunya*. GoodStats. https://data.goodstats.id/statistic/10-negara-pengguna-ai-terbanyak-indonesia-salah-satunya-RLlmC

Ridwan & Ediwarman. (1994). *Azas – Azas Kriminologi*. USU PRESS.

Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach. 4th Edition.* Pearson.

Saini, A. (2023). *Introduction to Artificial Intelligence*. Springer International Publishing.

Santoso, A. P. A., Rezi, & Aryono. (2023). *Pengantar Hukum Pidana*. Pustakabaru Press.

Sentinella, R. (2024, Oktober 30). *Council of Europe's Framework Convention on AI and its global implications*. IAPP News. https://iapp.org/news/a/council-of-europe-s-framework-convention-and-its-implications-for-global-ai-governance

Soekanto, S., & Mahmudji, S. (2003). *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Raja Grafindo Persada.

Sudarto. (2009). *Hukum Pidana I Edisi Revisi.* Yayasan Hukum Sudarto FH Undip.

Sulistio, F., & Salsabilla, A. D. (2023). Pertanggungjawaban pada Tindak Pidana yang Dilakukan Agen Otonom Artificial Intelegence. *UNES Law Review*, *6*(2), 5479-5490. https://doi.org/10.31933/unesrev.v6i2.1209

Tegmark, M. (2017). *Life 3.0: Being Human in the Age of Artificial Intelligence*. Knopf.

Veljković, S. Z., Ćurčić, M. T., & P.gavrilović, I. (2024). Dark sides of deepfake technology.

Military Technical Courier/Vojnotehnicki glasnik, *72*(3), 1441–1463. https://doi.org/10.5937/vojtehg72-49630

Biographies of Authors

Adria Fathan Mahmuda, Law Study Program, Faculty of Law, Andalas University, Padang City, West Sumatra 25163, Indonesia.

- Email: adriafathan26@gmail.com
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Mahesa Cakra Gusti, Law Study Program, Faculty of Law, Andalas University, Padang City, West Sumatra 25163, Indonesia.

- Email: mahesacakragusti31@gmail.com
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Faruq Anrusfi, Law Study Program, Faculty of Law, Andalas University, Padang City, West Sumatra 25163, Indonesia.

- Email: anrusfifaq@gmail.com
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A