Available online at: http://jurnal.uns.ac.id

Yustisia Jurnal Hukum

| ISSN (Print) 0852-0941 | ISSN (Online) 2549-0907 |

AI-Induced Fatalities: A Criminal Law Perspective from Indonesia and International Perspective

Vicko Taniady[1]
Faculty of Law, Monash University, Australia
Corresponding author's email: vtan0045@student.monash.edu

Article Information

Received for publication April 29, 2025
Accepted after corrections July 26, 2025

Keywords: *artificial intelligence; criminal liability; legal reform.*

DOI:10.20961/yustisia .v14i2.101636

Abstract

The rapid development of AI has raised legal challenges, particularly when AI causes harm or even death. This study analyses criminal liability in AI cases from the perspectives of Indonesian and international law, with a primary case study focusing on the death of a teenager resulting from interaction with an AI chatbot. The study aims to examine whether traditional principles of criminal liability (actus reus and mens rea) can be applied to AI and evaluate the readiness of the Indonesian legal system to manage AI-related cases. The research adopts a qualitative approach with doctrinal, comparative, and interdisciplinary analyses. The findings indicate that AI cannot fulfil the element of mens rea. Thus, criminal liability must be transferred to the actors behind AI, such as developers or service providers, through vicarious liability mechanisms. Comparatively, some jurisdictions, such as the European Union, have adopted a risk-based approach to regulate AI, while Indonesia still faces a legal vacuum. This study suggests that legal reforms are needed, including the establishment of a special category of liability for AI, mandatory risk assessment, and harmonising international regulations. Therefore, a responsive legal framework can be established to protect individual rights and ensure the responsible development of AI.

I. Introduction

This era has seen remarkable technological advancements, including numerous innovations drastically altering human life. (Suryono, 2023; Taniady & Siahaan, 2023). One of the most notable technical accomplishments is the introduction of Artificial Intelligence (hereinafter written to AI), which has become an essential component of human life.

AI's capacity for rapid data analysis and algorithmic decision-making has introduced efficiencies and conveniences that were once challenging to attain through traditional approaches (Soori et al., 2023). Many consumers today view the presence of AI as a futuristic technology (Davenport et al., 2020). The notable rise of generative AI tools, including Google Gemini, Chat GPT, Microsoft Copilot, Adobe AI, Deepseek, Meta AI, and other AI technologies, has garnered considerable consumer interest. These generative AI technologies can autonomously produce text, graphics, music, and other content based on straightforward directions from users.

Even if AI makes things easier and better, it presents problems and negative consequences that must be taken seriously (Alhitmi et al., 2024), algorithmic bias (Walker et al., 2023), replacement of human labour by machines (Intahchomphoo et al., 2024), and excessive dependence on technology (Zhang & Xu, 2025) are the primary focus of debates on AI ethics and regulation. However, discourse on AI must encompass criminal law, particularly when AI systems inflict harm that prompts inquiries into criminal liability. This article will analyse a compelling case in which AI has resulted in a fatality.

A 14-year-old boy from Orlando, Florida, named Sewell Setzer III, committed suicide after forming a profound emotional connection with an AI chatbot from the Character AI platform (Roose, 2024). The AI chatbot, named '*Daenero*' and inspired by a character from the TV series *Game of Thrones*, engaged in romantic and sexual conversations with Sewell (Roose, 2024). In one of their final conversations, when Sewell expressed his desire to '*come home*', the chatbot responded with phrases like '*Please do, my sweet king*,' which are believed to have reinforced his suicidal intentions (Roose, 2024). Sewell's mother, Megan Garcia, has filed a lawsuit against Character.AI and its founders, as well as Google, alleging negligence, wrongful death, and product liability (Montgomery, 2024; Roose, 2024). The lawsuit alleges that the platform failed to implement sufficient safety measures to safeguard teenage users from inappropriate content and detrimental relationships. Garcia emphasised that the chatbot failed to deliver suitable responses when Sewell articulated suicidal ideations and was reportedly accused of promoting such behaviours (Montgomery, 2024; Roose, 2024).

The action initiated by Sewell Setzer's mother is a civil claim grounded in negligence, product liability, and wrongful death. This case does not pertain to criminal issues. This terrible episode compellingly illustrates the necessity for legal experts to examine whether criminal law may and should address situations when an autonomous AI system contributes to an individual's death. This article does not aim to conflate civil and criminal frameworks, but rather uses this civil case to initiate a focused discussion on potential criminal liability involving AI systems.

The development of this case has ignited discourse over the notion of criminal accountability. In criminal law, both individuals and businesses can be held liable (Prananingrum, 2014). These two legal matters are related by the idea that criminal responsibility can only be imposed on legal entities that can be held accountable, which contains the elements of fault (mens rea) and act (actus reus). However, the existence of AI as a non-human creature poses a fundamental threat to the current legal structure. The Sewell case, in which an AI chatbot was suspected of contributing to someone's death, raises an important question: who is to blame for this incident? Which party can be held criminally accountable in such a case? Can the software developer, the corporation that provides the AI service, or another entity with control over the technology be held criminally accountable for the outcomes of the AI system they created? This problem becomes more complicated because AI lacks human-like cognition, intent, and will. AI is built on human-programmed or taught algorithms and datasets. The distinction between human and machine accountability, however, becomes blurred when AI can operate autonomously and cause real-world repercussions, such as urging someone to kill themselves. In this context, legal debate is discussing broadening the scope of criminal culpability, including vicarious liability, which allows organisations or technology controllers to be held accountable for the activities of the 'digital entities' they administer.

The article examines a complex and more essential question: how should the law respond when artificial intelligence (AI) causes injury or, in extreme cases, contributes to human death? While AI technology is revolutionary, it raises serious legal and ethical concerns, especially when these systems act independently and influence human decisions or behaviour in unexpected, even harmful, ways. The major goal of this study is to see if existing criminal liability rules, specifically *actus reus* (wrongful act) and *mens rea* (wrongful thinking), can be meaningfully used in AI scenarios. This study examines whether AI may be deemed a legal subject capable of bearing responsibility, or whether responsibility should be assigned to the human players behind the technology, such as developers, providers, and platform operators. This study will also examine how Indonesian criminal law currently views the position of AI and if the legal system is prepared to manage AI-related issues. In addition, this research intends to uncover legal tactics and frameworks that can serve as examples or warnings for Indonesia by performing a comparative analysis of international jurisdictions, including the United States, the European Union, and Australia.

This study examines foreign models while critically assessing their applicability to Indonesia's legislative and institutional framework. To work, legal transplants need to consider how well the law is enforced in the area, how well people understand technology, and the culture of the law in the area. This study is crucial due to the escalating impact of AI in daily life and the rising threat of legal ambiguity. Legal frameworks become essential as AI systems gain autonomy and their consequences grow more significant, transparent, and adaptable. Consequently, this study seeks to enhance the legal conversation around AI accountability and foster the creation of more adaptive legal frameworks, both domestically and internationally.

This study adopts a qualitative legal approach, combining doctrinal, comparative, and interdisciplinary methods to explore how criminal law should respond when harm is caused by artificial intelligence. The starting point is a doctrinal analysis, which allows this study to critically reflect on fundamental legal concepts (Bhat, 2020) such as *actus reus*, *mens rea*, and causality, and question whether these human-centred doctrines are still adequate in machine-driven actions. A comparative approach is used to examine how other jurisdictions deal with similar issues to strengthen the analysis. This approach helps reveal the possibilities and limitations of existing legal models, thereby providing valuable insights for reform in Indonesia. The comparison is descriptive and argumentative, highlighting how outdated or rigid doctrines may struggle to keep pace with technological advancements. This research also centres on a real-life case involving the tragic death of a teenager after interacting with an AI chatbot. This case illustrates the legal and moral vacuums that can arise when harm is caused by systems that operate autonomously but remain under human design and control. This case is a powerful example of why more precise legal boundaries and perhaps new legal categories are urgently needed.

Finally, this study utilises diverse disciplines, including philosophy, ethics, and technology, to rigorously analyse more profound inquiries: Can machines have intentions? Should AI be regarded as legal entities, or can accountability invariably be attributed to human choices? This multidisciplinary analysis substantiates the assertion that legal frameworks necessitate evolution in content and structure to combat emerging forms of digital harm effectively. This research seeks to comprehend current legal constraints and actively promote a more adaptive and forward-looking criminal justice system by integrating these methodologies.

II. Theoritical Foundations of Criminal Responsibility

A. Elements of Criminal Liability: Actions, Intentions, and Causality

In classical criminal law, criminal responsibility transcends the simplistic dichotomy of guilt and punishment. Furthermore, it seeks to comprehend human beings as entities possessing will, intent, and accountability for each action they elect to undertake. Criminal law posits that an individual can only be held accountable if three criteria are concurrently satisfied: the presence of an unlawful act (*actus reus*), the intent or mental culpability of the offender (*mens rea*), and a rational link between the act and its resultant consequences (causation and foreseeability).

Let us commence with the most evident: *actus reus*. In criminal law, *actus reus* signifies 'guilty act'; in legal practice and theory, this term involves more than mere observable physical actions (McAuley, 1988). It refers to the objective element of a criminal offence, specifically the legally forbidden act or omission, coupled with unavoidable consequences and circumstances that constitute the overall framework of a crime. The Rome Statute defines actus reus as having three important parts: conduct, consequence, and context (Hajdin, 2021). These three factors ascertain an individual's objective involvement in a criminal offence. Instances are observable in crimes of aggression, when actions such as scheming, organising, or executing an act of aggression against another state constitute the conduct component of *actus reus* (Child & Hunt, 2022). Nonetheless, not all types of 'activity' are easily classified. Controversies emerge when technologies like drones or autonomous weapon systems are employed in military operations. A drone that autonomously assaults a village unequivocally results in tangible repercussions, specifically civilian fatalities. In criminal law, a drone functions solely as an instrument. Criminal activities must be ascribed to a human agent, whether the system's operator, commander, or designer. This circumstance underscores that actus reus encompasses not just the occurrence of an event but also the attribution of responsibility for it.

This idea gets even more complicated when we talk about the philosophy of action that goes along with actus reus. Some experts, like McAuley and Davidson, stress the importance of human agency, which is the ability of a person to act with awareness and control (McAuley, 1988). When someone does something wrong, this is not just about the end consequence; it's also about whether the act was really what the person wanted to do. Problems can arise when the person who committed the crime says they didn't do it on purpose, as when someone is sick, tired, or having a seizure. The case of Hill v. Baxter is a common example. A driver who fell asleep and ran a red light was still found accountable because the choice to drive while fatigued was an action that might be seen as the commencement of a chain of events (McAuley, 1988).

To explain the relationship between action and consequence, Joel Feinberg's concept of the 'accordion effect' is highly relevant (McAuley, 1988). This theory states that an initial action (such as pressing a button) can be logically extended to a series of consequences (e.g., firing a missile, sinking a ship), provided that all of these are consequences of an act performed with a specific intention (McAuley, 1988). This shows that a perpetrator can be held responsible for the entire chain of consequences, provided that the initial action was intentional and can be rationally explained within a cause-and-effect framework. Thus, *actus reus* is not merely a matter of physical action, but of actions that can be legally attributed to a person as the perpetrator, based on conscious choice, control over the action, and logical connection to the resulting consequences. This is an essential foundation of criminal responsibility, because criminal law does not punish because something 'happened,' but because someone consciously caused something to happen.

This is where mens rea is relevant, the most human aspect of criminal law. While actus reus pertains to the actions performed, mens rea investigates the perpetrator's thoughts and intentions at the time of the crime. Understanding mens rea necessitates the examination of at least two significant yet linked factors separately. Initially, it pertains to the level or nature of responsibility determined by mens rea (Child & Hunt, 2022). This situation frequently incites discussions over the redefinition of terms such as 'intention,' 'knowledge,' and 'negligence' to meet legal requirements, including the necessity of distinct terminology to address particular categories of criminal behaviour (Child & Hunt, 2022). These differences in the degree of fault determine the extent of culpability or fault attached to the perpetrator. Second, mens rea cannot be separated from the specific purpose or objective the perpetrator wishes to achieve. In practice, a person cannot experience a mental state of 'intention' or 'knowledge' in the abstract without a specific object in mind (Child & Hunt, 2022). When we talk about 'intention,' we mean intention towards a result (e.g., causing the death of a person). Similarly, 'knowledge' means knowledge of specific facts (such as knowing that one's actions are unlawful or harmful to others). In other words, *mens rea* only has meaning when linked to the specific target of the act committed.

This relationship not only clarifies the concept of mens rea but is also normatively essential. Mens rea establishes a connection between human agency and criminal conduct, while assessing the degree of culpability based on that relationship (Child & Hunt, 2022). Attributing blame would lack a rational foundation without a definitive link between the perpetrator's intent or knowledge and the act and its repercussions. Likewise, labelling someone as 'malicious' without understanding their true intentions would be unjust.

The importance of the 'target' element in defining mens rea under applicable law has been recognised; nonetheless, it is limited to offences involving direct actions (present-conduct offences) (Child & Hunt, 2022). For instance, when an offender aims to commit theft, such intention is explicitly associated with appropriating another's property without consent. Identifying the 'target' of the perpetrator's intent or knowledge frequently becomes more intricate in sophisticated circumstances, such as technology-based crimes or actions involving autonomous systems. The perpetrator's activities may transpire via technical intermediates, necessitating a comprehensive examination to ascertain the link between the perpetrator's mental state and the ensuing repercussions.

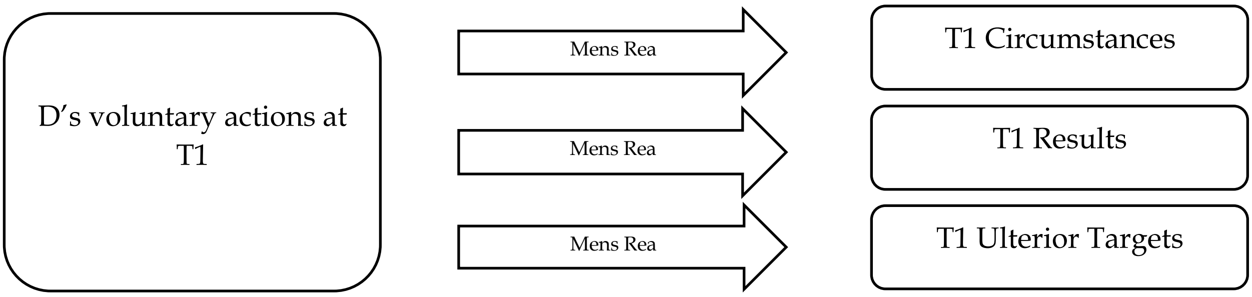

Figure 1. Present-conduct offences (Child & Hunt, 2022).
Abbreviation: D = Defendant; T = Time

Consequently, mens rea not only contributes to the categorisation of culpability but also guarantees that criminal liability is authentically assigned to the offender due to explicit intent or awareness of the act and its repercussions. Consequently, criminal law administers punishment not solely based on the occurrence of events, but also considering the manner and rationale behind them, as influenced by the perpetrator's awareness. The interplay between actus reus and mens rea embodies the essence of criminal law, indicating that not every wrongful act becomes a crime, nor must all adverse outcomes be penalised. Criminal law offers an opportunity to comprehend the human context, evaluating whether an individual merits punishment or is a victim of broader circumstances.

How can we ascertain that an action directly resulted in the purported consequences? This is where causation is relevant. Criminal law necessitates a rational and justifiable causal relationship between the action and its outcomes (McAuley, 1988). Furthermore, the principle of foreseeability arises: could the culprit have reasonably anticipated the consequences? For instance, if an individual abandons a little infant in a sealed vehicle during daylight hours, they ought to have foreseen the peril of fatality due to heat exposure (Child & Hunt, 2022). However, if the consequences are incredibly remote and unforeseeable, it would be challenging to impose criminal liability on them.

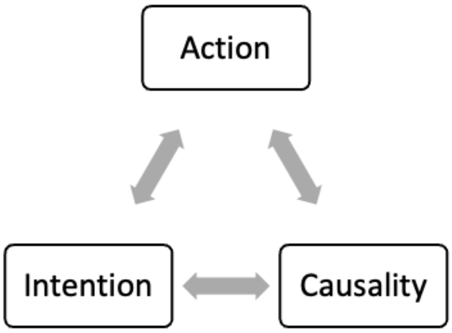

Figure 2. Element of Criminal Liability.

The three elements of action, intention, and causality are inseparable. They collaborate to guarantee that a conviction is not solely a matter of legal enforcement, but also morally and intellectually warranted to hold the individual accountable. In this context, criminal law serves not just as a mechanism of punishment but also as a manifestation of human values: fairness, autonomy, and accountability. Criminal law does not impose punishment arbitrarily; rather, it aims to comprehend, validate, and guarantee that justice is maintained for both the victim and the offender, who may have merely erred in judgment.

B. Application to Artificial Intelligence

In classical criminal law, criminal responsibility transcends the simplistic dichotomy of guilt and punishment. Furthermore, it constitutes an endeavour to comprehend humanity. Upon recognising that criminal liability encompasses not only actions but also the interplay between those actions (*actus reus*), intent or mental culpability (*mens rea*), and anticipated outcomes (causation and foreseeability), a pertinent inquiry has arisen in the technological era: What are the implications if artificial intelligence executes actions that lead to criminal repercussions? Can artificial intelligence be held accountable in the same manner as humans? This question does not exist in isolation. As the utilisation of AI proliferates in human existence, including driverless vehicles, criminal risk assessment algorithms, and autonomous weapon systems, legal discourse must reassess its normative basis. The consistent theme persists: how to guarantee justice while upholding the ideas of free choice and moral responsibility as foundational elements of criminal culpability.

In traditional criminal law, legal subjects are individuals or designated legal entities, such as companies, which possess free will, the ability to comprehend their conduct, and the potential for legal accountability. Humans are considered the principal agents in the legal system due to their free will, comprehension of the repercussions of their acts, and ability to make essential decisions (Alper, 1998). Furthermore, corporations are recognised as legal subjects because they are based on modern social and economic practices (Meyersfeld, 2025), where corporations perform functions equivalent to individuals in legal activities, thus requiring the application of accountability mechanisms. In the current framework, AI is still positioned as a legal object, where AI is considered to lack the same free will, consciousness, or legal capacity as humans and corporations. Therefore, it can be concluded that in criminal law, only agents can have the ability to be morally and legally responsible and subject to criminal sanctions.

However, as AI gains the ability to learn, make decisions independently, and act autonomously through technologies such as machine learning and deep learning (Xu et al., 2021), the distinctions between legal objects and subjects start to converge. Artificial intelligence has progressed beyond simply command execution; it now possesses the capability to adapt, make decisions based on dynamic data, and respond to unprogrammed scenarios. This phenomenon has initiated a discourse regarding the potential conferral of distinct legal standing to AI, termed 'electronic personhood.' Electronic personhood denotes artificial intelligence that exhibits significant autonomy and the ability to operate like humans, warranting recognition by law as a restricted legal entity (Brown, 2021).

The next question is whether AI can possess intent, a fundamental mens rea component. Intent in criminal law encompasses the deed, awareness, and volition to perpetrate an act and embrace its repercussions. In this instance, AI lacks cognition, emotions, and free will, which are the characteristics of humans. It lacks internal experiences that facilitate moral evaluation of its acts. Consequently, from a normative perspective, AI cannot be said to possess mens rea. Nonetheless, complexity emerges when artificial intelligence is engineered to replicate human decision-making processes. Certain systems can evaluate several situations and execute actions that seem 'deliberate' from an external viewpoint (Peters, 2023). This is where the legal dilemma emerges: should the law adapt to entities that can exhibit behaviour resembling intentionality, even if they do not actually possess consciousness?

These concerns address the difficulty by advocating for a transition from a subjective perspective to an objective-functional approach. This methodology does not necessitate evidence of awareness in AI, but emphasises design, control, and rational expectations of the system (Staszkiewicz et al., 2024). In other words, criminal responsibility may hinge on whether AI was developed adequately to prevent detrimental outcomes. Do the developers or operators of AI possess control or at least awareness of the potential risks that may emerge? This corresponds with the doctrine of constructive knowledge in criminal law, which permits an individual to be held liable for outcomes they ought to have anticipated or prevented, regardless of the absence of explicit purpose.

In practice, the culpability for AI activities is typically attributed to human actors via vicarious or delegated liability. This implies that individuals or legal entities responsible for AI creation, operation, or oversight may be held liable for any legal transgressions. Manufacturers may be held liable for accidents resulting from design flaws or technical problems; operators can face penalties for negligence in system oversight; and software developers may be accountable if their algorithms are shown to be troublesome or discriminatory. In complex AI systems, responsibility is frequently diffused across various stakeholders from the design phase to implementation, rendering the identification of ultimate accountability neither straightforward nor unambiguous.

In 2017, the European Parliament introduced the notion of electronic personhood, conferring distinct legal status upon highly autonomous AI (Nowik, 2021). This notion does not aim to equate AI with humans; instead, it is a pragmatic approach to legally attributing responsibility to entities without direct human oversight (Mordell, 2021). A legal entity representing AI allows the legal system to impose duties such as compensation funds, required insurance, or restricted civil liability, while maintaining the accountability of human actors.

This proposal has incited controversy. Concerns exist that firms or technology developers may utilise bogus legal entities to evade moral and legal accountability (Hern, 2017; Nowik, 2021). If AI is granted legal standing while companies retain control and ownership, there is no assurance that victims of AI-related errors would attain justice. Conversely, advocates of electronic personhood saw it as an essential legal advancement in response to inexorable technological progress (Hern, 2017; Nowik, 2021). They argue that just as corporations were once considered fictitious entities but are now critical legal subjects in modern systems, AI can also be regulated by a similar legal framework for clarity and effectiveness (Hern, 2017; Nowik, 2021).

Ultimately, applying criminal liability theory to AI undermines foundational legal concepts. Criminal law is predicated on the moral principle that individuals may only be penalised if they act with intent and culpability. Nonetheless, the appearance of beings capable of functioning without consciousness compels the law to reassess its comprehension of agency, intent, and accountability. AI compels us to reconsider: who bears the responsibility if people do not engage in detrimental activities, yet intelligent systems we develop and do not entirely govern do? This formerly theoretical dilemma has evolved into a pressing legal challenge, necessitating legal professionals to reevaluate the future of accountability in a society increasingly governed by algorithms.

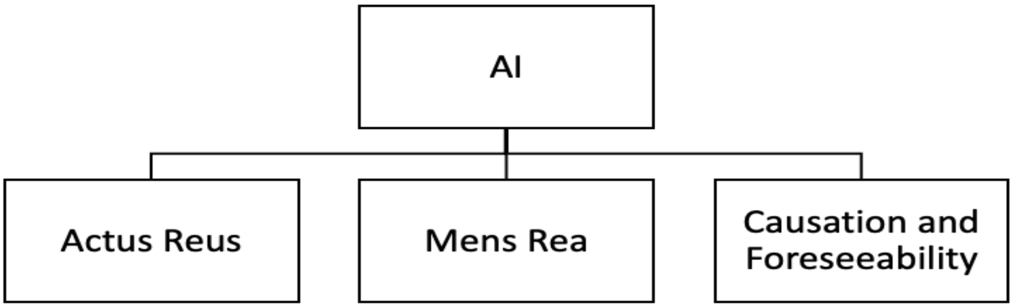

Figure 3. Evaluation of *Actus Reus, Mens Rea*, and Causation in the Context of AI.

III. Indonesian Criminal Law Perspective

The advancement of AI is a fundamental feature of the fourth industrial revolution, transforming the conventional paradigm into a technological epoch. The swift advancement of AI has elicited apprehensions about its ability to contravene legal statutes. This section will analyse how Indonesian criminal law can address the existing presence of AI. This analysis is crucial for determining criminal culpability and accountability when an AI system inflicts legal harm.

A. The status of AI in Indonesian law

In Indonesia's criminal law system, as outlined in Law Number 1 of 1946 on the Criminal Code, recognises just one legal subject: every individual. Companies have been recognised as legal entities under Law Number 1 of 2023 on the Criminal Code ('Indonesia Criminal Code', hereafter referred to as the current legislation in this study). Article 45(1) of the Indonesian Criminal Code establishes that businesses are accountable for criminal offences. Artificial Intelligence, a result of scientific engineering and lacking autonomy, has not yet been recognised as a legal entity within the criminal law framework of Indonesia.

According to the study, the root of AI in Indonesia is still perceived as a legal object, functioning merely as a tool employed by legal subjects to attain particular goals. This is founded on various legal statutes, notably Law Number 11 of 2008 on Information and Electronic Transactions, which delineates electronic systems as instruments or devices utilised by users. Moreover, Law Number 27 of 2022 about Personal Data Protection ("Personal Data Protection Law") categorises AI as a data processing system component, with accountability resting with the data controller or processor. Law Number 8 of 1999 on Consumer Protection ("Consumer Protection Law") classifies technology as a category of goods or services that may incur producer responsibility.

From a criminal law perspective, Indonesian criminal law recognises two types of offences: formal offences and material offences (Mansar & Lubis, 2023). Formal offences emphasise particular actions irrespective of their outcomes, whereas material offences necessitate the manifestation of consequences stemming from an action. If AI executes an action that satisfies the criteria of a formal offence, such as unauthorised access to an electronic system, then the technical components of the act are accomplished. Nevertheless, due to AI's absence of intent or malevolent intent (mens rea), the subjective component of a criminal act remains unfulfilled, complicating the straightforward application of criminal culpability to AI.

A similar approach to corporate criminal culpability is crucial in resolving this question. Corporations, while not human creatures, are acknowledged as legal entities capable of criminal culpability under specific concepts, including accountability through directors or individuals acting on behalf of the corporation. This is reflected in multiple laws and regulations, including Electronic Agents as defined in Article 1 of Law Number 19 of 2016, which amends Law Number 11 of 2008 on Information and Electronic Transactions (hereinafter written to ITE Law) and the Personal Data Protection Law. According to this legislation, legal organisations, including businesses that operate electronic systems or process personal data, may incur criminal penalties for legal violations. The approach allows for the integration of AI into an indirect criminal culpability framework, implicating the parties responsible for its design, development, and use. The emphasis of liability transitions from AI as an independent entity to the individuals or legal bodies responsible for it.

B. Actors behind the AI

Given that AI has not been designated as a legal entity with criminal culpability, the stakeholders in the AI life cycle—specifically programmers, developers, and deployers—must be regarded as entities subject to criminal accountability. This liability is not solely predicated on direct conduct, but rather on principles of culpability in criminal law, including culpa (negligence), recklessness, and dolus eventualis.

The concept of negligence in criminal law refers to a situation in which a person fails to act reasonably, thereby causing a result prohibited by law (Nuraeni & Sihombing, 2024). In the context of AI, a developer may be considered negligent if they ignore minimum safety standards or fail to anticipate the potential misuse of their technology. Recklessness has a higher degree of fault than negligence, as it includes an awareness of possible risks but a choice to ignore them (Greenberg, 2024). For example, a developer knows that their AI system can be used for fraud or data manipulation, but still launches it without adequate safeguards.

Furthermore, *dolus eventualis* becomes essential when discussing liability in the context of consciously accepted risk. *Dolus eventualis*, in criminal law, is a form of intent that recognises the possibility of an unavoidable consequence, but the perpetrator continues the act despite being aware of that possibility (Taylor, 2004). In other words, the perpetrator recognises the possibility and 'consents' to or accepts the risk of the consequence occurring. For example, suppose a developer creates an AI system that can make automated decisions in a financial system without human control, and subsequent breaches or significant losses occur as a result of the AI's decisions. In that case, the developer may be deemed to have acted with *dolus eventualis* if the risk was known beforehand.

Regulations such as the Consumer Protection Law provide a normative basis for assessing and taking action against parties who commit unlawful acts through electronic systems or digital products. Article 19 paragraph 1 of the Consumer Protection Law states that '*Business actors are responsible for compensating consumers for damage, contamination, and/or losses resulting from the consumption of goods and/or services produced or traded*'. Based on this, it can be concluded that business operators are responsible for losses arising from products they produce, including software and AI services that do not meet safety standards or contain hidden defects.

Meanwhile, the legal framework governing AI is very similar to the concept of Electronic Agents articulated in Article 1 of ITE Law and Article 1(3) of Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("PSTE Regulation") (Putra et al., 2023). According to Article 1 of the ITE Law and Article 1(3) of the PSTE Regulation, the definition of an Electronic Agent is as follows: '*An Electronic Agent is defined as a device that is part of an electronic system with the purpose of performing an action in the form of electronic information automatically, organised by a person or company*'. If we trace the term 'organised', it can be concluded that there is an Electronic System Operator who also functions as the controller of the Electronic Agent (Putra et al., 2023). From the analysis of these provisions, it is evident that there is a legal relationship between the Electronic System Operator (hereinafter written to PSE) and the Electronic Agent User (Putra et al., 2023). In this context, the AI Chatbot functions as an Electronic Agent that is part of the PSE. In relation to this, Article 36(1) of the PP PSTE explicitly states that:

> *"Penyelenggara sistem elektronik dapat **menyelenggarakan sendiri sistem elektroniknya atau melalui Agen Elektronik**."(in English:* Electronic system operators may **operate their own electronic systems or through Electronic Agents***)*

Moreover, according to Article 3, paragraph (1) of the PSTE Regulation, PSE is mandated to guarantee the reliable and secure functioning of the electronic systems it designates and is accountable for their functionality (Putra et al., 2023). This assertion is strengthened by Article 8 of the PSTE Regulation, which mandates that software supplied by PSE must be secure, dependable, and sustainable. This situation establishes a legal basis for attributing liability to PSE for losses incurred in electronic transactions, privacy, or data security associated with AI (Putra et al., 2023).

This context elucidates that while AI is not a legal entity, the individuals or entities responsible for AI may incur criminal liability under vicarious or indirect liability, contingent upon establishing a causal connection and an adequate degree of culpability.

IV. Practical Challenges in Law Enforcement

Discourse regarding artificial intelligence (AI) within the legal framework frequently centre on conceptual doctrines such as *actus reus* (the criminal act) and *mens rea* (the intent or culpability) (Bathaee, 2018). In practice, law enforcement has obstacles that extend beyond theoretical frameworks. Law enforcement necessitates more than mere doctrinal comprehension; it demands the capacity to execute rigorous factual and technological evidence, particularly in the context of increasingly intricate AI systems.

Once artificial intelligence is implicated in an incident or crime, law enforcement encounters significant challenges in collecting, analysing, and presenting evidence that satisfies legal criteria (Bérubé et al., 2025). This necessitates an aggressive change in digital forensics to enhance the ability to prevent and probe criminal activities (Klasén et al., 2024). One of the most pressing challenges in AI-involved law enforcement is the 'black box' problem (Brożek et al., 2024).

Contemporary AI systems, especially those utilising deep learning and support vector machine techniques, frequently function in a non-deterministic manner that is challenging for humans, including their developers, to trace or comprehend (Bathaee, 2018). Artificial intelligence can generate predictions and conclusions without elucidating their rationale, as its cognitive processes may rely on patterns beyond human comprehension (Hassija et al., 2024). The lack of transparency resulting from the intricacy of algorithmic frameworks and high-dimensional data is called the 'black box' problem (Hassija et al., 2024a). This opacity significantly complicates the establishment of causality and intent in a criminal context.

It is challenging to ascertain how AI arrives at a choice or forecast, which information influences the conclusion, or to acquire a hierarchy of the variables analysed by AI according to their significance (Bathaee, 2018). Without comprehending the methodology by which AI concludes, establishing the necessary causation to satisfy legal criteria will be exceedingly challenging. Likewise, since AI can operate independently of the programmer's intentions, discerning the motive underlying AI behaviours becomes unfeasible (Bathaee, 2018). This creates a dilemma between the need for transparency in systems that affect human lives and the desire to protect algorithmic secrecy and intellectual property (IP) (Steffen, 2024).

The 'black box' problem is exacerbated by limited access to AI source code and training data. In many cases, source code and training data are protected by intellectual property rights (IPR) and trade secrets, which makes companies reluctant to disclose them (Almada, 2023). Law enforcement agencies face significant obstacles in verifying the causes of accidents or AI behaviour. For example, if an AI developer refuses to disclose its internal architecture or training data, it will be very difficult for law enforcement agencies to determine whether a design flaw, data bias, or manipulation caused an AI decision or action (Almada, 2023). The conflict between the legal need for transparency and the protection of intellectual property is a key concern in new AI regulatory frameworks, such as the European AI Act (Steffen, 2024). This limits the authorities' ability to request deeper technical transparency.

The growing dependence of society on digital technology has rendered digital traces an essential element in investigations and legal proceedings. The acquisition of digital evidence from AI systems poses distinct obstacles. The vast quantity and diverse characteristics of digital evidence distributed across various platforms and devices render detection, recovery, analysis, and interpretation highly intricate (Klasén et al., 2024). Furthermore, the adaptive nature of AI systems, particularly those involving self-learning, raises issues of evidence integrity and authenticity (Bérubé et al., 2025). AI that continuously learns and adapts can dynamically alter digital traces, making it difficult to ensure that the evidence collected is genuine and has not been manipulated (Bérubé et al., 2025). The possibility of data manipulation or inadvertent alterations by AI self-learning mechanisms may diminish the evidentiary value in legal proceedings, casting doubt on its validity or dependability. Considering the data's complexity, legal practitioners must employ the most effective techniques to depict digital traces for judges and juries to comprehend visually. Nonetheless, these visualisations can modify and reinterpret information, generating additional comprehension bias.

Law enforcement agencies and judicial systems presently encounter considerable difficulties adapting to technological advancements. Law enforcement agencies face considerable challenges in comprehending the complexities of AI technology (Bérubé et al., 2025). Digital forensic experts require multidisciplinary expertise that includes investigative techniques, computer science, and law and ethics (Bérubé et al., 2025). However, there is a significant lack of knowledge and skills in the public sector regarding digital investigations, in contrast to private institutions that dominate development due to their greater financial capacity (Bérubé et al., 2025). To address this gap, continuous training is needed for law enforcement and legal professionals to keep pace with technological developments and understand the implications of AI (Klasén et al., 2024). Close cooperation with technology experts is also needed, including cross-sector collaboration between government agencies, research institutions, and law enforcement, as seen in the Digital Forensics Sweden (DFS) network (Klasén et al., 2024). In addition, the establishment of specialised units with in-depth expertise in AI and digital forensics to handle complex cases is essential (Klasén et al., 2024). The *European Forensic Science Area 2030* vision also emphasises the role of AI and new technologies in forensic science (Klasén et al., 2024). This collaborative approach aims to develop new technologies and methods that can be used throughout the digital investigation process, enabling the detection of crimes at an earlier stage and a better understanding of new criminal trends. This approach enables *man-machine cooperation*, leveraging the strengths of both humans and AI systems.

In the Indonesian context, these concerns are becoming progressively pertinent. Despite Article 5 of the Electronic Information and Transactions Law (hereinafter referred to as the ITE Law) affirming the validity of electronic information and documents as evidence, and extending Article 184 of the Criminal Procedure Code, practical applications indicate that the utilisation of electronic evidence remains suboptimal (Maronie, 2025). According to Eddy Hiariej, electronic information and documents, along with their printed outputs, constitute a new form of evidence in their own right (Maronie, 2025). However, to be recognised as valid evidence, such electronic information or documents must meet both formal and material requirements. Formal requirements refer to legal recognition of digital documents as stipulated in Article 5 (1) and (4) of the ITE Law, while material requirements are reflected in Articles 6, 15, and 16 of the ITE Law, which emphasise the importance of authentication, integrity, and accessibility of data.

Indonesia's judicial system continues to encounter deficiencies in technological and human resources. Digital evidence has attributes that markedly differ from physical evidence; it is susceptible to harm, readily alterable, and may be accessible solely via specialised software and technology. This evidence encompasses physical equipment, such as laptops and mobile phones, and digital data, including emails, system logs, device positions, and algorithm files.

Consequently, the capacity of investigators to acquire, store, and authenticate digital evidence lawfully is essential. Regrettably, not all law enforcement authorities possess the requisite skills and resources to execute this accurately and reliably. The practical obstacles AI presents to law enforcement are substantial, encompassing 'black box' issues and constraints in resources and experience.

Significant transformations in criminal procedure are necessary to accommodate the distinctive attributes of AI and digital technology. Essential recommendations for progression encompass: enhancing investigative and judicial capabilities via investment in training, development of both technical and non-technical skills, and the creation of specialized units; the necessity of robust and enduring collaboration between legal and technocratic domains; and the deployment of 'good AI' to counteract 'bad AI', specifically through the development and implementation of AI-driven digital forensic tools to detect and address the utilization of digital technology for illicit activities. By proactively and jointly tackling these difficulties, society may establish more robust and adaptive law enforcement institutions in the digital era, including Indonesia, which must not lag in building criminal procedural law attuned to contemporary needs.

V. Comparative and International Perspective

A. Article The United States

The emergence of AI in the United States has sparked discussions over regulation. The United States has regulations establishing the criteria for legal accountability of digital platforms via Section 230 of the Communications Decency Act (CDA) (Dickinson, 2025). Section 230 of the Communications Decency Act shields web platforms from liability for user-generated material. This rule was established to exempt these platforms from being classified as publishers of user-generated content, permitting them to control content without fearing legal repercussions. Nonetheless, the swift advancement of AI prompts a vital inquiry: do these regulations remain pertinent? In AI that autonomously produces material, the circumstances markedly diverge from the classification established under Section 230 of the CDA.

Furthermore, in line with criminal liability, several lawsuits filed by AI users who claim that AI encourages dangerous behaviour have been directed at corporations as the owners. This can be seen in several cases presented in the table below:

Table 1. Lawsuits filed in the United States related to AI (Grynbaum & Mac, 2023; Roose, 2024; The Guardian, 2024).

No.	Cases	Explanation
1.	*The New York Times v. Open AI*	The lawsuit was filed due to allegations of copyright infringement of NYTimes news articles used by OpenAI to train their artificial intelligence without permission and without paying royalties.
2.	*Walte Huang Family v. Tesla*	This case arises from allegations that Tesla overly marketed its Autopilot technology, causing drivers to believe they need not remain attentive, ultimately resulting in an accident that resulted in the death of Wei Lun Huang. The victim's family is litigating against Tesla for negligence, contending that the firm failed to alert drivers to maintain vigilance when utilising Autopilot.
3.	*Megan Garcia v. Google and Character.AI*	This case falls under civil law, as the mother of the deceased child is suing Google and Character.ai for damages incurred after her child's death. The lawsuit alleges negligence on the part of the platform in managing the use of AI that appeared to mimic her child, which could

	cause further emotional trauma to the family.

The table indicates that users will attribute responsibility to the corporation or the AI's owner when the AI err. The notion of corporate criminal liability permits firms to be held criminally accountable for the activities of their employees or agents that result in harm during their duties. Moreover, examining the Department of Justice (DoJ) trends in criminal law enforcement reveals greater emphasis on exploiting technology, including fraud-related offences, conspiracy, and cybercrime (Congress.Gov, 2023; Lewis Brisbois, 2024). Therefore, it can be concluded that the criminal law regime in the United States is increasingly considering the involvement of AI in events that pose a serious threat to public safety.

B. European Union

AI is currently pivotal in the global social and economic framework. As an independent decision-making entity, AI has infiltrated essential sectors including transportation, healthcare, financial systems, and law enforcement. This advancement also introduces new existential hazards, including dangers to human life. Inquiries regarding the qualification and attribution of criminal culpability when artificial intelligence results in a person's death have emerged as a pressing issue in the international legal landscape. The European Union's initiatives via Regulation (EU) 2024/1689 of the European Parliament and Council ("AI Act") (Presno Linera & and Meuwese, 2025), AI Liability Directive (Botero Arcila, 2024), and reforms to the Product Liability Directive (Rodríguez de las Heras Ballell, 2023) represent one of the most ambitious approaches to addressing these challenges, centred on the principle of risk-based regulation.

The AI Act establishes explicitly a mechanism for classifying high-risk AI systems under Article 6. Under these provisions, an AI system is classified as high-risk if it meets two cumulative criteria: first, the AI is used as a safety component of a product or constitutes the product itself as covered by the harmonised EU legislation listed in Annex I; second, the product must undergo a third-party conformity assessment before being placed on the market or put into service. Additionally, AI operating in critical sectors listed in Annexe III, such as biometrics, critical infrastructure control, educational selection, employment, essential public services, law enforcement, immigration, and democratic processes, are automatically considered high-risk.

However, Article 6(3) introduces an important derogation, allowing AI in Annexe III to be classified as not high-risk if it can be proven that it does not pose significant risks to health, safety, or fundamental human rights. This applies if the AI only performs narrow procedural tasks, enhances the results of prior human activities, detects decision-making patterns without replacing human judgment, or carries out preparatory tasks for decision-making processes that remain under human control. However, this exception does not apply to AI that performs profiling on individuals, and automated profiling retains its high-risk status without exception.

Article 6(4) requires that AI suppliers asserting their systems are not high-risk must document their risk analysis before marketing and register this evidence for submission upon request by national authorities. Additionally, Article 6(5) orders that the European Commission, in collaboration with the European Artificial Intelligence Board, shall issue practical guidelines by February 2026 detailing the execution of this classification, including a compilation of specific instances of AI deemed high-risk and those not. Article 6(6) to (8) ultimately confers the Commission's power to modify the exemption requirements, contingent upon the stipulation that such modifications do not diminish health, safety, and human rights protection standards.

This risk assessment method has significant implications for criminal responsibility. If a high-risk AI system malfunctions and leads to a fatality, it can be inferred that the manufacturer or operator anticipated the possible hazard. Modern criminal law fundamentally necessitates the existence of guilt, manifested as either gross negligence or recklessness. The classification of an AI as high-risk and its continued marketing or operation without sufficient protections can strongly imply gross negligence.

Unlike the civil liability scheme based on strict liability, which has been refined through the reform of the Product Liability Directive, the attribution of criminal liability still requires proof of subjective elements. In the context of AI, this can be achieved through the doctrine of corporate criminal liability (Buell, 2022) based on systemic negligence, whereby an organisation's failure to implement adequate risk mitigation procedures as mandated by sectoral regulations constitutes criminal liability.

A further concern that emerges is algorithmic transparency. Numerous contemporary AI systems, especially those utilising deep learning, function as 'black boxes,' rendering them challenging to comprehend and access, even for their engineers (Hassija et al., 2024b). Without access to AI's internal decision-making logic, law enforcement will struggle to establish the causal chain necessary for criminal liability attribution. To address this, the AI Act implicitly promotes the principle of explainability; failing to meet these standards could constitute gross negligence.

Furthermore, it should be emphasised that Article 5 of the AI Act prohibits the use of AI to support serious criminal acts such as terrorism, human trafficking, war crimes, and so on, as listed in Annexe II. Violations of this provision may strengthen criminal liability, as using AI in such activities violates security standards and contributes directly to the most serious human rights violations.

From a criminal policy perspective, applying the precautionary principle (Aven, 2023) is becoming increasingly relevant in the context of AI. When there is a serious potential risk to human life, but this cannot yet be fully predicted scientifically, failure to take reasonable preventive measures must still be considered a form of culpability. This encourages a shift in criminal law from a reactive, consequence-based model to a preventive, high-tech risk management model.

Ultimately, the EU's efforts through the AI Act, AI Liability Directive, and the updated Product Liability Directive form an essential framework, but further refinement is still needed to address the complexities of AI in criminal liability. Future criminal law must not only uphold the principle of individual culpability but also be sufficiently adaptive to address systemic failures and prevent the recurrence of tragedies caused by uncontrolled technology.

C. Australia

Australia is encountering difficulty reconciling old laws with emerging technological advancements, especially in artificial intelligence and digital harm. In the common law system of Australia, tort principles, including negligence (Australian Law Enforcement Commission, 2015), require the existence of a legal duty (duty of care), a breach of that duty, damage, and causation (Vines, 2000). Nonetheless, complications emerge when these ideas are implemented with non-human entities, such as artificial intelligence. The inquiry pertains to the legal accountability of developers, operators, or users of AI for the activities of autonomous AI. In classical law, these responsibilities generally emerge from explicit social or commercial interactions. In the context of AI, these interactions are frequently indirect or entirely unrecognised, exemplified by social media algorithms inflicting widespread psychological damage without direct personal engagement.

Regulators like the eSafety Commission are attempting to address this challenge through administrative and preventive approaches, prioritising prevention over litigation. Through the Online Safety Act 2021, eSafety was given the authority to address harmful content and compel platforms to remove harmful material, including that mediated by AI, such as deepfakes or algorithms that cause addiction and negatively impact users' mental health. However, this regulation focuses more on administrative responses than on establishing clear legal responsibility for technological failures, leaving gaps in civil and criminal law.

The Australian government's efforts to develop AI Ethics Principles and an AI Action Plan 2021 demonstrate an awareness of the importance of a values framework to guide AI development (Australia Government, 2021). Additionally, reforms to the Privacy Act 1988 reflect a shift toward stricter regulation of using personal data by AI systems (Office of the Australian Information Commissioner, 2024).

As such, the Australian legal system currently stands at a crossroads; it remains reliant on common law principles that require clear legal liability, while some seek to address the challenges posed by the harms resulting from the decisions and recommendations of rapidly evolving autonomous systems. Without more profound reforms, including the adoption of risk-based liability for AI and digital platforms, a significant gap will persist between the new harms that arise and the legal system's ability to provide adequate compensation to victims.

Although comparative legal analysis of Western countries provides many important insights, it is essential to recognise that not all legal approaches from developed countries can be directly applied in Indonesia. Concepts such as *electronic* *personhood* in the EU AI Act or the model of strict liability for high-risk AI, for example, are often assumed to function effectively in systems with robust oversight institutions, adequate data infrastructure, and consistent legal interpretation. Unfortunately, these conditions are not yet fully established in Indonesia.

Let us consider the imposition of such methodologies without assessing the preparedness of our institutions. In that scenario, the study jeopardises establishing purely symbolic regulations—progressive in theory but challenging to execute in practice. This research, while mainly relying on the experiences and models of the United States, the European Union, and Australia, underscores the significance of contextual adaptation. The legal strategy adopted must correspond with the local legal culture, the capabilities of law enforcement agencies, and the prevailing socio-political dynamics in Indonesia.

VI. The Need for Legal Reform on the Indonesian Regulatory Framework

The rapid advancement of artificial intelligence (AI) necessitates urgent legislative change regarding AI liability, particularly in developing nations like Indonesia. Like industrialised nations, Indonesia must contemplate regulation revisions to tackle the legal difficulties this technological innovation poses. One measure that can be implemented is clearly defining AI responsibility inside the Criminal Code (KUHP) and establishing lex specialis laws, especially addressing this issue. Indonesia presently has a legislative void in addressing circumstances where artificial intelligence inflicts harm, particularly in fatal incidents involving autonomous AI that lead to fatalities. Consequently, there is a necessity for explicit revisions to the national legal framework.

A vital aspect of this change is the creation of categories that differentiate between harm solely attributable to AI (AI-induced harm) and negligence facilitated by AI (AI-assisted negligence). This differentiation will elucidate the implementation of criminal and civil law. In instances where autonomous AI precipitates a tragic incident absent direct human participation, such as a lethal autonomous vehicle collision, a criminal law framework predicated on strict responsibility (liability without the necessity of demonstrating fault) may be contemplated. This method facilitates justice for victims even without individual culpability, as the harm resulted from unmonitored or uncontrollable AI.

This legislative change cannot advance without a definite direction. Consequently, it is imperative to appoint principal stakeholders to spearhead this transformation. The government, via the Ministry of Communication and Information Technology (Kominfo), in collaboration with the House of Representatives (DPR RI) and the Supreme Court, must establish a cross-sector task force that includes the Attorney General's Office, the National Police, the National Cyber and Encryption Agency (BSSN), alongside academics and technology industry stakeholders.

The initial steps can begin with the development of a national policy roadmap on criminal liability within the artificial intelligence system. This roadmap should include:

(1) identifying legal gaps, (2) developing risk-based regulations for AI, (3) establishing digital evidence standards in courts, and (4) strengthening the digital forensic capabilities of law enforcement agencies.

Additionally, Indonesia must implement mandatory risk assessments before AI systems are launched, especially for applications that could impact public safety and well-being, particularly children. Safety protocols for using AI involving children (child-safety AI protocols) are crucial. Children are the most vulnerable group to the negative impacts of AI, both through algorithmic manipulation that can influence their thinking and behaviour, and exposure to harmful content that is difficult to predict. Therefore, in-depth risk assessments and stricter regulations for high-risk AI applications must be prioritised.

As a hypothetical example, imagine an AI-based chatbot used in a children's learning application. If the chatbot indirectly encourages a child to engage in dangerous behaviour, who can be held criminally liable? The software developer? The platform provider? Or the parents as users? Without a clear legal framework, cases like this would create legal uncertainty and difficulties in determining who is responsible.

From an international point of view, it is imperative to develop a legal framework for AI liability that nations can universally implement. Previous frameworks, such as the UNCITRAL Model Law on Electronic Commerce, can provide a reference for formulating AI legislation applicable across multiple nations (Burman, 1997). Due to the cross-border characteristics of AI, an international framework under the UN or OECD is necessary to create norms of transnational accountability for damages produced by AI. This circumstance would establish legal certainty and avert gaps that negligent parties can abuse. For instance, corporations that create or manage AI in one nation may relocate to a jurisdiction with less stringent legislation, thus evading accountability for the resultant harm.

In this regard, global standards governing digital safety for children and the protection of human rights in the AI era must be a top priority. Without regulatory harmonisation, gaps will emerge between legal systems in different countries, creating legal uncertainty for victims seeking justice for the harm they have suffered. These gaps could also lead to exploitative practices in the technology industry, where AI developers or service providers choose jurisdictions with weaker laws to avoid accountability for the negative impacts of their products.

However, it should be noted that overly rapid legal changes also risk overregulation, which can hinder innovation and impose heavy compliance burdens on industry. Conversely, if changes are too slow, the state will lose control over technological developments and fail to protect the public from digital risks. Therefore, legal reforms must be carried out gradually, in a participatory manner, and based on evidence (evidence-based regulation).

As AI evolves to become more autonomous and influential on both national and international scales, it is imperative for Australia and other nations to swiftly implement a legal liability framework that is not merely reactive to existing losses but also proactive in averting foreseeable losses, such as fatal incidents potentially caused by autonomous vehicles. Robust legal reforms, international cooperation, and the enhancement of human rights protection principles will be crucial foundations for establishing an equitable and accountable AI governance framework in the future.

AI will advance unbounded without deliberate intervention and regulatory alignment, rendering the resultant harm progressively more difficult to mitigate. Conversely, appropriate legislative reforms can establish a framework that safeguards individual rights and promotes secure and advantageous social innovation.

VII. Conclusion

In the tragic case of Sewell Setzer, an AI chatbot is suspected of contributing to a teenager's suicide, highlighting the need for legal reform to handle AI's complicated challenges. Criminal responsibility becomes important if AI systems like chatbots and driverless vehicles engage directly with humans. When AI causes harm or death, the question arises: should AI or its creators and operators be held accountable? Indonesian and international law struggle to solve this question. AI lacks human-like consciousness or intent, making applying criminal law ideas like *mens rea* and *actus reus* problematic. However, the abuse of autonomous AI systems underlines the need to broaden legal responsibility, including corporate and developer vicarious liability for digital entities they administer. According to this study, policymakers, engineers, and ethicists should collaborate to create AI-responsible legal procedures. The study requires these initiatives to safeguard people from AI danger and promote ethical technological development. Thus, national and international legal frameworks must change to preserve fairness, equality, and human rights in the face of advanced AI technology.

VIII. Acknowledgments:

The author would like to express sincere gratitude to the Indonesian Education Fund Management Institution (LPDP) under the Ministry of Finance of the Republic of Indonesia for sponsoring his master's study at Monash University, Australia, and for supporting the development and publication of this paper.

References:

Alhitmi, H. K., Mardiah, A., Al-Sulaiti, K. I., & Abbas, J. (2024). Data security and privacy concerns of AI-driven marketing in the context of economics and business field: An exploration into possible solutions. *Cogent Business & Management*, *11*(1), 1–9. https://doi.org/10.1080/23311975.2024.2393743

Almada, M. (2023). *Governing the Black Box of Artificial Intelligence* (SSRN Scholarly Paper No. 4587609). Social Science Research Network. https://doi.org/10.2139/ssrn.4587609

Alper, J. S. (1998). Genes, free will, and criminal responsibility. *Social Science & Medicine*, *46*(12), 1599–1611. https://doi.org/10.1016/S0277-9536(97)10136-8

Australia Government. (2021). *Australia's AI Action Plan*. Commonwealth of Australia.

Australian Law Enforcement Commission. (2015). *What is a tort?* ALRC. https://www.alrc.gov.au/publication/traditional-rights-and-freedoms-encroachments-by-commonwealth-laws-alrc-interim-report-127/17-immunity-from-civil-liability/what-is-a-tort/

Aven, T. (2023). A risk and safety science perspective on the precautionary principle. *Safety Science*, *165*, 1–12. https://doi.org/10.1016/j.ssci.2023.106211

Bathaee, Y. (2018). The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology*, *31*(2), 890–938.

Bérubé, M., Beaulieu, L.-A., Allard, S., & Denault, V. (2025). From digital trace to evidence: Challenges and insights from a trial case study. *Science & Justice*, *65*(5), 1–11. https://doi.org/10.1016/j.scijus.2025.101306

Bhat, P. I. (2020). Doctrinal Legal Research as a Means of Synthesizing Facts, Thoughts, and Legal Principles. In *Idea and Methods of Legal Research* (pp. 143–168). Oxford University Press. https://doi.org/10.1093/oso/9780199493098.003.0005

Botero Arcila, B. (2024). AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review*, *54*, 1–17. https://doi.org/10.1016/j.clsr.2024.106012

Brown, R. D. (2021). Property ownership and the legal personhood of artificial intelligence. *Information & Communications Technology Law*, *30*(2), 208–234.

Brożek, B., Furman, M., Jakubiec, M., & Kucharzyk, B. (2024). The black box problem revisited. Real and imaginary challenges for automated legal decision making. *Artificial Intelligence and Law*, *32*(2), 427–440. https://doi.org/10.1007/s10506-023-09356-9

Buell, S. W. (2022). A Restatement of Corporate Criminal Liability's Theory and Research Agenda. *Journal of Corporation Law*, *47*(4), 937–961.

Burman, H. S. (1997). United Nations: Uncitral Model Law on Electronic Commerce. *International Legal Materials*, *36*(1), 197–209.

Child, J. J., & Hunt, A. (2022). Beyond the Present-Fault Paradigm: Expanding Mens rea Definitions in the General Part. *Oxford Journal of Legal Studies*, *42*(2), 438–467. https://doi.org/10.1093/ojls/gqab033

Congress.Gov. (2023). *Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes*. https://www.congress.gov/crs-product/R47557

Davenport, T., Guha, A., Grewal, D., & Bressgott, T. (2020). How artificial intelligence will change the future of marketing. *Journal of the Academy of Marketing Science*, *48*(1), 24–42. https://doi.org/10.1007/s11747-019-00696-0

Dickinson, G. M. (2025). *Section 230: A Juridical History* (SSRN Scholarly Paper No. 5164697). Social Science Research Network. https://doi.org/10.2139/ssrn.5164697

Greenberg, A. (2024). Awareness and the Recklessness/Negligence Distinction. *Criminal Law and Philosophy*, *18*(2), 351–367. https://doi.org/10.1007/s11572-023-09687-3

Grynbaum, M. M., & Mac, R. (2023). The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work. *The New York Times*.

https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html

Hajdin, N. R. (2021). The actus reus of the crime of aggression. *Leiden Journal of International Law*, *34*(2), 489–504. https://doi.org/10.1017/S0922156521000042

Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., Scardapane, S., Spinelli, I., Mahmud, M., & Hussain, A. (2024a). Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence. *Cognitive Computation*, *16*(1), 45–74. https://doi.org/10.1007/s12559-023-10179-8

Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., Scardapane, S., Spinelli, I., Mahmud, M., & Hussain, A. (2024b). Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence. *Cognitive Computation*, *16*(1), 45–74. https://doi.org/10.1007/s12559-023-10179-8

Hern, A. (2017). Give robots 'personhood' status, EU committee argues. *The Guardian*. https://www.theguardian.com/technology/2017/jan/12/give-robots-personhood-status-eu-committee-argues

Intahchomphoo, C., Millar, J., Gundersen, O. E., Tschirhart, C., Meawasige, K., & Salemi, H. (2024). Effects of Artificial Intelligence and Robotics on Human Labour: A Systematic Review. *Legal Information Management*, *24*(2), 109–124. https://doi.org/10.1017/S1472669624000264

Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, *362*, 1–7. https://doi.org/10.1016/j.forsciint.2024.112133

Lewis Brisbois. (2024). *DOJ's Strategic Approach to Countering Cybercrime and AI Misuse – Lewis Brisbois Bisgaard & Smith LLP*. https://lewisbrisbois.com/newsroom/legal-alerts/dojs-strategic-approach-to-countering-cybercrime-and-ai-misuse

Mansar, A., & Lubis, I. (2023). Harmonization of Indonesian Criminal Law Through the New Criminal Code Towards Humane Law. *Journal of Law and Sustainable Development*, *11*(12), 1–17. https://doi.org/10.55908/sdgs.v11i12.2381

Maronie, S. (2025). *Implementasi Penanganan Barang Bukti Elektronik dan Penerapan Alat Bukti Elektronik Dalam Penyidikan Tindak Pidana Perikanan*. Kementerian Kelautan Dan Perikanan. https://kkp.go.id/news/news-detail/implementasi-penanganan-barang-bukti-elektronik-dan-penerapan-alat-bukti-elektronik-dalam-penyidikan-tindak-pidana-perikanan-99zB.html

McAuley, F. (1988). The Action Component of Actus Reus. *Irish Jurist*, *23*(2), 218–239.

Meyersfeld, B. (2025). Corporations and positive duties to fulfil socio-economic rights: Developing international human rights law. *The International Journal of Human Rights*, *29*(2), 240–281.

Montgomery, B. (2024). Mother says AI chatbot led her son to kill himself in lawsuit against its maker. *The Guardian*. https://www.theguardian.com/technology/2024/oct/23/character-ai-chatbot-sewell-setzer-death

Mordell, D. (2021). Neither physical nor juridical persons: Electronic personhood and an evolving theory of archival diplomatics. *Archives and Records*, *42*(1), 25–39. https://doi.org/10.1080/23257962.2021.1873120

Nowik, P. (2021). Electronic personhood for artificial intelligence in the workplace. *Computer Law & Security Review*, *42*, 1–14. https://doi.org/10.1016/j.clsr.2021.105584

Nuraeni, Y., & Sihombing, A. S. (2024). The Malpractice Administration Procedure in the Vortex of Crime: An Indonesian Perspective and Its Comparison with Other Countries. *JURNAL AKTA*, *11*(2), Article 2. https://doi.org/10.30659/akta.v11i2.34556

Office of the Australian Information Commissioner. (2024). *Guidance on privacy and the use of commercially available AI products*. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products

Peters, U. (2023). Explainable AI lacks regulative reasons: Why AI and human decision-making are not equally opaque. *AI and Ethics*, *3*(3), 963–974. https://doi.org/10.1007/s43681-022-00217-w

Prananingrum, D. H. (2014). Telaah Terhadap Esensi Subjek Hukum: Manusia Dan Badan Hukum. *Refleksi Hukum: Jurnal Ilmu Hukum*, *8*(1), 73–92. https://doi.org/10.24246/jrh.2014.v8.i1.p73-92

Presno Linera, M. Á., & and Meuwese, A. (2025). Regulating AI from Europe: A joint analysis of the AI Act and the Framework Convention on AI. *The Theory and Practice of Legislation*, 1–20. https://doi.org/10.1080/20508840.2025.2492524

Putra, G. A., Taniady, V., & Halmadiningrat, I. M. (2023). Tantangan Hukum: Keakuratan Informasi Layanan AI Chatbot Dan Pelindungan Hukum Terhadap Penggunanya. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *12*(2), Article 2. https://doi.org/10.33331/rechtsvinding.v12i2.1258

Rodríguez de las Heras Ballell, T. (2023). The revision of the product liability directive: A key piece in the artificial intelligence liability puzzle. *ERA Forum*, *24*(2), 247–259. https://doi.org/10.1007/s12027-023-00751-y

Roose, K. (2024). Can A.I. Be Blamed for a Teen's Suicide? *The New York Times*. https://www.nytimes.com/2024/10/23/technology/characterai-lawsuit-teen-suicide.html

Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics*, *3*, 54–70. https://doi.org/10.1016/j.cogr.2023.04.001

Stafie, C. S., Sufaru, I.-G., Ghiciuc, C. M., Stafie, I.-I., Sufaru, E.-C., Solomon, S. M., & Hancianu, M. (2023). Exploring the Intersection of Artificial Intelligence and Clinical Healthcare: A Multidisciplinary Review. *Diagnostics*, *13*(12), 1–37. https://doi.org/10.3390/diagnostics13121995

Staszkiewicz, P., Horobiowski, J., Szelągowska, A., & Strzelecka, A. M. (2024). Artificial intelligence legal personality and accountability: Auditors' accounts of capabilities and challenges for instrument boundary. *Meditari Accountancy Research*, *32*(7), 120–146. https://doi.org/10.1108/MEDAR-10-2023-2204

Steffen, B. (Ed.). (2024). *Bridging the Gap Between AI and Reality: First International Conference, AISoLA 2023, Crete, Greece, October 23–28, 2023, Proceedings*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-46002-9

Suryono, M. V. A. (2023). Legal Reforming of Smart Contract in Supply Chain Demands Process between Retailer and Consumer. *Jurnal Kajian Pembaruan Hukum*, *3*(1), Article 1. https://doi.org/10.19184/jkph.v3i1.33610

Taniady, V., & Siahaan, S. T. (2023). Artificial Intelligence and the Constitutional Court: A Newpath of Making Independent Decisions? *Jurnal Kajian Pembaruan Hukum*, *3*(2), Article 2. https://doi.org/10.19184/jkph.v3i2.41726

Taylor, G. (2004). Concepts of Intention in German Criminal Law. *Oxford Journal of Legal Studies*, *24*(1), 99–127. https://doi.org/10.1093/ojls/24.1.99

The Guardian. (2024). *Tesla settles lawsuit over 2018 fatal Autopilot crash of Apple engineer*. https://www.theguardian.com/technology/2024/apr/08/tesla-crash-lawsuit-apple-engineer

Vines, P. (2000). The Needle in the Haystack: Principle in the Duty of Care in Negligence. *University of New South Wales Law Journal*, *23*(2), 35–57.

Walker, R., Dillard-Wright, J., & Iradukunda, F. (2023). Algorithmic bias in artificial intelligence is a problem—And the root issue is power. *Nursing Outlook*, *71*(5), 1–4. https://doi.org/10.1016/j.outlook.2023.102023

Xu, Y., Liu, X., Cao, X., Huang, C., Liu, E., Qian, S., Liu, X., Wu, Y., Dong, F., Qiu, C.-W., Qiu, J., Hua, K., Su, W., Wu, J., Xu, H., Han, Y., Fu, C., Yin, Z., Liu, M., … Zhang, J. (2021). Artificial intelligence: A powerful paradigm for scientific research. *The Innovation*, *2*(4), 1–21. https://doi.org/10.1016/j.xinn.2021.100179

Zhang, L., & Xu, J. (2025). The paradox of self-efficacy and technological dependence: Unraveling generative AI's impact on university students' task completion. *The Internet and Higher Education*, *65*, 1–10. https://doi.org/10.1016/j.iheduc.2024.100978