CORPS & PSYCHISME
P-ISSN: 2496-4476 E-ISSN: 2273-1571
Volume 13/ Issue 1/ 2026

The Problem of Criminal Liability for Cybercrimes Using Artificial Intelligence

Sbihie Chahinez
Associate Professor (Class B)
Hassiba Benbouali University – Chlef
ORCID: https://orcid.org/0009-0008-7897-5488 ; Email: c.sbihie@univ-chlef.dz

Received: 12/12/2025, Accepted: 02/02/2026, Published: 28 /03/ 2026

Abstract:

Recent years have witnessed a development in the field of artificial intelligence as a result of the tremendous progress in data processing technology. This development has shown the ability to significantly change lives, even in providing machines that can perform more complex and diverse tasks for widespread use in a group of sectors. This is due to its distinguished superior ability to develop its skills and build self-experience that allows it to make decisions independent of humans. The ability to face the most extreme circumstances makes artificial intelligence programs independent in their actions from the dependency of the producer, programmer, or user. However, artificial intelligence technologies have had serious repercussions as a result of their misuse, which has led to the emergence of new forms of crimes, whether crimes committed using artificial intelligence or crimes committed by artificial intelligence itself, which has begun to raise many problems, especially with regard to responsibility for the work of these programs and the extent of the suitability of current legislation and its ability to accommodate the characteristics of this technology. Accordingly, this study aims to focus on the problem of criminal liability for cybercrimes committed by artificial intelligence technologies.

Keywords : Cybercrime, artificial intelligence, technologies, criminal liability.

Introduction:

Artificial intelligence (AI) technology represents the most significant achievement of the Fourth Industrial Revolution due to its widespread use across various aspects of life. It has been utilized in military, political, and economic fields-with its industrial and service activities-and even in the security domain. This intelligence is now highly efficiently simulated by certain electronic applications, capable of sabotage, learning, and self-development without human intervention.

Given the importance attached to this topic, we have chosen to study it due to the unique nature of AI technologies. These technologies have come to mimic human behavior and even attempt to surpass it through autonomous decision-making and independence from their designers and producers. This has given rise to numerous legal problems, particularly those related to the foundations of liability for the damages they cause to others, as well as identifying the party responsible for such damages. Here, the question of criminal liability for AI cybercrimes arises based on the commission of an unlawful act. This necessitates investigating whether traditional and newly developed rules of criminal liability can cover AI liability in the

event it causes harm to others, especially since penal liability relies primarily on material punishment.

Study Problem: Based on the above, we raise the following core question:

To what extent are the general rules of criminal liability sufficient for the cybercrimes committed by artificial intelligence applications?

Study Objectives: Based on the posed problem, this research paper aims to highlight new concepts that explore the characterization of the digital environment, artificial intelligence, and cybercrime. Furthermore, it seeks to elucidate the relationship between AI and cybercrime, and whether criminal liability arises from cybercrimes committed by AI technologies.

Study Methodology: To answer the proposed problem and achieve the study's objectives, we opted to use the descriptive-analytical approach, as it suits the nature of the topic and its data, providing a clear and comprehensive picture.

Study Divisions: We have divided this paper into three main sections. In the first section, we highlight and define the concepts. In the second, we attempt to present models of cybercrimes committed by artificial intelligence. Finally, in the third section, we explore the problem of criminal liability for AI technologies committing cybercrimes.

Section One: Definition of Concepts

First: The Concept of Artificial Intelligence

1. Definition of Artificial Intelligence:

Linguistically: The word "intelligence" (Zakaa) is a noun. "Intelligent" (Zaki) is derived from "Zaka". When it is said "the boy is intelligent" (Zaka al-walad), it means he is quick to understand and insightful. The word "artificial" (Istina'i) is an adjective attributing something to being manufactured or unnatural. Thus, artificial intelligence is the ability of a machine or device to perform certain activities that require intelligence, such as actual reasoning and self-repair.[1]

Terminologically: The American scientist John McCarthy is considered the one who coined the term "Artificial Intelligence" in 1956. He defined it as: "the science and engineering of making intelligent machines, that is, the automation of activities associated with human intelligence, so that these systems provide their users with various services from education, guidance, interaction, decision-making, etc. In other words, it is the machine's ability to perceive its environment and respond to it independently, and to perform tasks that typically require human intelligence and decision-making processes, but without human intervention"[2]. AI has also been defined as: the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.[3]

The term artificial intelligence can be defined through a set of capabilities: the ability to deduce, the ability to acquire and apply new knowledge, the ability to perceive and process the surrounding objects, and the ability to make decisions based on the analysis of previous data.[4]

The preceding definitions reveal a broad perspective on the concept of AI, encompassing a variety of aspects and technologies. This indicates that AI includes diverse viewpoints, making it difficult to establish a single, precise, and comprehensive definition due

to the vast complexity and variety of models, applications, and approaches used in its development.

2. **The Origins of Artificial Intelligence, its Types, and Dimensions:**

When discussing the origins of AI, we must look far back in time. AI is not tied solely to its first appearance in its final form; rather, it is closely linked to the sciences, knowledge, and endeavors that led to its emergence. AI is the culmination of two thousand years of philosophical theories, humanities, cognitive theories, and educational foundations, in addition to 400 years of mathematics, logic, and probability sciences, all of which ultimately led to information technology designed to simulate the human mind.[5]

The stages of reaching AI in its conceptual sense date back to 1956 when a scientific conference was held at Dartmouth College in the USA. The term "Artificial Intelligence" was revealed at this conference by scientist John McCarthy, and the name was given to computers with massive capabilities matching the human mind in thinking and data processing.[6]

Technical studies and experiments rapidly emerged to find the best system to simulate the human mind. By 1973, attention was turned to speech recognition and processing. In 1980, an AI system was developed allowing users to interact with a machine carrying an integrated database. In the 1990s, integrated AI systems were updated within a comprehensive information environment, linking machines to global databases and networks, enabling humans to interact with machines just as they would with another human to ask questions and obtain precise information.[7]

In 2016, a conference was held at the White House regarding the future of AI, its ethics, and the necessity of developing this event to facilitate the activities of individuals, groups, and nations alike. This was widely welcomed globally as a step towards developing AI systems more accurately and beneficially. [8]

It is worth noting that each stage of AI development revealed a specific type of AI that improved communication, work execution, and facilitated life in various fields, shrinking the gap between human and artificial intelligence.[9]

3. **Fields of Artificial Intelligence:** AI relies on developing data-driven models and programs to learn patterns and make independent decisions. It includes the following fields:

- **Problem Solving:** This is the process of identifying the cause of a problem and finding a possible way to resolve it. It involves analyzing the issue, making decisions, and exploring multiple approaches to reach the most suitable and effective solution. The ultimate goal is to identify the best solution among the available options in order to achieve optimal results and solve problems in the shortest possible time. [10]
- **b. Artificial Intelligence in Strategy Games:** AI researchers have focused on chess, one of the most famous intellectual games that rely on intelligence and place two thinkers in complex situations where neither can win without logical reasoning and intelligence. In 1997, IBM's *Deep Blue* computer achieved a historic milestone by defeating Garry Kasparov, marking the first time a machine surpassed a human in this domain.
- **c. Application of Artificial Intelligence in Medicine:** AI is currently applied in clinical decision support and image analysis. These tools assist physicians in determining patient treatment, medications, and other requirements by providing quick access to relevant information. AI-assisted tools include computed tomography (CT), X-rays, and magnetic

resonance imaging (MRI), among other medical imaging techniques, for analyzing lesions and other indicators via computer. These tools help radiologists make accurate diagnoses, while AI predictive results benefit doctors, researchers, and patients. Gradually, AI is being integrated into digital health support systems. [11]

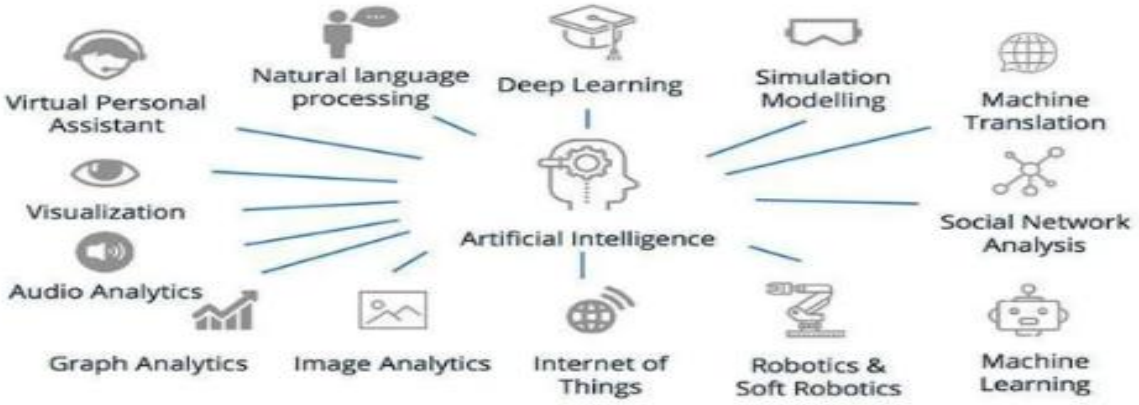
- **d. Pattern Recognition:** This is a specific type of artificial intelligence that enables systems to learn from data and identify patterns with minimal human intervention. Computers using machine learning can detect patterns and information that subsequently allow them to draw their own conclusions,[12] It involves teaching computers how to learn from data in order to make predictions or decisions. [13]It is a scientific field that enables algorithms to discover recurring patterns in datasets, which may include numbers, words, images, statistics, and more.[14]
- **E. Machine Learning:** This is a specific type of artificial intelligence that enables systems to learn from data and identify patterns with minimal human intervention. Computers employing machine learning can detect patterns and information that allow them to draw their own conclusions.

It involves teaching computers how to learn from data in order to make predictions or decisions. Machine learning is a scientific field that allows algorithms to discover recurring patterns in datasets, which may include numbers, words, images, statistics, and more.[15]

- **Deep Learning:** This is a subset of machine learning in which artificial neural networks-algorithms inspired by the human brain-learn from data in a manner similar to how humans learn from experience, iterating and adjusting each time to improve results. One of the reasons for the advancement of deep learning capabilities in recent years is the increase in data generation.[16]

Deep learning algorithms leverage the available computational power along with the widespread use of artificial intelligence. Examples include language translation, driverless delivery trucks, drones, computer vision in self-driving cars, service and chat robots, image colorization, facial recognition, as well as applications in medicine, pharmacy, marketing, and personalized entertainment.[17]

Figure No (01): Artificial Intelligence Applications



Source: Zhang Nan-Chen, Yuping-Zhu Kongjue. *The Future of Marketing Analytics: Trends and Emerging Technologies, International Journal of Advances in Business and Management Research (IJABMR)*. Published: 12/03/2024. Accessed: 10/07/2025, at: https://ejournal.svgacademy.org/index.php/ijabmr/article/view/30

Second: The Concept of Cybercrimes

1. **Definition of Cybercrime:** The term cybercrime consists of two parts: "crime" and "cyber," with "cyber" describing the computer or information age aspect. Jurists differ in their definitions[18].

Within the framework of defining cybercrime terminologically, perspectives have varied. Some scholars adopt a narrow view, while others adopt a broader one. Among the definitions proposed by proponents of the narrow approach, cybercrime is described as "any unlawful act that requires a significant knowledge of computer technology for its commission on one hand, and for its investigation and prosecution on the other".[19]In the same context, Professor Mass defines it in terms of informatics as" legal violations committed through informatics with the aim of achieving profit.The German scholar Tie de Man considers [20]" cybercrime as "any form of unlawful and socially harmful behavior committed using computers," focusing on the means of committing the crime.[21] These definitions indicate a narrow understanding of cybercrime, as they exclude many unlawful acts in which computers are used merely as a tool for their commission.

In contrast, there are definitions that have sought to broaden the concept of cybercrime in response to criticisms of the narrow approach. Some define it as “any intentional act or omission arising from the unlawful use of information technology with the aim of harming tangible or intangible assets,” and also as “the use of a computer as a tool to commit a crime, in addition to cases involving unauthorized access to the victim’s computer or data.[22]".

The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders adopted the following definition of cybercrime: “It is any crime that can be committed through a computer system or a computer network. In principle, this definition encompasses all offenses that can be committed in an electronic environment.[23]

As for the Algerian legislator, cybercrime has not been explicitly defined and is instead referred to as “crimes related to information and communication technology.” Under the provisions of Article 2 of Law No. 09-01,[24] it is defined as: “crimes affecting automated data processing systems as specified in the Penal Code, and any other crime committed or facilitated through an information system or an electronic communications system.” According to the Penal Code, this does not constitute a formal definition of electronic crime; rather, the legislator merely specifies the criminalized acts and the corresponding penalties[25].

2. **Characteristics of Cybercrime:** Based on its definition, cybercrime is characterized by features that distinguish it from other types of crime, including the following:

- **Transnational Crime:** This type of crime crosses borders and is not confined to a single jurisdiction. It may extend to multiple countries, raising issues related to jurisdiction, procedures, and investigation.
- **Difficult to Detect and Prove:** Cybercrime is extremely difficult to detect, and when it is discovered, it is often by chance. This is largely because perpetrators typically leave no visible external traces or deliberately destroy evidence.[26]
- **Non-Violent Crime:** Unlike traditional crimes, which may require the use of tools or violence, as in terrorism or drug-related offenses, cybercrime is considered non-violent. Activities such as transferring data from one computer to another or electronically

accessing a bank account do not require physical force or armed confrontation with law enforcement.[27]

- **Low Reporting Rate:** Due to the sensitive nature of cybercrime and the potential for public exposure or reputational damage to the perpetrator if reported, such crimes are infrequently reported. Most cases are discovered by chance, sometimes long after the crime occurred, and may be complicated by the geographical distance from the crime scene.[28]
- **Lack of a Common Concept of Cybercrime:** A defining feature of cybercrime is the absence of a universally accepted definition or legal concept, due to the lack of international coordination, absence of treaties, and differences in national legal systems.
- **Occurrence During Automated Data Processing:** A fundamental condition for cybercrime is that it occurs during the automated processing of data. Without this condition, cybercrime cannot be said to exist.
- **Cybercrime as an Emerging Crime:** Any crime targeting computers or using computers to commit offenses is considered a newly emerging crime.[29]

3. Types of Cybercrimes: According to the draft European Convention of 2001, they are classified into:

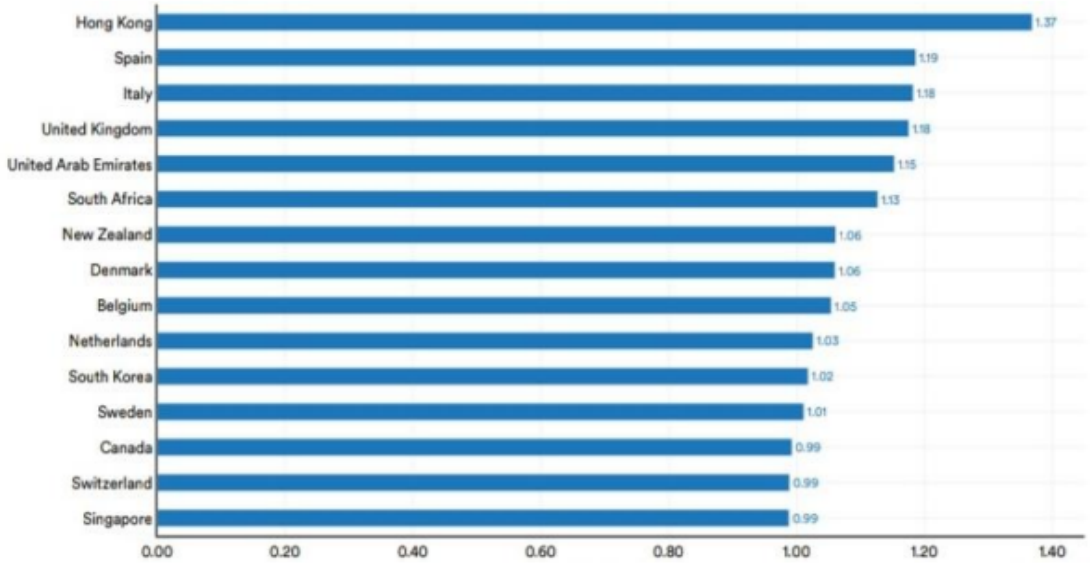
- Crimes targeting the safety and confidentiality of data and systems (illegal access, data destruction).
- Computer-related crimes (forgery and fraud).
- Content-related crimes (pornographic and immoral acts).
- Crimes related to persons and property (theft, fraud, privacy invasion, electronic terrorism).

Section Two: Models of Cybercrimes Committed by Artificial Intelligence

First: Employment of Artificial Intelligence:

AI is among the most important objectives countries strive to achieve, especially in the economic field, due to its multifaceted benefits.

Figure No (2): Ranking of Countries by Artificial Intelligence Adoption Index for 2023



Source: Hai, Stanford university, **Artificial Intelligence Index Report** ,2023, p180.

The figure illustrates that it measures the **relative AI adoption index**, indicating the rate at which AI talent is being employed. More specifically, it shows whether the employment of AI talent is growing faster, at the same pace, or slower than overall employment in a particular geographic region. In 2022, Hong Kong recorded the highest growth in AI employment at 1.4, followed by Spain and Italy, and then the United Kingdom and the United Arab Emirates.

Second: Models of Cybercrimes Involving Artificial Intelligence

Many machines that utilize AI technology surround us, such as robots, cars, airplanes, ships, and others. Among these, robots and cars are the most familiar to us due to their greater availability compared to other AI-powered machines.

1. **Robot Crimes:** A robot is defined as a device with mechanical programming that is electronically controlled to perform certain tasks and achieve objectives in place of humans. There are several types of robots, including:

- **Surgical Robots:** Typically used to perform surgical operations, which doctors can control remotely via integrated cameras to obtain a three-dimensional view.
- **Domestic Robots:** Used for household tasks such as washing dishes, serving food, and other chores.
- **Service Robots:** Deployed in universities or research and development teams to execute new functions and present them to the public.
- **Military Robots:** Used for bomb disposal, border surveillance, and unmanned aerial vehicles (drones).

Thus, a robot is a machine programmed to perform certain human functions and may resemble humans in some external features. These robots operate using algorithms programmed with artificial intelligence. They can be categorized into two types:

- **Simple Traditional Robots:** Tasked with specific, limited functions.
- **Advanced Robots:** Operate with complex algorithms, analyze massive amounts of data, and transition from merely receiving commands to self-learning, independent thinking, decision-making, and execution.

The nature of criminal acts committed by robots varies according to their type. Simple robots commit minor, less sophisticated crimes that are easy to prove and assign responsibility for. In contrast, advanced robots operating with AI algorithms exhibit more complex behaviors, commit novel types of offenses, and present challenges in proving the crimes and identifying the responsible party for legal accountability due to their autonomous and individualized nature.

2. **AI Technology Crimes in Social Media Applications:** The virtual world is currently considered a quasi-parallel platform to the real world, where people spend a significant portion of their day. Social media platforms are among the most prominent elements of the virtual world. Therefore, we will discuss the most notable AI-related cybercrimes associated with social media.

For instance, Facebook uses cookies to achieve certain objectives, such as verifying the user's identity, maintaining account security, determining user preferences, tracking location, and performing search analytics, among other functions. These cookies can only be accessed with the user's consent, and their use is strictly limited to the platform itself. Sharing them with

any other website or entity constitutes a violation of user privacy and may constitute a criminal offense.

However, no service comes without a price. If a service is free, you are often the price-this is what Facebook does. The platform does not only rely on cookies collected from the user's browser; it also filters voice calls and text conversations to identify keywords that reflect the user's interests. This information is then used for advertising purposes and to provide content aligned with user preferences. Many users notice that, for example, after mentioning a particular brand or expressing a desire for a certain type of food, advertisements for that brand or type of food appear on their Facebook feed. All of these practices constitute overreach by Facebook, violating user privacy and potentially amounting to criminal offenses.[30]

What reinforces our discussion regarding Facebook's exploitation of user data and its sharing with other companies is that researchers recently discovered that Facebook was collecting logs of calls and text messages on users' phones. However, the company later denied this claim, stating that call logging is a feature available only to users of Facebook Lite and Messenger on Android devices, and that the feature can be disabled. Nonetheless, making call logging optional does not justify Facebook's behavior if the default setting is to record calls. The practice would only be lawful and non-criminal if the default setting were not to record calls and users had to enable it themselves. This raises the question: what criminal liability does Facebook bear in the event of a user data leak?

As previously mentioned, Facebook collects data related to its users either through cookies or via its complex algorithms using artificial intelligence techniques to determine user interests and preferences. In most cases, obtaining such data is legally permissible and does not constitute a crime. However, the issue becomes critical when it comes to data leaks, which can be analyzed in two scenarios:

1. **Intentional Data Leak by Facebook:** If Facebook intentionally leaks user data, for instance by selling it to other companies, it bears full responsibility and commits a privacy violation offense as stipulated by law.
2. **Data Leak Due to Security Breach:** If user data is leaked as a result of an unintended security breach, Facebook's liability is partial rather than full, since the breach occurred without intent through the exploitation of security gaps. In this case, the primary responsibility falls on the individual(s) who carried out the breach and obtained the data. Facebook's responsibility is limited to failing to implement adequate security measures to protect user data. Ultimately, anyone who obtains personal data has a legal obligation to safeguard it and prevent unauthorized access, in accordance with applicable law. [31]

Below is the academic English translation, with the original structure, punctuation, and reference numbering preserved. For accuracy, English-language sources commonly date Isaac Asimov's "Runaround" to its first publication in 1942, although the source text states 1946.wikipedia+1

Section Three: Criminal Liability for AI Cybercrimes

In 1946, the science fiction writer Isaac Asimov, an American of Russian origin, published a short story entitled *Runaround*. The protagonist of the story was a mechanical man, or robot, programmed in accordance with three safety laws, namely:

First Law: A robot may not harm human beings, or even allow such harm to occur.

Second Law: A robot must obey human orders, except where such orders conflict with the First Law.

Third Law: A robot must preserve its continuity of operation and protect itself from malfunction, unless this conflicts with the First and Second Laws[32].

Although these laws were mentioned incidentally within the context of the story, many scholars in the field of artificial intelligence have adopted them as a kind of intellectual orientation or school of thought. They argue that the ideal robot should possess these qualities, or that, in order to prevent technology from turning against us with grave consequences, we must program and build robots in this manner.

Since AI robots and AI software are now used in a wide range of applications in industry, military services, medical services, science, games, and other related fields, the imposition of criminal liability on AI robots and AI software requires that the rules governing such liability first be identified, with attention to two principal elements: the external element, namely the criminal conduct, and the internal, mental, cognitive, or intentional element relating to that criminal conduct Accordingly, in the field of artificial intelligence, if we have a robot [33]. or any AI application performing a particular task and causing an error or malfunction-for example, by using personal information to commit multiple cybercrimes, such as supplying false information, fabricating videos, or creating and generating deceptive content by means of which human beings may be defrauded, as in the case of the influencer Sophia Mila, who is in fact a girl from the virtual world created by artificial intelligence and for whom an Instagram account was opened, through which followers were deceived and their money taken, while no one knows whether this account actually belongs to anyone-the strange question then becomes: what would artificial intelligence do with this money? If artificial intelligence causes harm, injures someone, or even causes a person's death, who would bear criminal liability in such a case? In truth, we cannot yet answer this question clearly, because there is still considerable controversy regarding the legal nature of artificial intelligence, which calls for the development of new rules focused on how intelligent robots may be held accountable for their criminal acts.

Nevertheless, in order to impose criminal liability on any type of AI entity, the existence of two elements must be established: the capacity to act and actual will. Hence, it is necessary to examine how criminal liability may be applied to autonomous AI applications and devices when they commit a cybercrime. Accordingly, we shall first address the possibility of applying the theory of the indirect perpetrator to AI cybercrimes, and then examine the issue of attributing personal liability to artificial intelligence in accordance with the elements of criminal capacity.

1. The possibility of applying the theory of the indirect perpetrator to AI cybercrimes:

It is generally agreed at the European level that the current rules of liability cover cases in which the cause of an act or omission by artificial intelligence can be attributed to a specific human agent, such as the manufacturer, the owner, or the user, and where that agent could have foreseen it. From another perspective, certain conceptions of criminal liability concerning AI entities and software have been proposed, and these may be summarized as follows:

- **Liability of the producer or owner for the commission of the crime:**

The criminal liability of the producer of artificial intelligence is among the most important issues raised when the latter commits any conduct constituting a crime under the

law. Therefore, examining the producer's criminal liability is necessary in order to clarify the extent of that role. The producer may protect himself through clauses included in the terms of use, which the owner signs, thereby placing sole criminal liability on the owner for crimes committed through that AI-based entity and disclaiming the producer's liability for any crime committed by it. Likewise, the owner or user may misuse that program, resulting in the commission of a crime. In this case, it is necessary to distinguish among three possibilities[34]:

a) The crime occurs solely as a result of the owner or user; had it not been for his conduct, the crime would not have occurred. Here, criminal liability falls entirely upon him. An example would be a user or owner disabling the autonomous control system in a self-driving car and leaving only the voice instructions issued by the AI program. In that case, he alone is controlling the vehicle. If the program issues a warning instructing him to take a particular action in order to avoid an accident, and he fails to comply, then criminal liability falls solely upon him.

b) The second possibility is that liability is shared jointly with the producer, the AI programmer, or other external parties; for example, where the owner of a vehicle alters the operating commands in a self-driving car with the assistance of a specialist in the field, with the aim of using it to commit a crime and denying his own criminal liability by attributing it to the vehicle and its manufacturer. In this case, criminal liability is shared. Article 42 of the Algerian Penal Code [35]defines such acts. Here, criminal liability may be attributed to the user of artificial intelligence where he uses it in an unlawful manner in order to commit a particular crime, or induces it to commit that crime, such that the user or owner becomes the indirect perpetrator, while the artificial intelligence becomes the material perpetrator. In this case, the theory of the indirect perpetrator may be applied, and full criminal liability attributed to the owner or user.

In sum, in both possibilities, the constituent elements of the material element are fulfilled through AI devices or robots, whereas the mental element is fulfilled through the programmer or the user. Although the crimes are committed through robots or AI devices, this does not in itself entail criminal liability for those devices. According to this conception, there is no legal distinction between an intelligent robot and a trained animal, or any other instrument of crime. Accordingly, criminal liability is established for both the programmer and the user for crimes committed by means of the intelligent robot, as they serve as intermediaries in perpetrating them, by analogy with the traditional theory of the indirect perpetrator.[36]

- **Liability for committing the cybercrime through an external party:**

In addition to the owner and the user, an external party may intervene in AI-related crimes, by entering the AI system through hacking or by any other method, taking control of it, and exploiting it in the commission of a crime. In this case, we are faced with two hypotheses[37]:

a) The first hypothesis is that the external party exploits a vulnerability in the artificial intelligence to commit the crime, and that this vulnerability resulted from negligence on the part of the owner or the manufacturer of the technology. In that case, criminal liability is shared between the external party and the person whose negligence led to the exploitation of that vulnerability. An example would be an owner of an AI system providing the access

code to the system controlling the AI technology to that external party, thereby enabling him to issue commands to the AI.

b) The second hypothesis is that the external party exploits a vulnerability in the artificial intelligence without the assistance or negligence mentioned in the previous case. In this situation, full criminal liability falls upon that external party alone. An example would be an external party hacking the cloud through which commands to the AI technology are stored and transmitted, and then issuing commands directing the artificial intelligence to commit a particular crime, such as ordering it programmatically to attack persons bearing specific characteristics, such as skin color or a certain type of dress.

- **Liability for crimes resulting from programmers' errors:**

In this case, a crime may occur as a result of a programming error committed by the programmer of the AI software. It may happen that the programmer releases the AI technology with defects that lead to crimes, and he would thus be criminally liable for them. A distinction must therefore be made between whether this conduct was intentional or not, so as to determine whether the crime occurred through intent or negligence, given the difference in the penalty prescribed for each.

Accordingly, it may be said that where one of the elements of liability is absent, it becomes difficult to attribute liability to AI devices. While the material element may be realized through an error by AI devices, the mental element cannot be expected to arise, because artificial intelligence does not possess legal personality; its will would have to be directed toward committing the crime intentionally. Therefore, most jurists agree that the indirect perpetrator is the one who commits the crime through another who is merely an instrument in his hands. In this regard, there are two trends:

a) One trend recognizes legal personality for AI devices so that they may be held accountable for their own personal acts. This would make them bear liability for the damage resulting from their acts, through the recognition of an independent financial patrimony of their own from which such damage may be compensated directly.[38]

b) The second trend holds that liability can be established only for a natural person and cannot be established for artificial intelligence, because most sanctions are not capable of being applied to it. In addition, attributing the crime to artificial intelligence would conflict with the principle of legality of crimes and punishments, and the purpose of punishment—namely general and specific deterrence—cannot be achieved in relation to AI devices [viii].

2. Attributing personal liability to artificial intelligence in accordance with the elements of criminal capacity:

The possibility that artificial intelligence may commit a crime on its own, without any programming error, as a result of autonomous development within the AI system under which it operates, has now become conceivable. This raises numerous questions about criminal liability. Can AI entities be punished like human beings, or like legal persons such as companies, against which sanctions may be imposed through the necessary procedural and legal adjustments?

The answer depends on the definition of criminal capacity, on the basis that criminal liability requires the offender to possess the capacity to be held accountable, since such liability is linked to the mental element of the crime. Some jurists view the criminal act not only in

terms of its material consequences or in terms of the legal provision criminalizing it, but also in terms of the capacity of the perpetrator and his bearing of the consequences of those acts. A crime may cause great harm; however, the absence of criminal capacity on the part of the perpetrator removes the basis of criminal liability because criminal intent is absent, whether due to the offender's young age, lack of will, or lack of awareness of the consequences of the act .[39] In other words, criminal capacity is the basis of liability, on the understanding that a person is not criminally accountable unless he is fit for such accountability, and this is only possible where two qualities are present: discernment or awareness, and freedom of choice. In this regard, Article 47 of the Penal Code provides: "No penalty shall be imposed on a person who was in a state of insanity at the time of committing the crime ...". Article 48 of the same law also provides: "No penalty shall be imposed on a person who was compelled to commit the crime by a force he was unable to resist." These provisions demonstrate that the absence of freedom of choice in cases of insanity, coercion, and minority leads to the exclusion of criminal liability.

The Algerian legislator did not define criminal liability and merely enumerated the grounds for its exclusion. Likewise, most Arab legislations have not defined criminal liability, leaving that matter to legal scholarship, and have confined themselves to removing criminal liability from those who lack awareness or will, such as the insane person, the non-discerning minor, and the coerced person, due to the absence of criminal capacity. Thus, a person is criminally accountable only if he possesses the necessary criminal capacity, namely the two elements of will or choice, and awareness.

This gives rise to the following question: can the element of knowledge and will be applied to crimes committed by artificial intelligence, as mentioned above?

The answer to this question is that human laws cannot be directly applied to artificial intelligence, and therefore, under current laws, we cannot impose a criminal sanction on AI applications. However, a judge may order the confiscation of the machine operating through artificial intelligence, and may also order its destruction. There may, however, be another answer, namely liability based on the natural probability of consequences, which presupposes deep involvement by programmers or users in the daily activities of artificial intelligence, but without any intention to commit any violation through it. For example, while carrying out its daily tasks, an AI entity may commit a crime of which the programmers or users become aware only after it has already been committed; that is, they neither planned nor participated in the crime. In such a case, an appropriate legal response is fashioned, depending on the ability of the programmers or users to foresee the commission of potential crimes. A person may then be held accountable for the crime if it was a natural and probable consequence of that person's conduct, and this basis has been used to impose criminal liability on accomplices.[40]

At this point, one may ask: what is the criminal liability of the entity itself when the model of natural probability is applied?

In answering this question, there are two views:

- If artificial intelligence acts as an innocent agent, without knowledge of criminal prohibitions, then it is not liable and is not criminally accountable.
- If artificial intelligence is not innocent, then it is liable and may be punished.

AI robots and devices may satisfy the requirements of criminal liability just as human beings do, by treating them as legal persons similar to companies possessing constitutional freedoms, especially in light of the development of artificial intelligence. It is therefore extremely important to hold them accountable for their acts. Criminal liability arising from acts of artificial intelligence would then not fall solely upon the programmer or the owner. One example is where an autonomous AI system makes decisions that result in harm, such as where the developer of a military aircraft designs an autopilot program that independently removes any obstacles to its mission. In one mission, the pilot aborts the mission because of bad weather, but the autopilot identifies the human pilot as an obstacle and ejects him from the cockpit, thereby causing his death. In such a case, the developer had no intention of killing the pilot, yet current laws would regard them as responsible. The proper option would be to impose criminal liability on the autopilot itself and correct the algorithms of its software. This would not absolve AI developers and the owner from criminal liability for acts they never intended.[41]

Finally, it is evident that it is difficult to hold artificial intelligence criminally liable for its harmful acts, since it remains a tool that is used, despite its ability to simulate human behavior, and in the absence of legal texts regulating its liability when any error or damage occurs.

Conclusion:

The massive technological explosion at the end of this century and humanity's ability to create intelligence that simulates its own has helped improve living conditions and facilitate our lives by providing all means of comfort and convenience. However, this progress has also raised numerous questions and challenges. In this study, we attempted to address some of these issues, particularly those related to criminal liability for unforeseen cybercrimes committed by AI programs and other legally prohibited actions, which require legislative and regulatory intervention to manage the problems they present. It is important to note that AI technologies are, in essence, the result of human efforts that have endowed machines with such capabilities.

Reaching a stage where a virtual world is recognized and regulated by law could shift the balance from a blessing to a potential curse, placing human interests in inevitable conflict with a virtual world. This could create problems even more complex than those currently faced. The matter has indeed become particularly challenging, especially following Saudi Arabia's initiative to grant citizenship to the robot Sophia. Although this decision may appear laughable to the majority, it represents a reality that carries genuine concerns, which a few have expressed while remaining largely unacknowledged by the majority.

Study Results: Through this study, we reached several results, highlighted as follows:

1. There is no unified definition of artificial intelligence, which is characterized by the ability to move, self-learn, respond to variables, and adapt to the surrounding environment.
2. Currently, there are no specific laws regulating machines possessing artificial intelligence. Current legislation does not keep pace with the rapid development of AI technology; in the eyes of the law, these technologies remain mere tools executing users' orders. Legal texts are unable to protect users from machine errors or address the consequences of AI acting unpredictably.

3. Criminal liability is a personal liability concerning human beings, requiring knowledge and will. It is restricted to human individuals and cannot be directly imposed on an artificial entity.
4. There is a severe lack of special laws regulating the use of AI and its breaches, especially concerning cybercrimes. The regulatory frameworks currently available fail to keep up with the continuous advancements in AI technology.

Footnotes:

[1] - Islam El-Desouky Abdel Nabi, *The Role of Artificial Intelligence in International Relations and International Liability for its Use*, The Legal Journal, Saudi Arabia, 2020, p. 1450.

[2] - Mustafa Imad Mohammed Al-Bayati, *The Limits of Artificial Intelligence and the Emerging Liability at the International Level*, Al-Qadisiyah Journal for Law and Political Science, University of Kufa, Faculty of Law, Vol. 13, No. 2, 2022, p. 271.

[3] - Ghofran M. I. Hilal & others, *The Governance of Artificial Intelligence in Line with the International Human Rights Law*, SHARI'A AND LAW SCIENCES, The University of Jordan, Volume 49, No. 4, 2022, p. 129.

[4] - Ahmed Saad Ali Al-Borai, *Applications of Artificial Intelligence and Robots from the Perspective of Islamic Jurisprudence*, Cairo, Al-Azhar University, Faculty of Islamic and Arabic Studies for Boys, 2022, p. 25.

[5] - Pradipta Kumar Das & Others, *Artificial Intelligence lecture notes*, India, Veer Surendra Sai University of Technology, 2014, pp. 9-13.

[6] - Ihab Khalifa, *Artificial Intelligence: The Effects of the Increasing Role of Smart Technologies in the Daily Lives of Humans*, Trends of Events Journal, Abu Dhabi, No. 20, 2017, p. 62.

[7] - Rasha Mohammed Sa'em Ahmed, *Management Applications of Artificial Intelligence in Administrative Decision-Making*, Master's Thesis, Jordan, Middle East University, 2022, pp. 11-16.

[8] - Samia Qamoura et al., *Artificial Intelligence Between Reality and Expectations: A Field Technical Study*, International Conference "Artificial Intelligence: A New Challenge for the Law", Algeria, 2018, pp. 2-3.
[9] - Jatin Borana, *Applications of Artificial Intelligence & Associated Technologies*, Proceeding of International Conference on Emerging Technologies in Engineering, Biomedical, Management and Science, India, Jodhpur National University, 2016, pp. 64-67
[10] -. Kamilia, 2024, *What Is Artificial Intelligence: Definition & Sub-Fields Of AI*. Published on: 01/04/2025. Accessed on: 13/07/2025, at :https://www.softwaretestinghelp.com/what-is-artificial-intelligence/

[11] - Srivastava, R., *Applications of Artificial Intelligence in Medicine*. Centre for Cellular and Molecular Biology-CSIR, Hyderabad, India, 9(2), 2024, p. 138.

[12] -Boesh, Gaudenz, *What is Pattern Recognition? A Gentle Introduction*. Published on: 11/10/2024. Accessed on: 13/07/2025, at :https://viso.ai/deep-learning/pattern-recognition/

[13] - Flam, Seth, *Benefits of Machine Learning in Healthcare*, Foresee Medical. Published on: 24/01/2025. Accessed on: 10/07/2025, at :https://www.foreseemed.com/blog/machine-learning-in-healthcare

[14] - Wilson, Andrew, *Branches of AI: A Simple Guide to 28 Fields of Artificial Intelligence*. Published on: 14/05/2023. Accessed on: 10/07/2025, at :https://approachableai.com/branches-of-ai/

[15] - Robert, J., *Machine Learning: Définition, fonctionnement, utilisations*. Published on: 18/11/2020. Accessed on: 04/07/2025, at :https://liora.io/machine-learning-tout-savoir

[16] - Marr, Bernard, *Qu'est-ce que l'IA d'apprentissage profond? un guide simple avec 8 exemples pratiques*. Published on: 01/10/2018. Accessed on: 01/07/2025, at https://www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deeplearning-ai-a-simple-guide-with-8-practical-examples/?sh=da33388d4bad.

[17] - Wang, Ming-Hwa (n.d.), *Artificial Intelligence and Subfields*. Ph.D. Adjunct, Department of Computer Engineering, Santa Clara University, Available at: https://www.cse.scu.edu/~m1wang/ai/AI_subfields.pdf, p. 11.

[18] - Aimour Radia, *Cybercrime and its Combating Mechanisms in Algerian Legislation*, Academic Journal for Legal and Political Research, No. 01, 2022, p. 91.

[19] - Baara Saida, *Cybercrime in Algerian Legislation*, Master's Thesis, Mohamed Khider University - Biskra, 2014/2015, p. 11.

[20] - Messaoud Shahira, *Cybercrime in Algerian Legislation*, Master's Thesis, Abdelhamid Ibn Badis University - Mostaganem, 2020/2021, p. 06.

[21] - Belaid Mansouria, *The Procedural System for Cybercrime in Algerian Legislation*, Master's Thesis, Abdelhamid Ibn Badis University, Mostaganem, 2019/2020, p. 09.

[22] - Mrabti Roumaissa, *Cybercrime: Between the Limits of Danger and the Necessities of Confrontation*, Journal of Governance and Economic Law, No. 01, Tunisia, 2023, p. 61.

[23] - Law No. 09-04 issued on August 5, 2009, comprising specific rules for the prevention and combating of crimes related to information and communication technologies, Official Gazette, No. 47.

[24] - Si Hamdi Abdel Moumen & Qira Souad, *Cybercrime and its Confrontation Mechanisms in Algerian Law*, Al-Biban Journal for Legal and Political Studies, No. 01, Bordj Bou Arreridj, June 2022, p. 61.

[25] - Al-Hussein Faraj, *Cybercrime and its Repercussions on National and Citizen Security Between Legal Combating and Detection and Investigation Agencies*, Journal of Public Administration, Law and Development, No. 01, 2022, p. 76.

[26] - Thayb Mousa Al-Badaniyah, op. cit., p. 20.

[27] - Mankhrafis Yamina, *Cybercrimes via Social Media with Social and Moral Dimensions*, Journal of Rights and Human Sciences, No. 01, 2023, p. 1304.

[28] - Si Hamdi Abdel Moumen & Qira Souad, op. cit., pp. 62-63.

[29] - Sultan Ibrahim Al-Hashimi, *Jurisprudential Rulings Related to Social Media*, Global Journal of Islamic Marketing, UK, 2016, p. 18.

[30] - Electronic Privacy Information Center, *Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks*. Published on: 18/06/2018. Accessed on: 04/07/2025, at :file:///C:/Users/hi/Downloads/EPIC-SCOM-Facebook-June2018.pdf

[31] - Abdelkader Al-Kamli, *Did the Three Laws Pave the Way for Robot Dominance?*, Published on: 24/03/2024, Accessed on: 05/10/2024, Available at the following link: https://www.aljazeera.net
[32] - Ben Aouda Haskar Murad, *The Problem of Applying the Rules of Criminal Liability to AI Crimes*, University of Djelfa, *Journal of Law and Human Sciences*, Vol. 15, No. 1, 2022, Algeria, p. 197.

[33] - Ibid., p. 198.

[34] - Ordinance No. 66-155 Promulgating the Algerian Penal Code, dated 18 Safar 1386 AH, corresponding to June 8, 1966, Official Gazette of the People's Democratic Republic of Algeria, No. 49, issued on 21 Safar 1386 AH, corresponding to June 11, 1966, p. 702.

[35] - Muhannad Walid Al-Haddad, *The Problem of Applying the Provisions of Criminal Liability to the Actions of Robots Equipped with Artificial Intelligence*, Si El Haouès University Center of Barika, Tobna Journal for Academic Scientific Studies, Vol. 07, No. 01, Algeria, 2024, p. 1171.

[36] - Ben Aouda Haskar, op. cit., pp. 199-200.

[37] - Abdelmalek Ashwaq & Bennani Souad, *Artificial Intelligence and its Impact on the Legal System*, Journal of Law and Environmental Sciences, No. 02, 2023, p. 552.

[38] - Ibrahim Ahmed Ibrahim, *Criminal Liability Resulting from Artificial Intelligence Errors in Emirati Legislation: A Comparative Study*, PhD Thesis, Ain Shams University, Egypt, 2020, p. 155.

[39] - Abdelhamid Al-Malihi, *Criminal Protection for Juvenile Delinquents in Moroccan Legislation and the Bet on Reform - An Analytical Statistical Study*, Dar Al-Maarefa Publishing, Morocco, 2017, p. 242.

[40] - Ben Aouda Haskar, op. cit., p. 201.

[41] - Abdelhamid Al-Malihi, op. cit., p. 202.