

CRIMINAL LIABILITY ARISING FROM ARTIFICIAL INTELLIGENCE CRIMES UNDER OMANI LAW

Said Ahmed Said Al Yahyai¹, Izura Masdina Mohamed Zakri², Waleed Al Rushdi³

¹ Faculty of Law, Universiti Malaya, s2183308@siswa.um.edu.my

² Faculty of Law, Universiti Malaya, izuramas@um.edu.my

³ Military Judiciary, Sultanate of Oman, smile.secret55@gmail.com

Abstract: Artificial Intelligence (AI) crimes are considered complex in most of their descriptions and are modern compared to other crimes. Recently, they have become widespread, posing a risk that must be addressed through the enactment of deterrent legislation. This is due to the emergence of systems that act without direct human instruction, which strains the mental element on which criminal liability conventionally depends. The Sultanate of Oman has shown interest in digital transformation and specifically in artificial intelligence. The researchers aim to explore the legal personality of artificial intelligence and define the criminal liability arising from AI crimes. They also discuss the legal challenges in applying criminal liability provisions to AI crimes and whether there are criminal theories that could be applied to AI crimes. The study highlights the extent to which Omani criminal legislation keeps pace with AI crimes. Some writers predict that AI entities will acquire self-awareness, though this remains contested. What is not contested is that such systems increasingly act without human instruction, which presents significant challenges for investigators, judges, and legislators. The study therefore examines whether a derivative legal personality, modelled on that of companies and exercised through producers, programmers, manufacturers, and users, offers a workable basis for attributing criminal liability, rather than treating AI entities as full legal persons in their own right. The research will follow an analytical method in terms of analyzing texts in current legislation and a descriptive method in terms of formulating opinions, experiences, and developing plans and future visions to confront AI crimes. The researchers will present several results and recommendations in the conclusion of the study.

Keywords: Artificial Intelligence, Criminal Liability, Crimes, Legal Personality, Corporate Analogy, Attribution, Robot.

1. INTRODUCTION

Artificial Intelligence (AI) is among the most prominent and perilous outcomes of the Fourth Industrial Revolution. It operates through neural networks that emulate the human mind in style and method. Manufacturers predict that these networks are capable of learning and making choices like humans and believe that they will be able to self-develop and program without human intervention. It is important to note that AI technologies are still evolving rapidly, with new programs and systems emerging daily. As such, AI's presence is becoming ubiquitous in all aspects of life—home, hospitals, transportation, entertainment, industry, agriculture, education, and other essential sectors.

In line with the Vision Oman 2040, the Sultanate of Oman has shown significant interest in information technology, including artificial intelligence. This interest is evidenced by the Ministry of Transport, Communications, and Information Technology's establishment of the National Program for Artificial Intelligence and Advanced Technologies in 2022, as a key implementation program of the National Digital Economy strategy. This underscores Oman's commitment to AI technologies. The ministry's program oversees legislation that act as a safeguard by regulating and setting controls and provisions governing the field of AI.

Despite AI's notable benefits, such as enhancing efficiency, saving time, effort, and money for institutions and individuals, it is important to acknowledge that AI is a double-edged sword. While it offers numerous advantages, the



potential for crimes committed by manufacturers, programmers, owners, users, or external parties, as well as by AI itself, is expected. Issues have arisen where AI is capable of making autonomous decisions and carrying out retaliatory and aggressive actions independently. For instance, an AI-operated robot in a Volkswagen factory was involved in a human's death, another robot accidentally broke a child's finger during a chess game, a self-driving vehicle caused severe injuries to a woman, another resulted in a fatality, and an AI technology in the United States implicated a woman in a crime she did not commit; this occurred due to the American police's use of facial recognition software, which led to her wrongful accusation, though charges were later dropped due to insufficient evidence. These are not just isolated incidents but present significant legal challenges.

2. PROBLEM STATEMENT

The emergence of artificial intelligence (AI) has introduced unprecedented legal and ethical challenges, particularly in the realm of criminal liability. A pressing issue arises when AI systems act autonomously, committing crimes without direct human intervention. Such actions prompt critical questions about the allocation of criminal responsibility: Who should be held accountable? Is it the programmer, owner, manufacturer, or the AI entity itself? These questions remain unanswered in many legal systems, including Oman's, where the rapid development of AI technologies has outpaced the corresponding legislative frameworks.

AI systems are increasingly capable of making independent decisions, exhibiting behaviors akin to free will, and performing actions that may result in harm or violation of laws. This raises questions about whether AI should be granted legal personality to account for its autonomous actions. Furthermore, the concept of the mental element in criminal law—traditionally centered on intent, awareness, and design—becomes highly complex when applied to AI. How can traditional legal doctrines accommodate AI's cognitive processes? If AI is recognized as legally responsible, can traditional penalties such as imprisonment or fines be meaningfully imposed on an entity devoid of physical or economic constraints?

The absence of clear legal frameworks governing AI crimes leaves a significant gap, making it challenging for investigators, judges, and legislators to address such cases effectively. Additionally, the extent to which theories of moral agency and the conditions for liability can be applied to AI crimes remains unclear. For example, should AI systems be treated as independent moral agents, or should their actions be attributed to the humans involved in their creation or operation? These questions highlight the need for a robust legal framework capable of addressing the unique challenges posed by AI.

This study aims to bridge the gap by exploring the criminal liability arising from AI crimes under Omani law. It seeks to determine the feasibility of granting legal personality to AI entities and proposes legal solutions to address the gaps in traditional criminal theories. By doing so, the research aims to inform legislative developments in Oman and provide a foundation for aligning AI-related legal rules with traditional frameworks. The study is particularly significant given Oman's Vision 2040 and its emphasis on integrating AI into the national economy, underscoring the urgent need for a comprehensive legal approach to AI crimes.

This problem underscores the necessity for legislative and theoretical advancements to address the legal complexities of AI crimes, ensuring accountability and alignment with evolving technological realities.

3. RESEARCH SIGNIFICANCE

The existence of an independent entity that thinks, chooses, and intends its actions necessitates an investigation into the criminal liability arising from crimes committed by artificial intelligence and determining who is responsible. Experts anticipate that AI systems are capable of making autonomous decisions with their own free will, independent of the programmer, owner, or any other party involved in programming the AI. This new reality requires exploration into granting legal personality to artificial intelligence. Furthermore, the significance of this research is evident in its attempt to draw the attention of the Omani legislator to the need to create new legal rules related to artificial intelligence and to align them with traditional legal rules. Recognizing the importance of this field, the Sultanate of Oman established the National Program for Artificial Intelligence and Advanced Technologies. This confirms the expansion in the use of AI technologies. His Majesty Sultan Haitham bin Tariq – may God protect him and grant him peace – emphasized in his speech at the eighth session of the Council of Oman, stating, "We are determined to make the digital economy a priority and a pillar of the national economy, and we have directed the preparation of a national program for the implementation and localization of artificial intelligence technologies, with a push to prepare legislations that will contribute to making these technologies as one of the main enablers and stimulators of this sector." This was an inspiration in researching the criminal liability arising from AI crimes.

4. RESEARCH METHODOLOGY

The study follows a descriptive-analytical approach. The analytical approach involves analyzing the texts of current legislations, determining the most appropriate legal classification for application, and the doctrinal criminal theories related to criminal liability. The descriptive aspect involves formulating opinions and experiences and developing plans and future visions to address crimes involving artificial intelligence.

5. THE LEGAL PERSONALITY OF ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) is a branch of computer science characterized by its ability to simulate the human mind, train itself, and enhance its performance. AI processes data comprehensively and swiftly, surpassing human capabilities, and performs complex tasks rapidly, earning significant global importance. Consequently, scholars and researchers have delved into studying the essence of AI and conducting thorough research to pave the way for formulating legal rules to regulate its operations. However, it has not yet received sufficient analysis.

This chapter will be addressed in two sections: the first defining artificial intelligence, and the second discussing its legal personality.

5.1 Definition of Artificial Intelligence

Artificial Intelligence is defined as "a branch of computer science that enables the creation and design of computer programs that mimic human intelligence, allowing the computer to perform certain tasks instead of humans, which require thinking, understanding, hearing, speaking, and moving." (Al-Sharqawi, 1998)

The Research and Information Center in Abha defines it as "a simulation of human intelligence and understanding its nature through computer programs capable of emulating intelligent human behavior." (Center for Studies and Information, 2021)

Dr. Adel Abdelnour defines AI as "a science whose primary goal is to make computers and other machines acquire intelligence, enabling them to perform tasks that are still exclusively human, such as thinking, learning, creating, and communicating." (Abdelnour, 2005)

Kurzweil, one of the most renowned researchers in artificial intelligence, defines it as "the art of manufacturing machines capable of performing operations that require intelligence, as humans do." (Khaled, 2019)

Dr. Amir Farag defines it as "advanced technology aimed at simulating intelligent human behavior to produce software or intelligent machines capable of thinking and making decisions independently." (Faraj, 2023)

From the above definitions, it is evident that they all agree that artificial intelligence is a simulation of human intelligence, performing tasks characteristic of humans, such as thinking, learning, creating, concluding, and decision-making.

Upon examining Omani law, it is found that the legislator has not addressed the definition of artificial intelligence in any related legislation. No specific definition appears in the Law on Combating Information Technology Crimes, Law No. 12/2011, despite its definitions of information technology, electronic data, and information technology means in Article 1. Similarly, the Electronic Transactions Law, Law No. 69/2008, does not adopt a clear definition of AI, although it contains several definitions. While some of the definitions in these laws somewhat follow the mechanism for dealing with intelligent systems, they do not truly capture the essence of artificial intelligence. A definition should be clear and comprehensive to facilitate understanding and awareness for those addressed by the law, ensuring that a term is not interpreted contrary to the legislator's intent.

The researchers see a need to regulate artificial intelligence through specific legislation that defines the legal frameworks, rights, duties, obligations, and criminal, civil, and legal responsibilities.

5.2 The Legal Personality of Artificial Intelligence

The discussion on the legal personality of artificial intelligence in this research will be confined to the question of whether a derivative legal personality, modelled on that already conferred on companies, may be attributed to AI systems for the limited purpose of allocating liability. The study does not argue that AI entities should be granted full legal personality in their own right; the personality considered here operates through the cluster of actors behind the system—producers, programmers, manufacturers, and users. Before delving into the legal personality of artificial

intelligence, it is essential first to touch upon the types of entities recognized as having legal personality by Omani legislation, namely natural persons and juridical persons.

Historically, legal personality was initially granted to natural persons. Legal personality is inherently linked to humans and ceases with their absence. Thus, it is entirely contingent upon being born alive, as clarified by Article 29 of the Civil Transactions Law (Civil Transactions Law, 2013) and Article 301 of the Penal Code (Penal Code, 2018). Subsequently, for legal, economic, social, and political necessities, human thought led to the recognition of legal personality for juridical persons, creating a different type of legal entity. This was due to the evolution in various fields, which collectively fostered the recognition of legal personality for juridical persons, granting them a number of rights as outlined in Article 49 of the aforementioned Civil Transactions Law, most notably having an independent financial liability.

Therefore, the Omani legislator has determined that both natural and juridical persons have their independent legal personalities; the former is acquired by virtue of being born alive, and the latter upon being recognized with legal personality (either general or special juridical person).

It is crucial to clarify that legal personality is a mechanism used by the legislator to acquire rights and bear obligations imposed by the law, applicable to both natural and juridical persons. However, artificial intelligence is neither a natural person nor a juridical person but a product of technological evolution that might be considered a virtual entity. Thus, the question arises: is it possible to recognize legal personality for it?

The recognition of legal personality for artificial intelligence has sparked debate similar to that seen in the early 19th century when legal personality was granted to juridical persons due to legislative gaps in various legal issues. This prompted Western legislators to adopt and recognize this legal status, affirming that legal personality is a legal acknowledgment rather than an innovation. Similar controversy arose in 2015 when French legislation adopted a new legal status for animals, defining an animal as "a living being with the characteristic of sentience, subject to laws that protect it, governed under the legal system of things." This led some to regard it as a recognition of a special type of legal personality for animals, as the system, when granting legal personality, considers two aspects: the subject of the right ("things") and the bearer of the right ("persons"). Granting animals a legal status broke from the general principle by creating a third category between things and persons, which prompted the amendment of many legal texts to align with the new legal status of animals.

Following this precedent, some scholars argue that artificial intelligence deserves recognition within a framework of ethical and legal rules that delineate its boundaries (Al-Khatib, 2020, pp. 16–17). The present study does not follow that argument as far as a distinct personality standing alongside natural persons, juridical persons, and animals. The corporate analogy is the more defensible route: personality is conferred for defined purposes and exercised through identified human actors (Novelli, 2023).

The legal and realistic need imposes the recognition of legal personality, and therefore, with the continuous and rapid development of artificial intelligence systems entering various fields, and their capability to act with independent will from their creators, holding them criminally responsible for their actions can only be achieved by recognizing their legal personality, analogous to juridical persons (Idlabi, 2023, p. 62).

The European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics asked the Commission to explore the possibility of establishing a specific legal status for the most sophisticated autonomous robots, so that they might be treated as electronic persons responsible for making good any damage they cause (European Parliament, 2017). This applies particularly when robots emerge with the ability to think, adapt, learn, and make decisions autonomously without human intervention (Jahloul & Odeh, 2019, p. 764). That position did not survive. In its resolution of 20 October 2020 on a civil liability regime for artificial intelligence, the European Parliament stated that any change to the existing legal framework should begin from the clarification that AI systems have neither legal personality nor human conscience, and that harm involving such systems is nearly always the result of someone building, deploying, or interfering with them (European Parliament, 2020). The European position has therefore moved away from electronic personhood and towards allocating liability among identifiable human and corporate actors (Nowik, 2021; Gless & Ligeti, 2024).

The researchers accept the narrower proposition that legal personality need not be confined to human beings, as reflected in the idea that "all humans are persons, but not all persons are humans." What follows from this, however, is only that personality may in principle be conferred on a non-human entity by legislative choice, in the way it is conferred on a company. It does not follow that intelligent robots should hold full legal personality in their own right. According to this perspective, the concept of a person is not meant to refer only to natural persons. It is necessary to

distinguish between a person and a human, considering that a person is a human reality before being a legal concept. In the field of law, a person is one who possesses legal personality. Thus, in legal language, it is inappropriate to conflate the terms person and human, as they are not synonymous. Some have argued that the basis of legal personality is not consciousness, will, or human characteristic, but includes social value (Nassakh, 2020, pp. 220–221; Al-Qousi, 2018, p. 77).

This perspective further asserts that as artificial intelligence, such as robots, becomes capable of making and implementing decisions independently of human intervention, it cannot be considered a mere object under the supervision of others (the manufacturer, owner, user, designer, programmer). Instead, its autonomy must be reflected in how liability is allocated. This does not mean that any entity possessing self-awareness and independent will thereby qualifies for legal personality; it means that the law must identify which human or corporate actor bears responsibility for the system's autonomous output. This is the objective pursued by the European Parliament through the recommendation agreed upon in February 2017, which advises the European Commission to establish specific rules for robots, including granting them legal personality, financial liability, and rights. The European legislator has moved towards giving robots a special legal status in the future as new generations emerge, which will lead to granting rights to them and imposing obligations upon them. The purpose of this regulation is to clarify responsibilities in the event of damage, where evidence can be presented for the damages and the causal relationship between the damages and the harmful behavior of the robot (Nassakh, 2020, pp. 221–222).

Regarding the extent to which artificial intelligence possesses perception, studies have shown that a relationship of friendship and empathy between humans and machines will develop. Some scholars further propose a transitional stage from artificial intelligence to artificial perception, on the view that such systems may eventually display creativity and simulate human emotional responses. This remains a contested proposition rather than an established finding, and there is at present no evidence that such systems are aware of the actions they perform. Thus, the moral element in artificial intelligence will be realized through the sensory reception of data, its analysis, and understanding. Most artificial perception entities are equipped for such sensory receptors, visual and auditory perceptions, physical connectivity, touch, and more. Through the analysis of this data, artificial intelligence entities attempt to mimic the processes of understanding and perception characteristic of natural humans (Al-Haddam, 2022, pp. 136–137).

Geoffrey Hinton, often regarded as the godfather of artificial intelligence, left his post at Google in May 2023 in order to speak freely about the risks of the technology, warning that AI systems may become more intelligent than people and may learn to manipulate them (Metz, 2023; Al-Shamikh, 2023). His warnings concern the safety and controllability of AI systems. He does not argue that such systems should be granted legal personality, and the present study does not treat his remarks as support for that proposition.

Accordingly, there arises a need for a special legal framework for artificial intelligence in the Sultanate of Oman. Rather than recognising AI entities as full legal persons, such a framework should confer a derivative personality on the AI system on the model already used for companies, so that the system can serve as a point of legal attribution while responsibility is borne by the producers, programmers, manufacturers, and users behind it. This includes establishing ethical rules governing AI and granting the framework recognition in criminal law so that certain general rules, as will be explained in the second section, may apply. This recognition is inevitably forthcoming due to the rapid and limitless development of artificial intelligence, which has invaded our societies and become reliant in various fields. It has been argued that AI systems will become capable of making autonomous decisions without human intervention, though claims that they will possess consciousness remain contested and unproven. Even where autonomy weakens the causal link between an AI error and its manufacturer, the appropriate response is not to treat the system as an independent person but to allocate responsibility across the actors who designed, produced, deployed, and used it. The primary purpose of this recognition is to determine the criminal liability arising from it, not to grant it the rights enjoyed by humans. This is because it will be difficult in the future for victims to trace who is responsible for the harm caused by independently decision-making AI due to the involvement of multiple individuals in its creation or use as a smart machine (producers, programmers, owners).

6. Criminal Liability Arising from Crimes Committed by Artificial Intelligence

The criminal liability resulting from the actions of artificial intelligence poses a challenge to criminal law scholars, as mentioned in the first chapter, especially when a smart machine commits a crime independently of human intervention. It is known that criminal liability is based on a fundamental principle in criminal law, the principle of personal punishment, which means that the penalty prescribed by law is imposed on the perpetrator of the crime and does not extend to others. This principle is emphasized by the state's basic law (Basic Law of the State, 2021) in Article 26, which states, "Punishment is personal." This is also reinforced by the Penal Code in Article 4, which states, "No

person shall be held accountable for another's crime." Additionally, for criminal liability to be established, it must be prescribed by law, applying the principle of legality of penalties, which is referred to in the aforementioned Article 26 of the state's basic law and Article 3 of the Penal Code, both of which stipulate, "There is no crime and no punishment except by law."

This chapter focuses on identifying the parties responsible in these crimes to determine the appropriate legal rules to apply, whether to a human or a sentient smart machine, and the legal issues facing the application of criminal liability provisions to AI crimes. It is organized as follows: First Section: Parties of Criminal Liability in AI Crimes Second Section: Legal Issues in Applying Criminal Liability to AI Crimes

6.1 Parties of Criminal Liability in AI Crimes:

The parties linked with criminal liability in this type of crime are the manufacturer or programmer, the owner or user, the external party, and the artificial intelligence itself. It is essential to initially identify these parties and determine the possibility of applying the theory of moral agency to the first three parties in cases where they commit intentional or unintentional crimes.

6.1.1 the Manufacturer or Programmer:

The criminal liability of the manufacturer or programmer of artificial intelligence arises when the act emitted by the AI is attributed to the manufacturer or programmer and constitutes a criminal offense, and they have contributed to it. This is the case, for example, if the AI is manufactured and programmed in such a way that it commits a crime intentionally (Itmaizi, 2022, p. 64), like killer robots and drones programmed to engage in criminal conduct such as murder (Idlabi, 2023, p. 90), taking into account that the crime may occur due to a programming error by the AI programmer, such as releasing AI technology with errors that cause criminal offenses. It is necessary to distinguish between intentional and accidental commission of the crime to determine whether the crime was committed deliberately or by mistake. The study of the manufacturer's criminal liability is particularly significant in this regard, as the manufacturer may protect themselves by including terms in the usage agreement signed by the owner or user that absolves them of liability and assigns criminal liability for crimes committed by the AI to them (Dahshan, 2020, p. 127).

In fact, the situations mentioned regarding the liability of the manufacturer or programmer align with the theory of moral agency, where the nature of the robot here corresponds with a legally unaccountable person who lacks consciousness and perception. We see, along with some scholars, that analogy in this case is not prohibited; because it is an analogy in rules related to eligibility and not punitive rules related to the principle of legality of punishment (Hassan, 2022, p. 28).

Thus, the researchers propose the possibility of applying the theory of moral agency provided for in Article 37(c) of the Penal Code only to non-sentient AI entities that are not recognized as having artificial perception, whether for intentional crimes or various forms of negligent crimes. However, it is seen that for this theory to be applied to AI entities, the current text needs to be amended by replacing the term "others" with "the last person" since the term "others" includes both humans and machines, and by adding "or does not possess artificial perception" at the end of the paragraph. This is because AI entities that possess artificial perception will bear responsibility themselves with penalties appropriate to their nature when they are recognized as having legal personality. The article would read after the proposed amendment, "Whoever employs another by any means to carry out the act that constitutes the crime, if this other is not criminally responsible or is well-intentioned or does not possess perception."

6.1.2 The Owner or User:

The owner or user is the individual who receives the product or machine and utilizes it for their service or for serving their clients in various fields, such as medicine, industry, or security, among others. Typically, this person is the controlling or monitoring party over the machine's performance, operating it based on their instructions, such as performing surgical operations (Al-Mulla, 2021, pp. 111–112). There are possibilities of intentional crimes caused by the owner or user, such as disabling the automatic control in self-driving cars while keeping the AI's voice commands active. In this scenario, if the owner or user is warned by the AI to avoid a specific incident and fails to comply, they alone would bear criminal liability if a particular crime occurs (Dahshan, 2020, p. 129). Additionally, crimes by AI could occur due to unintentional mistakes by the owner or user, and they would bear criminal responsibility accordingly (Abdullah & Awani, 2023, p. 12).

Following the principles discussed above, the owner or user can be held accountable according to the theory of moral agency and the general principles of criminal liability for criminal outcomes resulting from the use of AI applications, whether intentional or accidental, depending on the form of the mental element involved. There is no legal barrier to addressing non-intentional criminal liability for owners and users of smart applications if they are incompetent to handle them, such as if someone in the medical field uses them without sufficient technical skill for that use. This means that determining the criminal liability of the owner or user depends on the assumption of their ability to supervise and prevent the harmful outcome that necessitates criminal accountability. Therefore, they bear responsibility in cases of non-intentional mistakes arising from oversight (Jindi & Omar, 2020, p. 232).

It's also possible that a crime occurs due to the behavior of the owner or user with other parties (the manufacturer and programmer, the AI technology itself, or an external party). For instance, a car owner may alter the operating commands in a self-driving car with the help of a specialist to use it to commit a crime and shift the responsibility away from themselves and onto the car and its manufacturer. In such cases, the criminal liability is shared between the owner and the assistant (Al-Dessouki, 2022, p. 1181), which is covered by the rules of contributory liability provided in Article 38 of the Penal Code. By examining this text, we urge the Omani legislator to add in the last paragraph of the article, "Rules of participation apply to AI entities that possess artificial perception," to address defenses that may argue the non-applicability of participation rules to AI entities proven to have awareness and artificial perception.

6.1.3 The Artificial Intelligence System as a Point of Attribution:

This refers to the smart machine, intelligent agent, delegate, android, or robot, among other terms indicating the perception and interaction of artificial intelligence. It operates autonomously through deep learning algorithms that enable it to think, move, initiate, and evolve, as well as make decisions independently of human intervention (Al-Mulla, 2021, p. 112).

Some scholars equate artificial perception with human cognitive perception, arguing that it enables AI entities to discern their surrounding circumstances. That equivalence is contested, and it does not establish comprehension in the sense criminal law requires of a culpable actor. What can be said is that such systems increasingly operate without direct instruction from their manufacturer, programmer, or owner. Where an AI system causes harm without direct human intervention, using capabilities that sometimes exceed those of humans, the difficulty is not that a new criminal subject has emerged but that the existing subjects are harder to identify (Al-Haddam, 2022, pp. 143–144). On the corporate analogy, liability in such a case attaches to the system as a legal construct and is discharged through the producers, programmers, manufacturers, and users who stand behind it, in the same way that corporate criminal liability operates through the natural persons who act for the company (Simmler, 2024).

Another possibility for attributing criminal liability to this entity involves the participation of one of the parties (the owner or user, the manufacturer or programmer, or an external party) with the artificial intelligence in committing the crime, thereby becoming partners in the crime. For example, a smartphone user might root the phone, allowing applications to control the device (the AI entity), and give it commands that harm other applications or people through those applications (Idlabi, 2023, p. 96).

6.1.4 The External Party:

The criminal liability of the external party arises when they hack into artificial intelligence systems by any means, take control of them, and use them to commit crimes, such as an external party unlawfully entering a computer system, implanting viruses, or seizing stored data and information (Saqr, 2021, p. 131). The external party's liability can take two forms:

1. Exploiting a vulnerability in artificial intelligence entities to commit a crime, which was a result of negligence by the manufacturer, programmer, or owner. In this case, the criminal liability is shared between the external party and the party whose negligence facilitated the exploitation of the vulnerability. An example of this is an AI owner negligently giving access codes to the AI's control systems to an external party, facilitating the latter's issuance of commands to the AI (Moussa & Belal, 2020, pp. 40–41).
2. Exploiting a vulnerability in the artificial intelligence technology without assistance or negligence from the aforementioned parties. In this case, the responsibility falls solely on the external party, such as hacking into the cloud storage (Tigareti, n.d.) used to store and send commands to the AI technology, subsequently issuing commands to the AI to commit a specific crime, such as an external party programming the AI to attack individuals with certain characteristics, like skin color or specific attire (Dahshan, 2020).

6.2 Legal Challenges in Applying Criminal Liability to AI Crimes

Applying criminal liability provisions to AI crimes is not limited to identifying the responsible parties and determining appropriate penalties for these entities. It also raises several legal challenges that require examination and resolution to find suitable legal solutions. Therefore, we review some legal challenges and suggestions for addressing them, drawing the attention of legislators and researchers to consider them more deeply. These include:

6.2.1 The feasibility of applying defenses to criminal liability concerning crimes committed by artificial intelligence:

The discussion on defenses to criminal liability for crimes committed by AI only arises if these entities are granted legal personality based on their artificial perception. The question then is, can defenses to liability be applied to AI crimes? Some suggest that this is possible, allowing for the exemption of sentient AI entities from punishment if an external source intervenes, hacks the AI entity, and influences its behavior, leading to its inability to control its actions. Thus, the crime would not be attributed to it (Dahshan, 2020, p. 121). For the application of defenses to liability, it is required that the AI entity be aware and capable of sufficiently discerning its actions, then an external source disrupts its autonomous capabilities or affects them in any way, or causes a malfunction in its electronic mind by attacking it with viruses that impair or eliminate its perception and will (Al-Haddam, 2022, p. 155).

Upon reviewing the provisions regulating defenses against criminal liability in the penal code, we find that natural persons under the age of nine at the time of committing the crime, as outlined in Article (49), benefit from these defenses. Additionally, those who were insane at the time of the crime and lacked perception or will, or who suffered from a mental defect, or were in a coma resulting from the involuntary or unknowing consumption of drugs or intoxicants, or for any other reason determined by science to cause loss of perception or will, as stated in Article (50), are also exempted from liability.

Furthermore, necessity as a defense is available to those compelled to commit a crime to protect themselves, their property, or their honor, or that of others, from an imminent grave danger, without their will contributing to the situation, and the crime must be necessary and proportionate to the danger, as confirmed by Article (51).

The researchers support the scholarly view that defenses against liability could be applicable to artificial intelligence entities with artificial perception that are recognized as having legal personality, analogously to the Omani legislator's exemption of those lacking perception or will from liability, as in Article (50) of the penal code. However, it is necessary to specify defenses against liability either in a special law concerning artificial intelligence or by amending the section on defenses in the penal code, as it does not currently apply to these entities.

6.2.2 The feasibility of self-defense rights for artificial intelligence entities:

The feasibility of self-defense rights for artificial intelligence entities is also considered. Self-defense is recognized as a condition that negates liability, and the penal code addresses this in Articles (46-48), concluding that legitimate self-defense is only permissible in defense of a human life. Therefore, under these legal provisions, AI entities cannot defend themselves or others, even if they possess artificial perception, despite what is stated in Article (46): "There is no crime if the act is performed in legitimate self-defense... when the defender faces a danger to himself, his dignity, his property, or that of others..." However, if an AI-operated robot is used by its owner for self-defense, does it have the right to defend its owner if attacked?

The penal code's provisions on legitimate defense address natural persons, whether defending or being defended against, but they do not permit a sentient robot (android) to defend its human owner or user (Al-Dessouki, 2022, p. 1189). Opinions differ on the possibility of a robot defending its owner under two scenarios. Some scholars believe that if a robot, equipped with advanced systems, can balance between an attack on its owner and its own defensive actions, it might be possible for it to act in defense (Al-Haddam, 2022, p. 153). If this capability is absent in the robot, then the owner fully bears the criminal liability for any harm the robot causes to others while defending its owner, considering the robot merely as an instrument of crime in this case (Sweif, 2022, p. 149).

In response to the question of whether artificial intelligence entities have the right to self-defense, we align with the view that distinguishes between two scenarios: If the robot, like a human, has the capacity for bounded rational behavior and can proportionately defend itself, then it should be allowed to defend itself from any attack by a human or another robot (Dahshan, 2020, p. 120). Since we recognize its liability and demand proportionate punishment, logically, we must also support this view to prevent the robot from being defenseless against attacks. However, if the robot lacks the capacity for discernment in movement, thought, and reaction, then it should not be permitted to use

the right to self-defense, to ensure human safety, given that humans are irreplaceable, unlike machines (Al-Dessouki, 2022, p. 1190).

6.2.3 The applicability of duty performance and legal authorization defense to artificial intelligence:

The applicability of duty performance and legal authorization defense to artificial intelligence is discussed. The penal code refers to this defense in Article (45) when a public official acts in compliance with a legal duty or lawful order from the competent authorities, or if the act is committed in good faith in execution of a law. The researchers pose two questions: Will the world see a new kind of public official in AI entities? And what is the extent to which the duty performance and legal authorization defense applies if AI is considered a public official?

Given the advancements in AI and its expected future capabilities in thinking, analysis, perception, and awareness, AI is likely to be present in various institutions. In 2018, Saudi Arabia employed a robot in a governmental role in the Ministry of Education, a step aimed at enhancing the public sector's development in the kingdom, even issuing the first ID card to an automated public employee (Sky News Arabia, n.d.). The researchers believe that the world will witness genuine public employment of AI entities, especially robots, in the public and even private sectors.

In conclusion, regarding the question of whether the duty performance and legal authorization defense applies to AI, we believe that this defense can apply to AI entities considered public officials, provided they possess legal personality.

The researchers also raise questions that require further exploration: Can AI entities experience physical or moral coercion? Consequently, another question arises: To what extent can AI entities that are forced to commit a specific crime due to physical or moral coercion be exempted from liability based on available defenses? Another question is whether it is conceivable that AI entities will have ages that determine their perception and awareness, and whether the world will set ages for AI entities similar to the way a human under nine is not held liable. Finally, are the penalties in the penal code, designed for deterring morally complex humans with emotions, suitable for new intelligent entities? It appears that these penalties, designed to instill remorse and regret, may not be appropriate for entities without such feelings, an issue that science may reveal in the future. However, the researchers believe that the existing penalties in the penal code are not suitable for these entities if they are recognized as having legal personality.

7. CONCLUSION:

Criminal liability for crimes arising from artificial intelligence (AI) presents numerous legal challenges and issues, due to AI's current capabilities of making autonomous decisions, independent of human intervention, and its ability to self-improve. Thus, AI might commit crimes more severe than those typically committed by humans. Therefore, AI entities should not be viewed as one homogeneous group; distinctions must be made based on their decision-making autonomy and level of development. AI cannot merely be seen as silent tools and machines whose actions are solely the responsibility of their owners or users. Some AI entities, as this research has demonstrated, will achieve a level of artificial perception necessitating that they be held accountable for crimes they commit independently of their owners or users.

It is crucial for the Omani legislator to address the rules of criminal liability in relevant laws, to amend some of these, and to create new legal provisions that can accommodate a new legal personality in the future—that of AI entities with artificial perception. It is also necessary to devise penalties appropriate for AI entities and other provisions that address crimes committed by responsible parties in AI-related crimes, and to address the legal challenges that may arise in applying the provisions of criminal liability.

The research concludes with several findings and recommendations, as follows:

8. FINDINGS:

The study reveals that artificial intelligence (AI) is currently one of the most complex and controversial topics, particularly in the legal domain. Despite its rapid advancement, Omani penal laws and other similar legislations have not yet addressed the issue of criminal liability for AI-related crimes. While the Cybercrime Law and the Electronic Transactions Law offer some guidance on dealing with smart systems, their definitions fall short of capturing the essence of AI.

A pressing need exists for legal systems to provide a clear basis for attributing liability when AI systems cause harm. The continuous and accelerated development of these systems, and their growing capacity to act without direct human instruction, underscores their potential to cause harm for which no responsible party is readily identifiable. The

evidence does not, however, support the claim that recognition of full legal personality for AI is inevitable; the trend in comparative practice runs in the opposite direction (European Parliament, 2020).

There is no inherent legal obstacle to conferring a derivative legal personality on an AI system, on the model already used for companies, provided its scope is limited to the attribution of liability. Claims that AI cognition will reach a stage of creativity and human-like emotion remain speculative and cannot carry the weight of such a recognition. The purpose of any such personality is not to grant AI the rights enjoyed by humans, nor to constitute it as an autonomous criminal subject, but to provide a stable point through which liability can be traced to the producers, programmers, manufacturers, and users behind the system.

The study also identifies key parties associated with criminal liability for AI-related crimes: the manufacturer or programmer, the owner or user, the AI system itself, and third parties. While the theory of moral agency can apply to these parties, it does not extend to the AI system itself. In cases where AI is deliberately misused or negligently handled by its owner or user, resulting in criminal acts, liability is attributed to the human parties. Where the system acts without direct instruction, liability should be distributed among the producers, programmers, manufacturers, and users according to their respective contributions, in the manner of corporate criminal liability, rather than assigned to the system as an independent offender (Ellamey & Elwakad, 2023; Simmler, 2024).

9. RECOMMENDATIONS:

Based on the findings, the study makes the following recommendations:

1. **Derivative Legal Personality for AI Systems:** Rather than recognising AI entities as full legal persons, the legislator should confer a limited, derivative personality on AI systems on the model already applied to companies. Its sole function would be to provide a point of attribution through which criminal liability is traced to the producers, programmers, manufacturers, and users responsible for the system.
2. **Legislation for AI Legal Frameworks:** A specialized legal framework should be developed to define the derivative legal personality of AI systems and the allocation of responsibility among the actors behind them. This framework should also establish ethical guidelines for AI governance and propose penalties tailored to the unique nature of intelligent entities, ensuring effective deterrence.
3. **Capacity Building for Omani Youth:** Efforts should be made to equip Omani youth with the skills and knowledge necessary to keep pace with advancements in AI technology. This includes training programs that focus on understanding AI cognition and its ability to operate autonomously from human oversight.
4. **Preliminary Legal Regulations for AI Ownership:** Legal conditions and prerequisites should be introduced as an interim measure for individuals seeking to own physical AI entities, such as robots or autonomous vehicles, until comprehensive legislation governing their use is enacted.
5. **Mandatory Insurance for AI Entities:** Robots, autonomous vehicles, and other AI-driven systems should be insured to ensure compensation for individuals harmed by AI actions. This would provide a safety net for victims and foster accountability within AI operations.

References

Books and Articles:

1. Abdelnour, A. (2005). *Introduction to the world of artificial intelligence*. King Abdulaziz City for Science and Technology.
2. Abdullah, A. K., & Awni, M. (2023). Criminal liability for the use of robots: A comparative study. *Al-Farabi Journal of Humanities*, 2(2).
3. Al-Dessouki, M. M. A. (2022). Crimes of artificial intelligence technologies and independent electronic legal personality: A comparative study. *Journal of Legal and Economic Research*, (81).
4. Al-Haddam, S. (2022). *Law in the face of artificial intelligence: A comparative study* [Master's thesis, Sidi Mohamed Ben Abdellah University].
5. Al-Khatib, M. I. (2020). Artificial intelligence and the law: A critical comparative study of French and Qatari civil legislation. *Journal of Legal Studies*, Ahmed Bin Mohammed Military College.
6. Al-Mulla, M. S. (2021). The historical dimensions of the development of the theory of criminal liability and the dialectics of its application in the era of artificial intelligence: An analytical and prospective study. *Journal of Kuwait International Law College*, 10(Special Supplement).
7. Al-Qousi, H. (2018). The problem of the person responsible for operating the robot: The impact of the "Human Proxy" theory on the feasibility of future law. *Jil Journal of Advanced Legal Research*, (25).

8. Al-Sharqawi, M. A. (1998). *Artificial intelligence and neural networks* (1st ed.). Center for Publishing.
9. Center for Studies and Information. (2021). *Artificial intelligence*. Abha Chamber.
10. Dahshan, Y. I. (2020). Criminal liability for artificial intelligence crimes. *Journal of Sharia and Law*, 34(82), 100–144.
11. Ellamey, Y., & Elwakad, A. (2023). The criminal responsibility of artificial intelligence systems: A prospective analytical study. *Corporate Law & Governance Review*, 5(1), 92–100. <https://doi.org/10.22495/clgrv5i1p8>
12. European Parliament. (2017). *Civil law rules on robotics: European Parliament resolution of 16 February 2017 with recommendations to the Commission* (2015/2103(INL)).
13. European Parliament. (2020). *Civil liability regime for artificial intelligence: European Parliament resolution of 20 October 2020 with recommendations to the Commission* (2020/2014(INL)).
14. Faraj, A. (2023). *Rules of liability for operating AI robots in civil and criminal contexts for damages caused: A comparative study* (1st ed.). University Publications Press.
15. Gless, S., & Ligeti, K. (2024). Regulating driving automation in the European Union – criminal liability on the road ahead? *New Journal of European Criminal Law*, 15(1), 33–57. <https://doi.org/10.1177/20322844231213336>
16. Guerra, A., Parisi, F., & Pi, D. (2022). Liability for robots II: An economic analysis. *Journal of Institutional Economics*, 18(4), 553–568. <https://doi.org/10.1017/S1744137421000837>
17. Hassan, M. G. I. (2022). Criminal liability arising from the harms of using artificial intelligence in the medical field: An analytical study. *Journal of Legal and Economic Studies*, (8).
18. Idlabi, O. M. M. (2023). *Criminal liability for artificial intelligence acts* [Master's thesis, Qatar University].
19. Itmaizi, S. A. A. (2022). *Artificial intelligence under criminal law* [Master's thesis, Al-Quds University].
20. Jahloul, K. H., & Odeh, H. A. (2019). Civil liability for damages caused by robots: A comparative analytical study. *Route Educational & Social Science Journal*, (5).
21. Jindi, K. Y., & Omar, D. A. P. (2020). Applications of the theory of moral agency in crimes resulting from artificial intelligence. *Al-Qadisiyah Journal of Law and Political Science*, 11(2).
22. Khaled, A. B. (2019). *Applications of artificial intelligence as a modern approach to enhancing the competitiveness of business organizations* (1st ed.). Arab Democratic Center for Strategic, Political, and Economic Studies.
23. Moussa, O., & Belal, W. (2020). *Legal implications of using artificial intelligence* [Master's thesis, Ziane Achour University].
24. Nassakh, F. (2020). The legal personality of the new entity: “The virtual person and the robot.” *Al-Ustath Al-Bahith Journal for Legal and Political Studies*, 5(1).
25. Novelli, C. (2023). Legal personhood for the integration of AI systems in the social context: A study hypothesis. *AI & Society*, 38(4), 1347–1359. <https://doi.org/10.1007/s00146-021-01384-w>
26. Nowik, P. (2021). Electronic personhood for artificial intelligence in the workplace. *Computer Law & Security Review*, 42, 105584. <https://doi.org/10.1016/j.clsr.2021.105584>
27. Saqr, W. M. M. A. (2021). Criminal liability for artificial intelligence crimes: An analytical and prospective study. *Journal of the Spirit of Laws*, 96(96).
28. Simmler, M. (2024). Ensuring accountability for robots and AI under criminal law. In W. Barfield, Y.-H. Weng, & U. Pagallo (Eds.), *The Cambridge Handbook of the Law, Policy, and Regulation for Human–Robot Interaction* (pp. 798–812). Cambridge University Press. <https://doi.org/10.1017/9781009386708.050>
29. Sweif, M. M. (2022). *Artificial intelligence crimes: The new criminals* (1st ed.). New University Press.
30. Zahra, M. M., & Abu Zaid, M. M. (2018). *An introduction to legal studies according to Omani law* (1st ed.). University Book Publishing House.

Laws:

31. Basic Law of the State. (2021). Royal Decree No. 6/2021 issuing the Basic Law of the State. *Official Gazette*, Issue No. 1374, issued on January 11, 2021.
32. Civil Transactions Law. (2013). Royal Decree No. 29/2013 issuing the Civil Transactions Law. *Official Gazette*, Issue No. 1012, issued on May 12, 2013.
33. Penal Code. (2018). Royal Decree No. 7/2018 issuing the Penal Code. *Official Gazette*, Issue No. 1226, issued on January 11, 2018.
34. **Websites:**
35. Al-Shamikh, I. (2023, May 15). "The sorcerer's trick backfired: Why did Geoffrey Hinton, the godfather of AI, decide to resign now?" *Al Jazeera Midan*. Retrieved from <https://www.aljazeera.net/midan/miscellaneous/technology/2023/5/15> (Accessed December 8, 2023).
36. Metz, C. (2023, May 1). "The godfather of A.I." leaves Google and warns of danger ahead. *The New York Times*. <https://www.nytimes.com/2023/05/01/technology/ai-google-chatbot-engineer-quits-hinton.html>
37. Sky News Arabia. (n.d.). "Techni" the robot: The first robotic employee at the Ministry of Education in Saudi Arabia. <https://www.skynewsarabia.com/amp/technology/1211218>
38. Tigareti. (n.d.). *Electronic cloud: A service for transferring and storing data remotely via the internet*. <https://tigareti.com/electronic-cloud/>