http://dx.doi.org/10.18623/rvd.v23.5177

CRIMINAL LIABILITY IN RELATION TO ARTIFICIAL INTELLIGENCE: A COMPARATIVE STUDY OF SELECT JURISDICTIONS AND VIETNAM

RESPONSABILIDADE CRIMINAL EM RELAÇÃO À INTELIGÊNCIA ARTIFICIAL: UM ESTUDO COMPARATIVO DE JURISDIÇÕES SELECIONADAS E DO VIETNÃ

Article received on: 11/3/2025
Article accepted on: 2/3/2026

Ha Le Thuy*
*University of Law, Hue University
Hue, Viet Nam
Orcid: https://orcid.org/0000-0001-7881-2090
hlthuy@hueuni.edu.vn

Nguyen Van Nghiep**
**Faculty of Law, Da Lat University
Lam Dong, Viet Nam
Orcid: https://orcid.org/0009-0008-8550-254X
nghiepnv@dlu.edu.vn

Nguyen Thi Van Anh**
**Faculty of Law, Da Lat University
Lam Dong, Viet Nam
Orcid: https://orcid.org/0009-0004-9791-1421
anhntv@dlu.edu.vn

The authors declare that there is no conflict of interest

Abstract
Artificial intelligence (AI) has become widespread in social life, bringing many benefits and profoundly changing how people work and live. However, alongside its positive values, AI also creates significant risks, especially when exploited to commit crimes, posing challenges to the legal system, particularly criminal law. Despite this, most countries have yet to recognize AI as an independent subject of criminal responsibility. Determining criminal responsibility for AI therefore becomes a complex legislative issue in the context of digital transformation. This article examines international experiences and uses a comparative legal approach to assess the necessity of imposing criminal liability on AI. The article concludes that rather than granting AI legal personhood or treating it as a criminal actor, it is more appropriate to assign criminal liability to the human or corporate actors who develop, deploy, or operate AI systems. This ensures the core principles of modern criminal law, the stability of the legal system, and enhances adaptability to technological advancements.

Resumo
A inteligência artificial (IA) tornou-se comum na vida social, trazendo muitos benefícios e mudando profundamente a forma como as pessoas trabalham e vivem. No entanto, além de seus valores positivos, a IA também cria riscos significativos, especialmente quando explorada para cometer crimes, apresentando desafios ao sistema jurídico, particularmente ao direito penal. Apesar disso, a maioria dos países ainda não reconhece a IA como um sujeito independente de responsabilidade criminal. Determinar a responsabilidade criminal pela IA torna-se, portanto, uma questão legislativa complexa no contexto da transformação digital. Este artigo examina experiências internacionais e usa uma abordagem jurídica comparativa para avaliar a necessidade de impor responsabilidade criminal à IA. O artigo conclui que, em vez de conceder personalidade jurídica à IA ou tratá-la como um agente criminoso, é mais apropriado atribuir responsabilidade criminal aos agentes humanos ou corporativos que desenvolvem, implantam ou operam sistemas de IA. Isso garante os princípios fundamentais do direito penal moderno, a estabilidade do sistema jurídico e aumenta a adaptabilidade aos avanços tecnológicos.

Keywords: Artificial Intelligence. Criminal Law. Criminal Liability. Legal Liability

Palavras-chave: *Inteligência Artificial. Direito Penal. Responsabilidade Criminal. Responsabilidade Jurídica.*

1 INTRODUCTION

The development of various related techniques such as machine learning algorithms, big data, cloud computing, AI-specific chips, and open-source software frameworks has driven the remarkable progress of AI. AI not only possesses the ability to perceive, understand, learn, and make decisions, but is also rapidly becoming a versatile technology and an intelligent platform, widely used in many areas of the economy and society, delivering new products and services. With the widespread application of AI, many ethical issues in AI science and technology are attracting societal attention, such as: algorithmic discrimination, unfair AI decision-making, information cocoons, misuse of personal information, privacy violations, AI security, algorithmic black boxes, technology abuse, risks to employment, and impacts on social ethics. Meanwhile, thanks to impressive technological advancements over the past decade, not only can AI today perform tasks previously reserved for humans, but the development of certain autonomous and cognitive features, for example, the ability to learn from experience and make nearly independent decisions, has made them increasingly similar to agents interacting with their environment and capable of significantly altering it. However, alongside these benefits, AI also carries inherent risks, and there have even been real-world incidents causing harm to individuals, states, and society. In this context, legal liability arising from harmful actions by AI becomes a crucial issue.

Notable examples include the incident in 2018 (The Guardian, 2018), when a woman was fatally struck by a self-driving car operated by Uber in Tempe, Arizona. Most recently, a deepfake recording mimicked the voice of a Maryland high school principal, containing racist and anti-Semitic comments. (AP, 2024) The fake principal audio is an example of a branch of artificial intelligence known as generative AI. This incident raised alarm bells about the growing dangers of AI and the increasing need for stricter regulation

of this technology. In another case (The Guardian, 2024), Hugh Nelson used AI to create child abuse images by photographing children and transforming them into sexually explicit images. This was the first such case in the UK and, fortunately, was later prosecuted for child sexual abuse offenses involving the use of AI as a tool. For example, a serious workplace accident in Thailand resulted in a fatality when a worker was crushed by a robotic arm unexpectedly while bending over to spread materials. Similarly, a South Korean engineer was killed when a robotic arm mistakenly identified him as a box of vegetables, grabbed him, and pinned him to a conveyor belt, causing his death. (Dan Tri, 2024). These recent incidents around the world demonstrate that AI has been involved in causing direct or indirect harm to humans, particularly in creating criminal legal consequences.

As AI progresses and becomes increasingly prevalent, future criminal law must be adequately equipped and amended to properly address the complex issues and criminal liability associated with AI. This requires a thorough analysis of existing legal frameworks and the development of revised standards, considering the unique characteristics of AI systems and their potential implications for criminal liability. Thus, society can ensure that the legal system is adequately prepared to address any illegal activities arising from AI technology (Nanos A., 2023). Therefore, it is also time to define criminal liability for AI, or at least clearly, specifically, and in a principled maner link AI-related criminal liability to a particular entity, rather than simply relying on existing legal regulations and seeking relevant laws for interpretation and application. Given the necessity and importance of defining criminal liability for AI, the following research questions arise and need to be addressed: Can AI be held criminally liable like humans or legal entities? How do the laws of various countries around the world regulate this issue? What adjustments are needed in Vietnamese law to enable the application of criminal liability to AI?

2 RESEARCH METHODS

This article is primarily based on the analytical-synthetic method of legal studies, clarifying the theoretical basis of criminal responsibility, the constituent elements of crimes, theories on the legal status of AI, and models of criminal responsibility such as

AI as a tool, AI as an accomplice, or AI as a direct subject. Based on this foundation, academic viewpoints are systematized and critically evaluated to form the overall argument of the study.

In addition, the article employs a comparative legal method by comparing the regulations of the legal systems of several countries around the world, thereby identifying general trends and differences in approaches to criminal responsibility related to AI. The selection of countries for comparative study was based on criteria such as: the EU being a pioneer in building a comprehensive legal framework for AI, while the United States represents the world's leading AI developer, China has a strong model of state governance and tight control over technology, and Türkiye emphasizes the element of fault in its civil law system. These jurisdictions provide a comparative spectrum of regulatory models and doctrinal approaches to AI-related criminal liability.

Simultaneously, the article uses legal research methods to analyze current legal documents to assess the regulatory mechanisms and draw legislative lessons that can be inherited and applied to Vietnam.

3 RESEARCH RESULTS

3.1 Perspectives on determining the legal status and criminal liability of AI

It is undeniable that AI has been causing damage and posing threats to humans and society. Cases of harmful behavior by AI have been reported in countries around the world, such as accidents caused by robots to humans (Tue Uyen, 2023). In addition, other harmful behaviors that AI can perform include hacking into technology systems to create clones of itself; AI appropriating resources without regard for the safety of others to achieve its designed goals. AI can even obstruct traffic or cause traffic accidents. Because AI can make rules independently of its developers' intentions, it is entirely possible for AI to become a tool, like a robot, that participates in traffic and causes accidents. The entities involved in AI causing harm may include: the manufacturer of the system, the AI user or programer of the software running on that system, and the owner of the AI. So, who is considered the perpetrator of a crime and liable for criminal responsibility? To answer whether AI is subject to legal responsibility in general or criminal responsibility

in particular, it is first necessary to determine the theoretical and legal basis for establishing criminal responsibility, as well as to determine the legal status of the AI entity. Criminal responsibility is a type of legal responsibility arising from a court judgment, and therefore, if the defendant's actions cause physical or mental harm, they can be punished under criminal law (Bertolini A., Episcopo F., 2022). It can be understood that, in order to determine criminal responsibility for an entity, it is first necessary to determine whether that entity has legal capacity. If an entity has the legal capacity to be held criminally responsible for its socially dangerous actions, it must demonstrate moral capacity, that is, the ability to understand and recognize its actions and to control them according to that understanding. For contemporary AI systems, although they exhibit functional autonomy and adaptive learning capabilities, they do not possess self-awareness, free will, or moral understanding in the philosophical sense. Their "decisions" are the result of algorithmic processing, not autonomous moral consideration.

To assign criminal responsibility to a particular entity, it is necessary to base it on the traditional definition of criminal responsibility for that entity, which is the individual. To apply criminal responsibility to an individual, there must be two main elements: an external or factual element, i.e., the criminal act (actus reus), and an internal or mental element, i.e., knowledge or shared intention regarding the act (mens rea) (Hallevy G., 2010). Based on this, there are three perspectives corresponding to three models of criminal responsibility:

The first perspective views AI as a type of property, or more accurately, a type of machine used by humans as a tool or means to perform actions according to human will or desire. With this perspective, determining criminal responsibility for AI is based on the entity using that property. For example, the product of AI is robots created by humans. Therefore, if the actions of these AIs cause damage, the user or owner will be held responsible for the damage caused by the AI. They argue that AI organisms lack the ability to perceive, thus there is no legal distinction between machines used to commit crimes and the AI itself (El-Kady, R., 2024). Alternatively, another interpretation, but with a similar nature, suggests a psychological connection between behavior and attributing that behavior to the perpetrator. This psychological connection is not found in AI but is closer to that of natural humans (Bilal, A., 2010). A person accused of a crime must possess sound mental and intellectual capacity. The formation of a stable mental

and emotional state is necessary for attributing criminal responsibility (Saqr W., 2021). Therefore, it can be said that criminal behavior cannot be attributed to AI. Criminal behavior is voluntary, and will is the essence of the moral element of crime, and this only applies to humans. For a law to take effect through will, it must be conscious. This means the will must be discernible and without choice (El-Kady, R., 2024).

Corresponding to this viewpoint is the model of accountability through other accountability: viewing AI as a tool or intermediary even though the entity itself commits the harmful act. This is similar to a person using an entity that lacks criminal responsibility or is underage and suffers from mental illness or other diseases that impair cognitive abilities and/or the ability to control behavior to commit a socially dangerous act, which is considered a crime. In this case, the AI is considered innocent because it is the humans who use the AI entity to commit the crime, without using its advanced capabilities or using a very old version of an AI entity, lacking the advanced capabilities of modern AI entities.

The second viewpoint argues that AI is an electronic human. This is a new perspective in legal science in general and criminal law in particular. According to this view, considering AI as an electronic human provides a basis for AI's autonomy, allowing it to make decisions and execute those decisions as dictated by the outside world. AI can act and cause harm in ways it deduces itself. Therefore, it must be held accountable for its actions as an electronic human. While it's undeniable that AI surpasses human intelligence in some aspects, it certainly also has shortcomings in others (Watson D., 2019). Nevertheless, AI is still considered an autonomous entity within a certain framework, capable of manipulation and making judgments that may surpass human thought and ability in certain situations. Autonomy is further explained by one author as: self-awareness or consciousness, the ability to interact independently in its operating environment, and the ability to learn (Bertolini, A., 2013). Supporting this view is the approach proposed by the European Parliament in 2016: In the long term, a specific legal status should be created for AI so that at least the most sophisticated automated AIs can be established as electronic beings responsible for any damage they cause. Simultaneously, electronic legal capacity could be applied to cases where AI is capable of making autonomous decisions or interacting independently with third parties.

From this perspective, the new theory has replaced the traditional theory, which views AI and robotic systems as subjects and their owners as merely holders of the things that bear the blame, much like the owner of a regular car. Although AI moves with mental judgment nearly like humans, with logic and balance, it is not a controlled, subservient creature like a machine. Corresponding to this perspective is the natural consequential liability model. Programers or users are unaware of the offense until it has occurred; they do not plan to commit any offense and they do not participate in any part of the execution of that particular offense. Corresponding to this perspective is the direct liability model, meaning that the AI itself must be directly responsible for what it causes, without necessarily going through a specific group of people as mentioned above.

However, this view currently lacks widespread scientific consensus because it seems to contradict both traditional and modern conceptions in the history of criminal law, that the subject of criminal responsibility is only an individual or a legal entity.

The third perspective views AI as similar to a legal entity. This view has gained more consensus in the scientific community when considering another entity as similar to a legal entity. In his research, Avila argued that AI is an electronic legal entity (Avila, SMC., 2021). He reasoned that if legal personality is separated from the human foundation, there would be no way to deny legal personality to robots, as these objects do not possess any human characteristics. He also emphasized that if the law grants legal personality to assets used for specific purposes, such as robots, then the rights and obligations of those assets are not exclusive to humans. This reflects the view that AI could also have legal personality as an electronic legal entity. However, the author also stressed that when defining legal personality for this new type of entity, debates are inevitable. At the same time, continued research to confirm the existence of AI as a new entity granted legal personality is an inevitable trend in the future, especially for countries where the model for determining the legal personality of natural individuals is incomplete and not fully developed.

Traditional views only consider individuals as subjects of criminal responsibility, while modern views consider legal entities as subjects of criminal responsibility, which can be an organization or any other entity similar to an organization. Therefore, the issue of regulating criminal responsibility for AI is similar to regulating criminal responsibility for a legal entity. This is because a legal entity, or organization, is an intangible entity

without a brain or intellect, far different from the traditional subject of a human being. Similarly, AI is not a specific human being; it does not have a human brain or intellect. And if it does, it is only programed to mimic a specific human being. However, not everything that AI does constitutes an act performed by a human entity. Therefore, understanding AI's responsibility as the responsibility of a legal entity when committing dangerous acts is also a reasonable viewpoint. This will not significantly affect the process of building, enacting, or amending criminal law related to AI's criminal liability. Agreeing with this view, one author argues that if all specific objective and subjective elements of a criminal act are met, then criminal liability can be applied to any entity, such as a human, a company, or an AI entity (Hallevy, G., 2010). To support this view, another author suggests that AI may not adhere to the same rules as humans, because AI can perform tasks that humans cannot physically perform (Hu, Y., 2018). Furthermore, since some crimes only involve knowledge, it is understandable that even an AI could face criminal responsibility because it would then be equipped with sufficient knowledge, even more so than humans.

In short, it is clear that there are still dissenting views that oppose AI as a natural entity and should not impose criminal responsibility on it, based on arguments about consciousness and will—in other words, the distinction between behavior as an external, objective manifestation and fault as an internal psychological manifestation of the crime. Most scholars still argue that it is neither necessary nor advisable to impose criminal responsibility on AI, stemming from the traditional principle that individuals are the subjects of criminal responsibility, and more importantly, that this would not significantly alter criminal law to address the advancements in new technologies. Meanwhile, others continue to argue that criminal liability should be imposed on AI or that those involved with AI, such as AI programers and users, should be identified to address the challenges facing criminal law in keeping pace with the advancements in automation and AI (Beck, S., 2019).

3.2 Regulation of criminal liability in relation to AI in selected jurisdictions and Vietnam

Globally, debates about the criminal liability of AI began to emerge after the European Parliament officially adopted a civil code for robots on February 16, 2017. Since then, various studies have discussed the issue of criminal liability for AI. A notable example is Harllevy's work, which proposes three models of criminal liability for AI: (1) AI as a tool, (2) AI as an accomplice, and (3) AI directly responsible as an electronic entity (Hallevy, G., 2010). Current legal practice shows that major countries and jurisdictions do not recognize AI as a criminal subject. Instead, they clearly define AI as merely a tool, and criminal liability is placed on the human or legal entity using AI. This is demonstrated through AI-related laws enacted by countries around the world, especially technological powerhouses, such as the EU Artificial Intelligence Act 2024 and the AI Safety Governance Framework.

The European Union was the first country to enact an artificial intelligence law. This law stipulates that the following entities are subject to its regulation: (Article 2(1)): (i) Suppliers introducing or using AI systems in the EU market or introducing general-purpose AI systems (GPAI) into the EU market; (ii) AI system implementers established/located in the EU; (iii) Suppliers and implementers of AI systems in a third country, if the outputs created by the AI system are used in the EU (Hanh, 2024). Chapter 2 of this Law also stipulates prohibited AI practices in Article 5, including: acts of marketing, putting into use, or using AI systems for illicit purposes aimed at causing or potentially causing substantial harm to that person, another person, or another group of people (EU AI Act, 2024). The EU AI Act applies a tiered system of penalties and sanctions to AI system operators. Specifically: Tier 1, non-compliance with the prohibition will incur the heaviest fine under the EU AI Act – up to €35,000,000 or up to 7% of the company's annual worldwide revenue; Tier 2, non-compliance with the obligation will incur a fine of up to €15,000,000 or up to 3% of the company's annual worldwide revenue; Level 3, providing inaccurate, incomplete, or misleading information to authorities can result in fines of up to €7,500,000 or 1% of total global revenue (EU AI Act, 2024). Previously, the EU already had a legal framework related to AI through the European Union’s Treaty, which includes key provisions such as regulations concerning

obligations related to the most significant violations caused by AI applications and technologies, from Articles 7 to 13 of Chapter 3 of the Treaty (El-Kady, R., 2024).

Under German criminal law, company employees can commit various criminal offenses through AI money laundering. Specifically, fraud under Section 263 of the German Criminal Code ("StGB"), capital investment fraud under Section 264a of the StGB, misrepresentation under Section 331 of the German Commercial Code ("HGB"), or false advertising under Section 16(1) of the Unfair Competition Act ("UWG"). For example, whether fraud constitutes fraud depends in detail on whether the action created a misunderstanding among the company's customers about the use of AI in the product and whether the customers were influenced in their purchasing decisions. Without the use of AI, it is possible that these effective advertising statements constitute fraud. Offenses committed by company employees in connection with this matter can be attributed to the company and may result in legal liability for the company and its officers and directors (Hogan Lovells, 2024).

China has become one of the few countries to take the lead in enacting AI legislation to implement AI governance through legal means. Along with measures to govern AI such as proactively issuing macro-strategies and specific policies, and continuously improving technological ethics through the establishment of the National Technology Ethics Committee in July 2019, China has also prioritized ethics in effective AI governance. Therefore, the country has issued the "Convention on Self-Discipline of the AI Industry" and the "Guidelines for Reliable AI Operation" of the AI Industry Development Alliance (AIIA), the "Beijing Common Understanding on AI" and the "Declaration of Responsibility of the AI Industry" of the Beijing AI Research Institute, and the "Guidelines for Preventing Ethical AI Safety Risks" of the National Information Security Standardization Commission. In China, AI-based law enforcement is tightly integrated into the criminal justice system, utilizing technologies such as facial recognition, predictive policing, and "smart court" systems. Leveraging AI to analyze data and assist judges in decision-making often raises concerns about potential privacy violations and biased outcomes due to the massive amount of data collected and analyzed by the government (Michelle Petersen, 2022). In 2023, China issued regulations on Interim Measures for the Management of Generative Artificial Intelligence Services. Article 21 of this document stipulates the responsibilities of AI service providers.

Accordingly, service providers who violate these regulations will be subject to penalties under the Cybersecurity Law, Data Protection Law, Personal Information Protection Law, Science and Technology Development Law, and other relevant laws of China (CCAW, 2023). From a criminal law perspective, China has stipulated several offenses related to AI. However, these offenses are only aimed at prosecuting individuals and organizations that use AI as a tool to commit crimes. For example, the Chinese Criminal Code, amended in 2015, stipulates the following offenses: Anyone who uses an information network to commit any of the following acts, if the circumstances are serious, and anyone who intentionally provides technical assistance such as internet access, server hosting, network hosting or transmission of communications, or provides assistance such as advertising or payment, to others using the information network to commit crimes, if the circumstances are serious, shall be sentenced to imprisonment for a term not exceeding three years or detention, and may also be fined (Articles 287a and 287b). In addition, the law also stipulates that if an entity commits the above-mentioned crime, that entity will be fined, and the person directly responsible and other directly responsible persons will be punished according to the above-mentioned level for individuals (CLC, 2020). Although the concept of criminal liability of enterprises has been introduced, the extension of this principle to non-human entities such as artificial intelligence is still not legally resolved. Meanwhile, Chinese law stipulates that the act of using AI to insult or threaten others, causing serious consequences and disrupting social order, will be prosecuted and punished for the crime of disturbing public order under Article 293, Clause 1, Point (2) of the Criminal Code. Anyone who fabricates false information, or intentionally spreads fabricated false information on the internet, or organizes or incites others to spread such information on the internet, causing serious disruption of public order, will be convicted and punished for the crime of disrupting public order under Article 293, Clause 1, Point (4) of the Criminal Code (Procuratorial Daily, 2013). Thus, according to this regulation, AI is a digital tool or means for criminals to fabricate and disseminate false information online. For this act, the perpetrator will be prosecuted for disturbing public order. This means there is no separate crime specifically for using AI to commit crimes in China's current Criminal Code; there are only supplementary provisions regarding the use of AI to commit crimes. This regulation shows that Chinese law recognizes AI-related offenses but considers them as separate circumstances from ordinary criminal offenses.

The United States is also working to establish a national set of rules on AI through its executive branch, alongside the application of some AI-specific rules at the state level. The United States does not yet have specific regulations for the criminal prosecution of AI systems. Instead, criminal liability is assessed based on existing legal doctrines, primarily focusing on the accountability of individuals or corporations that design, control, or deploy AI technology (Mangi, D. B. et al., 2025). This also shows that U.S. law still places the emphasis of determining criminal liability on criminal intent. AI is not considered a legal entity, and therefore direct liability cannot be assigned to AI; instead, the responsibility of the entities behind it must be considered (Abdelaziz, D. K. A., 2025). For example, Section 2 of the U.S. Take It Down Act, signed into law on May 19, 2025, supplements Section 223 of the Communications Act of 1934 (47 U.S.C. 223), which addresses digital forgery involving AI. Specifically, the act of using software, machine learning, artificial intelligence, or any other technological or computer-generated means to create any visual image that clearly depicts an identifiable individual without that individual's consent may be considered a crime (related to digital forgery or related to intimate images). The penalties include fines or imprisonment for up to three years, or both. In addition, offenders may have their assets related to the crime confiscated and be required to compensate for damages caused by the violation (119th Congress, 2025).

Turkish criminal law, in Article 37, stipulates: "Every person who jointly performs acts or activities defined as crimes under the law shall be held responsible as an agent" (Turkish Penal Code, 2004). Accordingly, the subject of a crime is expressed as "anyone" or "someone," indicating that the existence of real people, human beings, is necessary for a person to be considered the subject of a crime. Furthermore, Article 21, Paragraph 1 of the Turkish Criminal Code also stipulates that the occurrence of a crime depends on the presence of the element of intent. Moreover, for an act to be recognized as a crime, it must be voluntary and capable of producing an impact in the outside world; this means that for involuntary acts, no criminal responsibility arises. (Öztürk & Erdem, 2018, p. 204). Determining the criminal responsibility associated with AI-related conduct requires an initial assessment of the typicality element within the general theory of crime, in the context of whether these acts meet the definitions and legal conditions set forth in relevant laws. However, based on current legal provisions, it can be determined that, under Turkish criminal law, non-human entities cannot be considered subjects of a crime.

On December 10, 2025, Vietnam enacted the Law on Artificial Intelligence, marking a new step forward in legislation related to AI. This law specifically emphasizes the role and importance of AI governance, entrusting the State with the authority to apply management measures corresponding to the risk level of each AI system. Management is only mandatory for systems with a clear risk of harm; it also encourages controlled experimentation, open standards, and voluntary codes of conduct. Furthermore, Article 7 of the Law stipulates six prohibited behaviors, strictly forbidding the use of AI as a tool to violate the law, especially acts of forgery, perception manipulation, harming vulnerable groups, and threatening national security and social order. The law also prohibits the use of high-tech research and testing to legitimize illegal activities. Article 29 stipulates that organizations and individuals who violate the provisions of this Law and other relevant laws concerning artificial intelligence shall, depending on the nature, extent, and consequences of the violation, be subject to administrative penalties or criminal prosecution. If damage is caused, compensation must be paid in accordance with civil law (National Assembly, 2025). Comparing this with the provisions of this Law, it can be seen that the Vietnamese Penal Code also has specific provisions on crimes to address dangerous acts related to AI that cause harm to people and society. Specifically, these include: the crime of illegally providing or using information on computer networks and telecommunication networks (Article 288), the crime of illegally accessing computer networks and telecommunication networks (Article 289), and the crime of obstructing or disrupting the operation of computer networks (Article 290). These are crimes belonging to the group of crimes against information technology. Besides this group of crimes, other offenses in the Criminal Code involve the use of AI to commit violations such as: the crime of violating the secrecy or security of correspondence, telephone calls, and telegrams (Article 159), the crime of disseminating obscene cultural products (Article 326), the crime of humiliating others (Article 155), and the crime of defamation (Article 156) using AI to fabricate or insult the dignity and honor of others. Individuals also use AI to commit fraud and misappropriate property (Article 174), using AI to impersonate voices, images, and faces for campaigning, voting, or paying personal income tax. In addition, Vietnam has enacted laws related to AI, such as the Cybersecurity Law, the Information Technology Law, and most recently, the Law on Personal Data Protection, which include regulations related to protecting cybersecurity and prohibited acts related

to AI. However, it is evident that our current legal framework lacks direct legal provisions regarding legal liability in general and criminal liability in particular for damages caused by AI, as well as lacking criminal procedural regulations applicable to cases involving AI.

Table 1

Comparative overview of laws in various countries regarding legal liability related to AI

Criteria	EU	United States	China	Türkiye	Vietnam
Specialized Legal Framework	EU AI Act 2024	No specific AI law; fragmented regulation at federal and/or state levels	No unified AI law; several specialized regulations related to AI	No specific AI law; Criminal Code applies	Artificial Intelligence Law 2025; Criminal Code
Legal Status of AI	AI is not recognized as a criminal subject	AI is not recognized as a legal or criminal subject	AI is not recognized as a legal subject	Non-human entities are absolutely excluded as criminal subjects	AI is not recognized as a subject of criminal liability
Model for Determining Criminal Liability	Liability of developers, providers, deployers, and operators	Liability of designers, controllers, and deployers of AI systems	Liability of AI service providers and users; individuals and entities may be responsible	Liability imposed only on individuals at fault in design, operation, or use	Liability imposed on users, developers, and commercial legal entities when at fault
Approach to AI-Related Offenses	Prohibits certain high-risk AI practices; significant administrative fines	Prosecuted under specific offenses (e.g., digital forgery); based on mens rea doctrine	AI treated as a tool; offenses prosecuted under traditional criminal provisions	Requires voluntary conduct and intent; AI cannot meet these conditions	Applies cybercrime provisions and traditional offenses involving AI
Policy Trend	Risk-based governance and compliance obligations; no criminalization of AI	Focus on accountability and technological control; case-based prosecution	Strong state-led governance; emphasis on prevention and AI ethics control	Protection of traditional criminal law doctrine; no expansion of subjecthood	Combines risk governance with prosecution of AI misuse; AI itself not criminalized

Based on the legal regulations in several countries around the world, including Vietnam, the following observations can be made:

Firstly, to date, no country has stipulated criminal liability for AI. Countries have not yet considered AI as an independent subject of criminal responsibility. Even though the level of automation in AI systems is increasing, legal views remain consistent: AI lacks the cognitive abilities, will, or ethics of humans to constitute fault (mens rea), and therefore cannot be a subject of criminal responsibility. Instead, countries still stipulate

indirect criminal responsibility for AI users or operators, manufacturers or programers, or legal entities—these are the entities involved in using AI as a tool to commit crimes.

Secondly, criminal responsibility in cases involving AI is determined for human entities within the technology value chain. Specifically, the relevant entities involved in the design, programing-provision, deployment-operation, and usage phases include: developers/businesses, manufacturers/operators, and exploiting organizations. Criminal liability arises for these entities when incidents or damages caused by AI occur. For example, if an AI developer makes a design error or programs an algorithm that causes the AI to commit harmful acts, the developer will be held criminally liable. If a business or manufacturer provides or deploys an AI product to customers or consumers without proper risk assessment and monitoring, neglecting safety obligations and causing damage, they may be held criminally liable. And in the operation and usage phase, if the operator or exploiter directly operates the AI and intentionally causes damage, they will be held criminally liable for their actions. This model is clearly reflected in the EU AI Act 2024/1689, the Automated Vehicles Act 2024 (UK), the Deep Synthesis Regulation 2022 (China), and the Take It Down Act 2025 (USA).

Thirdly, based on identifying the subject of criminal responsibility according to the technology value chain, the laws of various countries also recognize AI-related crimes as an aggravating circumstance, indicating a significantly increased level of danger to society compared to ordinary crimes. Countries tend to increase criminal liability for certain offenses involving the use of AI or increase penalties when AI-related crimes are committed, rather than establishing it as a separate offense.

Fourth, legislative and law enforcement practices show a trend in countries to prioritize risk prevention over punishment. This means that countries do not prioritize criminal liability for AI, nor do they criminalize the behavior of AI as an independent entity. Instead, they focus on defining criminal liability for the use or exploitation of AI, as well as establishing regulations to prevent risks from manifesting as actual consequences. This also reflects a shift in the function of criminal law in the digital age, from a traditional model emphasizing "punishment of consequences" to an approach that focuses on "prevention, control, and governance of technological risks." In this context, the scope of criminal liability is expanded to address crimes using AI as a tool, negligent

or irresponsible acts in the design and security control of AI systems, as well as the liability of legal entities when using AI for profit, fraud, or data manipulation.

3.3 Implications for Vietnam

From the legislative experiences of the aforementioned countries, it can be seen that Vietnamese law also needs timely adjustments and clear direction regarding the issue of criminal liability related to AI. This adjustment is not intended to criminalize the technology itself, but rather to control the risks arising from the design, deployment, and practical use of AI. It also aims to align with the current technological development context and to harmonize with international law and the laws of countries that are leaders in technology and have long had policies and legal frameworks related to AI and the issue of legal liability for AI users. Specifically:

First, criminal law needs to clearly define the criminalized acts involving AI, such as: using AI for fraud, information manipulation, identity forgery (deepfake), unauthorized access to data systems, dissemination of prohibited content, or creating AI products that seriously endanger national security, social order, and human rights. Specifying these acts is not intended to "criminalize AI," but rather to prevent the misuse of AI as a tool for crime.

Secondly, it is necessary to clarify the mechanism for determining criminal liability for entities that use, develop, or manage AI. In the context of AI's automation and machine learning capabilities, the key issue is not to hold the AI system itself accountable, but to determine the relationship between human behavior and the consequences caused by AI. Accordingly, liability could be placed on: (i) individuals who directly use AI to commit crimes; (ii) developers or providers of AI systems if there is intentional or serious unintentional error in design or implementation; and (iii) commercial entities if the act is performed in the name of or for the benefit of that entity.

Thirdly, in the context of rapidly developing technology, criminal law needs to be amended to combine specific and open provisions, allowing the application of traditional offenses to acts involving the use of AI, while also adding aggravating circumstances or new elements of the crime when AI increases the level of danger to society. For example, amendments could be made to recognize "the use or exploitation of artificial intelligence

systems to conceal, amplify, or commit a crime" as an aggravating circumstance in criminal liability under Clause 1, Article 52 of the current Criminal Code (National Assembly, 2015). This circumstance could be applied to crime groups such as invasion of privacy, financial fraud, production of fake content, and high-tech crimes. This approach ensures the stability of the legal system while meeting the requirements of protecting society from new technological risks.

Fourth, continue researching and refining the draft Decree guiding the newly issued Artificial Intelligence Law of 2026 as a basis for the early implementation of the Law's provisions in practice. The Decree aims to build a comprehensive legal framework for risk management of artificial intelligence systems, promote the sustainable development of the AI ecosystem in Vietnam, ensure national security, social order and safety, and the legitimate rights and interests of people; while simultaneously strengthening the effectiveness and efficiency of state management and creating favorable conditions for organizations, businesses, and individuals.

Finally, perfecting the criminal legal framework for AI must be placed within the overall national technology governance strategy, linked with other legal tools such as cybersecurity law, personal data protection, civil liability, and administrative management mechanisms. Only with synchronized coordination among legal branches can the legal system effectively control the risks posed by AI, while encouraging responsible and sustainable innovation.

4 CONCLUSION

From a comparative legal and theoretical analysis perspective, it can be asserted that recognizing artificial intelligence as an independent criminally responsible entity currently lacks a solid foundation, both cognitively and legally. Contemporary AI systems have not yet reached the level of autonomy in terms of free will, cognitive capacity, and the ability to make errors in the legal sense (mens rea) – the constituent elements of criminal responsibility. Therefore, assigning criminal status to AI not only poses a theoretical challenge but also risks eroding the core principles of modern criminal law. Furthermore, the goal of criminal law in the current context should not be the "criminalization of technology," but rather the control of technological risks and the

assurance of the principle of ultimate human responsibility. Criminal law functions to define the boundaries of socially unacceptable acts and allocate responsibility to those entities with control, foresight, and a duty to act cautiously regarding the consequences. Therefore, criminal responsibility should still be placed on individuals and legal entities involved in the design, deployment, management, or use of AI systems that cause harm.

Vietnam has designed and enacted a separate law for AI. However, because it is still in the process of adaptation and initial application based on fields where artificial intelligence applications pose risks or damages, caution is necessary in regulating criminal liability related to AI. Therefore, the proposed legal model for Vietnam in the current context, as presented in this paper, suggests: not recognizing AI as an independent criminal liability subject, but expanding the scope of criminal liability for entities that produce, use, and operate AI within the technology chain. Furthermore, the law should stipulate that the use of AI as a tool for committing crimes constitutes an aggravating circumstance for certain offenses, in order to promptly address crimes related to AI. Ultimately, the legal framework should focus on preventing the risks and dangers of AI-induced technology rather than solely on detecting and prosecuting AI-induced violations. This is because AI is not the subject of crime, but rather a test of the regulatory capacity of modern criminal law; the focus must remain on ensuring that humans, as subjects with will and responsibility, remain central to the legal order in the age of artificial intelligence.

REFERENCES

119th Congress. S.146 To require covered platforms to remove nonconsensual intimate visual depictions, and for other purposes, 2025. Available from: https://www.congress.gov/bill/119th-congress/senate-bill/146/text/is?utm. Access on: 12 January 2026.

Abdelaziz, D. K. A. A comparative analysis of legislation and international conventions regarding criminal liability for AI misuse and crimes. *Journal of Infrastructure, Policy and Development*, 9(1), 10722, 2025.

Avila Negri SMC. Robot as Legal Person: Electronic Personhood in Robotics and Artificial Intelligence. *Front. Robot. AI* 8:789327, 2021. DOI: 10.3389/frobt.2021.789327.

Beck, S. Autonomous Systems and Criminal Law – new impulses for the concept of responsibility?, 2019. Available from: https://www.inf.uni-hamburg.de/en/inst/ab/eit/about/ newsfeed/2019/ 20190703-beck.html. Access on: 22 November 2025.

Ben Finley. Deepfake of principal's voice is the latest case of being used for harm. AP, 2024. Available from: https://apnews.com/article/ai-maryland-principal-voice-recording-663d5bc0714a3af221392cc6f1af985e. Access on: 23 November 2025.

Bertolini A. Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules. *L. Innovation Techn*, 2, 214–247, 2013. DOI: 10.5235/17579961.5.2.214.

Bertolini A., Episcopo F. Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. *Front. Robot. AI* 9:842213, 2022. DOI: 10.3389/frobt.2022.842213.

Bilal, A. Principles of the Egyptian Penal Code - General Section. *Dar AlNahda Al-Arabiya*. (In Arabic), 2010.

El-Kady, R. Artificial Intelligence and Criminal Law. *In:* Tavares, M., Azevedo, G., Vale, J., Marques, R., & Bastos, M. (Eds.). *Artificial Intelligence Approaches to Sustainable Accounting*, 2024. pp. 34–52.

El-Kady, R. Challenges of Criminal Liability for Artificial Intelligence Systems. In book: *Exploration of AI in Contemporary Legal System*s. Edition 1st, Chapter 1st, Publisher IGI Global, 2024, pp.1-42.

European Parliament, Civil Law Rules of Robotics, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html. Access on: 19 December 2025.

Hallevy, Gabriel. The criminal liability of artificial intelligence entities-from science fiction to legal social control. *Akron Intellectual Property Journal*, Vol. 4, Iss. 2, 2010.

Hannah AI-Othman. Man who used AI to create child abuse images jailed for 18 years. The Guardian, 2024. Available from: https://www.theguardian.com/uk-news/2024/oct/28/man-who-used-ai-to-create-child-abuse-images-jailed-for-18-years. Access on: 5 December 2025.

Hogan Lovells. Criminal law implications and compliance strategies for AI use AI washing black box high risk AI, 2024. Available from: https://www.hoganlovells.com/en/publications/criminal-law-implications-and-compliance-strategies-for-ai-use-ai-washing-black-box-high-risk-ai#. Access on: 1 February 2026.

Hu, Y. Robot criminals. *University of Michigan Journal of Law Reform. University of Michigan. Law School*, 52, 2018.

Mangi, D. B., Butro, I., & Memon, T. A. AI and Criminal Liability: Theoretical Dilemmas in Applying Criminal Law to Artificial Intelligence. *The Critical Review of Social Sciences Studies*, 3(2), 2174-2186, 2025.

Nanos, A. (2023). Criminal Liability of Artificial Intelligence. Charles University in Prague Faculty of Law Research Paper No.2023/III/2.

National Assembly. Vietnam's Artificial Intelligence Law, 2025. Available from: https://datafiles.chinhphu.vn/cpp/files/vbpq/2026/01/luat134.signed.pdf. Access on: 2 January 2026.

Öztürk, B., & Erdem, M. R. Uygulamalı ceza hukuku ve güvenlik tedbirleri hukuku. *Seçkin Yayıncılık*, 2018.

Petersen, M. China has created the world's first AI prosecutor, Science, 2022. Available from: https://www.zmescience.com/science/china-has-created-the-worlds-first-ai-prosecutor/. Access on: 2 February 2026.

Sam Levin, Julia Carie Wong. Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian. The Guardian, 2018. Available from: https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe. Access on: 23 November 2025.

Saqr, W. Criminal liability for artificial intelligence crimes, "a prospective analytical study.". *Spirit of Law*s, 33(96), 2021.

T. Thuy. Tragedy in the factory: The moment a robot unexpectedly killed a worker. Dan Tri, 2024. Available from: https://dantri.com.vn/khoa-hoc/bi-kich-trong-nha-may-khoanh-khac-robot-bat-ngo-giet-chet-cong-nhan-20240403102515213.htm. Access on: 22 November 2025.

Tue Uyen. Accidents caused by robots to humans, Tuoi Tre Thu Do Newspaper, 2023. Available from: https://tuoitrethudo.vn/nhung-vu-tai-nan-robot-gay-ra-cho-con-nguoi-238018.html. Access on: 23 November 2025.

Turkish Penal Code, 2004. Available from: https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/Turk%C4%B1sh%20Cr%C4%B1m%C4%B1nal%20Code.pdf. Access on: 20 December 2025.

Watson D. The Rhetoric and Reality of Anthropomorphism in Artificial Intelligence. *Minds & Machines*, 2019. DOI: 10.1007/s11023-019-09506-6.

Authors' Contribution

All authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

Thuy, H. L., Nghiep, N. V., & Anh, N. T. V. (2026). CRIMINAL LIABILITY IN RELATION TO ARTIFICIAL INTELLIGENCE: A COMPARATIVE STUDY OF SELECT JURISDICTIONS AND VIETNAM. Veredas Do Direito, 23, e235177. https://doi.org/10.18623/rvd.v23.5177