Legislative Industry Challenges In Confronting Artificial Intelligence Crimes

Mayada Moustafa El-Mahrouki

Associate Professor of Criminal Law Criminal Justice Criminal law. Naïf Arab University for Security Sciences (NAUSS) Riyadh, Saudi Arabia
Email ID: MElmahrouki@nauss.edu.sa ORCID ID: 0009-0002-5448-5296

Abstract:

The world is witnessing unprecedented development and progress in the field of information technology at a speed that races against time and these developments have resulted in the emergence of artificial intelligence tools that has become a tangible reality because, of its capabilities that exceed human capabilities and even become a simulation of human behavior. With the advent of "robot", society's view changed from considering these tools and technologies as just software behind a programmer or operator, to the possibility of creating a self-contained robot with an independent legal personality that entails rights and obligations, which represents a challenge for legislators to create Legal frameworks and rules commensurate with the special nature of this virtual reality, in several ways, whether in terms of protecting it or in terms of protecting society from its harms or failure to fulfill its obligations. With these challenges, many legal problems arise as to how to imagine the existence of a legal personality for a tool that does not have freedom and will, even if that tool had a reaction and decision independent of its manufacturer, programmer, or operator. So; The presented scientific paper aims to shed light on anticipating and predicting the challenges facing the legislative industry in the field of artificial intelligence technologies and discussing the difficulties that face it related to the possibility of creating an independent legal personality for artificial intelligence tools through which rights can be fulfilled and obligations assumed, and even the possibility of establishing criminal responsibility and inflicting Punishment in the event that these technologies commit crimes punishable by law.

Keywords: Artificial Intelligence -Foreseeing the future -Legal personality -Legislative challenges.

Introduction

Artificial intelligence, with its various tools, [1]represents the latest findings in the world of information technology, and even one of the most important, current, and future challenges for the legal field. The law was not immune to these developments. Rather it should reflect the factual problems and find the appropriate response to it. There is a reciprocal relationship between the law and technical developments

---

Email ID: MElmahrouki@nauss.edu.sa

over time, including information technology. This prompted discussions and research on the legal regulation of these new technologies, especially since artificial intelligence has become capable of performing tasks performed by human intelligence, such as perception, planning, and the ability to solve problems.

The fields in which this type of intelligence is used are many and varied, and this has many advantages, namely the speed of completing tasks, the ability to solve complex problems, and thus greatly reducing the chances of error. Among those technologies applied in our daily lives are self-driving cars, drones, navigation systems, robots...etc.

In contrast, there has been a need to develop policies and legal rules that determine how artificial intelligence and its tools work and even how to protect it, as well as confront the consequences that could result from its use. Is it possible to imagine the establishment of an independent legal personality for artificial intelligence? This will be discussed in two sections, the first of which deals with the industry's legislative challenges in the field of artificial intelligence. The second section will address the attempts to develop legal systems that govern the field of artificial intelligence in comparative legislation.

The research problems lie in the fact that information technology data has added new patterns and images, especially those related to artificial intelligence techniques and tools, which have become available and indispensable tools for everyone. Because these tools have become like the human mind, it has become the source of injury for others and the victim of attacks from others. The damage it may cause to others may represent a flagrant violation of human dignity, especially if this happens arbitrarily and without legal justification.

The necessity of searching for a way to confront this new reality was imperative for the legislative authority. For them, the main question lies in the following: How can we overcome the legislative challenges that stand in the way of the future of artificial intelligence technologies, and create legal systems capable of governing this new creature?

The research also aims to answer several sub-questions, including: Are the general rules of criminal law appropriate for implementing the responsibility of artificial intelligence systems in the event they commit crimes? Can artificial intelligence bear criminal liability? Is it possible that there are reasons for justification or impediments to liability for artificial intelligence like a natural person? What about the responsibility of the programmer or operator of an artificial intelligence system if those systems commit intentional or unintentional crimes? Is artificial intelligence treated like a natural person, a legal person, or a thing? How can an independent legal personality be envisaged? Is it necessary to find technical guarantees that prevent artificial intelligence from turning into a tool that can destroy humanity?

The research contributes to studying and addressing the legislative challenges facing legal systems in dealing with artificial intelligence, through discussing and analyzing the legal problems that represent a challenge to this legislation. It will certainly be a question to think about solutions and recommendations that can contribute to confronting these challenges.

Method

The research will adopt a descriptive and analytical approach, as well as a comparative approach. It aims to discuss, compare, and interpret the legal principles and provisions that are appropriate to the nature of the functions performed by artificial intelligence with its various means and tools. How to apply those provisions to the special nature of these new technologies is a pivotal issue in this approach.

Search Division

The research was divided into two sections as follows:

First Section: The industry's legislative challenges in the field of artificial intelligence.

Second Section: legislative attempts to establish legal systems governing the field of artificial intelligence.

First Section: Legislative Industry Challenges

In the field of artificial intelligence

-Is AI a Legal Entity?

The primary goal of establishing a legal system that governs the issue of artificial intelligence is to achieve a balance between encouraging innovation and keeping pace with the latest technologies and protecting basic rights and freedoms. Especially since the main fear of these technologies is that they are not subject to the law, especially the criminal law.

Previously, there was fear about legal entities such as companies, and how to determine their responsibility if they committed crimes, but after they were considered entities that had an independent legal personality, and could be subjected to criminal liability, this helped this type of fear to disappear. The question that arises is: Can artificial intelligence entities be subject to criminal law like any other legal entity?

To find an answer to this question, we must contemplate the following issues:

1st: The nature of the legal personality of artificial intelligence:

The general rule in criminal law is that only those who have freedom of choice and will are accountable. This freedom of choice and will are the basis of the moral element as they are the basis for committing the crime. This means that the law does not consider it unless it is conscious, since the function of punishment is to satisfy justice and achieve deterrence. In fact, justice is not achieved unless the punishment is applied to those who deserve it, and deterrence is inconceivable except for a person who can control his actions and can abide by the provisions of the law. This does not negate the recognition of the criminal liability of the legal person but makes it more difficult to accept. **How can artificial intelligence techniques fulfill the two elements of criminal liability**? (Hosni Mahmoud, 2018).

This means that there is no responsibility except through the awareness attributed to the person who committed the crime, which requires us to distinguish between legal responsibility and legal personality. The fact that legal personality is not linked to a human being - as is the case for a legal person - is therefore separate from the existence of mind or awareness. Having legal personality does not necessarily mean legal responsibility. The most obvious example of this is that a person who suffers from insanity or lack of awareness is recognized by law as a legal personality, without legal responsibility.

Since 1961, a jurist has provided an enumeration of the functions necessary for artificial intelligence systems, which are: searching and recognizing patterns, learning, extrapolation, and planning. Therefore, any artificial system or algorithmic process performs any of these functions in its broad sense, to achieve certain goals in the world. It can be described as an artificial intelligence. Accordingly, some have defined artificial intelligence as "the computational part of the ability to achieve goals in the world (McKinney, 2015)

This required research on the nature of the legal personality of the robot, with the necessity of distinguishing between the concept of personality and the concept of the human. The attribute of being human is only granted to a living being, while the attribute of personality has transcended the limits of man and is no longer linked to the attribute of humanization. There is an opinion that the attribute of humanization is separate in its philosophical rooting from the attribute of personality in its legal dimension. Humanization has a philosophical meaning whereas personality has a legal meaning. Perhaps the most prominent evidence of this is the recognition of the legal personality of legal persons (Al-Khatib, 2019). The matter has evolved into recognizing of animals as legal persons and considering them as living, conscious beings with laws that protect them, therefore their rights must be respected and recognized.

2nd: The legal debate about legal responsibility for artificial intelligence:

If we want to discuss the legal responsibility of artificial intelligence, especially criminal liability, we mean the responsibility that falls on artificial intelligence at the time of committing a criminal act, which raises widespread controversy about the possibility of artificial intelligence being considered criminally responsible. Does the existence of a legal personality for artificial intelligence make it capable of responding criminally before the law? (Stela Enver, 2022). We should recall that the recognized persons of the law are either the natural person or the legal person, and the law grants each of them a legal status consistent with its nature. **As for artificial intelligence**, **it does not meet the description of humans or a legal entity, so does the description of a thing apply to it**?

When the announcement of the birth of a new type of machine that would participate with humans as intelligent creatures on Earth began, some criticized this expression by saying that machines, including computers, cannot always be as insightful or creative as humans (Terry Winograd, 2006). This raised the question about the essence of humanity. Does it work? Humans are thinking machines. Does artificial intelligence know what the law is, and understand the difference between legality and illegality? This makes the human element that provided her with the concept of legal knowledge, based on which she now has artificial intelligence - and not independent artificial awareness that enables her to distinguish between legitimate and illegitimate acts. If realized it would make its legal status like the legal status of someone lacking legal capacity, such as a minor.

In contrast, a supportive side of jurisprudence envisages the possibility of building a legal personality for artificial intelligence systems, through which these entities can bear criminal responsibility. Among these opinions, the jurist "Hallevy", who envisioned three models through which criminal liability could be established (Hallevy, 2010). For AI entities, we will discuss them as follows:

First Model: Assigning Responsibility to the Moral actor "responsibility through another person: Since artificial intelligence tools are merely machines and not absolute human beings, and do not possess any human characteristics, artificial intelligence cannot be considered a perpetrator of a crime. This model considers the capabilities of artificial intelligence to be like those of a child with incapacitated capacity, or an insane person who lacks criminal capacity.

In this case, the machine is considered responsible through another person who used it as a tool to commit the crime. The moral perpetrator of the crime is the one who instigate or assist others to commit it. He is the one who carried out the crime, but through someone else. The law does not distinguish between this tool, whether it is an object, or an animal trained to perform the desired organic movement, or even a human being who is minor or of good faith and hence not capable of responsibility. This is of course different from incitement, which is considered a type of criminal participation.

Example: The programmer designs a program for a robot working in a factory, and the robot causes a fire at a specific time at night in the factory. The robot here is the one who committed the crime intentionally, but the programmer is the real and actual culprit of this crime, if he has the criminal intention to commit this act. However, he used the robot as a tool to carry out his criminal behavior, and hence it can be considered a moral agent whenever he commits the actus Reus of the offense.

This means that if artificial intelligence was intentionally programmed to commit punishable criminal behavior, and a person was controlling it, then he alone will bear criminal responsibility if the criminal intent was present with its two components, knowledge, and will since he was aware that the use of intelligent systems would lead to committing the behavior. So artificial intelligence systems were subject to the will of the programmer or operator in committing criminal behavior (Al-Lami, 2021)

This can be based on what the European legislator called for to recognize the theory of the "human representative," who is the person responsible for compensating for damages caused by robots. He also opened the way to recognizing the legal personality of robots in the future and directed the Civil Law Rules Committee to study the issue of recognizing the legal personality of robots.

This is what was already included in the set of ethical principles and guidelines for artificial intelligence in the Emirate of Dubai, in the United Arab Emirates, for the year 2019 AD (Bishr, 2019). Which included, concerning the controls governing accountability for artificial intelligence systems, that "accountability for the results of the artificial intelligence system does not lie in the system itself, but rather accountability is divided between those responsible for design, development, and application."

Accordingly, the legal result resulting from this model is that the designer, programmer, or operator is held criminally responsible for the crime committed, and artificial intelligence does not bear any responsibility.

Second Model: implementing responsibility based on expected consequences: This model is based on the ability of the programmer or operator to predict potential crimes committed by artificial intelligence. This model differs from the previous model in that the programmer or operator did not have the intention to commit criminal behavior and did not plan or intend to commit it, while the first model assumes the presence of criminal intent of the programmer or operator, using artificial intelligence as a tool to commit the crime.

Consequently, when an artificial intelligence system is programmed to detect threats coming from the Internet, and protect the computer from some threats such as viruses and hackers, and after the program is activated by the programmer, the artificial intelligence enters websites to detect those threats and destroy any program. He viewed it as a threat. In this case, what the artificial intelligence committed is considered illegal entry and represents an information crime. Here the programmer did not instigate the artificial intelligence system to commit this act that constitutes a crime, but he had to expect that.

According to this model, the responsibility in this case falls on the programmer if this crime is the expected result of his programming, according to the criminal liability for error resulting from negligence in following what the law requires as to the duty of caution against potential risks. The responsibility here is not intentional on the part of the manufacturer, programmer, or operator. or even the user.

Third Model: Direct Responsibility of Artificial Intelligence: This model assumes that artificial intelligence systems are considered as human being in committing crimes, and this means that artificial intelligence can be held accountable when committing a criminal crime just like humans (Richard, 1986).

But the question that arises in this case is how can AI entities meet the requirements for criminal liability. It is true that these technologies exceeded human capabilities in some ways and exceeded human intelligence. However, it has not yet been proven that it can meet the requirements of criminal liability (David, 2009).

Based on this model, it is possible to admit holding artificial intelligence criminally accountable, on condition that it can fulfill the two elements of responsibility. Nothing hence prevents jumping to this conclusion as long as these entities are able to control their organs mechanically, and as long as the action issued by them was carried out by them.

A robot performing an electrical movement can cause a shock to a person standing nearby and hence may be liable for assault. This act fulfills the requirements of the criminal conduct that constitutes the crime of assault or battery.

There is an opinion that artificial intelligence systems are not qualified to endure criminal liability, especially since criminal liability requires mental capabilities such as knowledge, intent, negligence, or recklessness, as required by criminal law.

In this perspective, we can presuppose the existence of the electronic personality which is liable for the criminal act. Thus, it can be assumed that the A.I has the intention to commit the crime (David, 2009)

-Evaluating the different opinions regarding the report on criminal liability for artificial intelligence:

The opinion that deserves discussion and study is the one that acknowledges the possibility of a legal personality for artificial intelligence. However, the question arises whether the artificial intelligence systems could be subject to the rules of criminal liability, such as liability defenses, for example.

If we return to applying the rules of criminal responsibility with regard to the impediments to that responsibility, we find among those impediments young age or insanity. Since a young person is unable to understand what is wrong and is unable to distinguish between right and wrong, he lacks the foundation of criminal responsibility. The same is true for insanity, as mentally ill patients are unable to distinguish right from wrong or control their impulsive behavior.

If this is applied to artificial intelligence systems, we will find that most artificial intelligence algorithms are highly capable of analyzing what is permissible and prohibited to do. When artificial intelligence algorithms work correctly, there is nothing preventing them from using their capabilities to analyze the data they receive, but the question is raised if these entities suffered a defect in the operating system, or if the algorithms of these systems suffered a malfunction or a virus causing them to become out of control and were involved in a crime being committed: may they be exempted from responsibility? We find it possible to equate it with insanity or loss of consciousness in human beings (Edward, 1984).

Another question is raised: can we admit the criminal participation of artificial intelligence entities? We find that this can be imagined according to the model of direct liability presented previously. The criminal liability of artificial intelligence systems does not replace the criminal liability of the programmer or operator. A human being can collude with an automated entity as a partner and take one of the forms of participation such as aiding or abetting. When the realistic and mental capabilities of an automated entity are available, its responsibility is established, and the responsibility of the human perpetrators who

participate with it in committing the crime is also conceivable, then the responsibility falls on all of them, regardless of whether the perpetrators are humans or machines (Anthony, 2002).

The question is also raised as to the application of defenses such as causes of justification. We find that the answer to this question is the same as with regard to impediments to liability. It is possible to imagine the application of justification such as legitimate defense, a state of necessity, and the use of the right. Since the causes of justification are objective and closely related to the material nature of the crime and have nothing to do with the person or the psychology of the perpetrator. No difference is then made between being a human or a machine. If a police order is issued to a robot to arrest a person illegally, the robot carrying out the order may not be criminally responsible.

Finally, how can custodial penalties be applied to artificial intelligence systems? Since the goal of punishment is to rehabilitate violators of the law, will the same purpose be in the case of artificial intelligence? We found those who tend to say that it is possible to correct the behavior of electronic entities just like humans (LIMA, 2023).

If we assume that artificial intelligence systems can be held criminally accountable, how can penalties such as imprisonment, fines, or the death penalty be applied in practice? These are the same problems that faced - previously legal persons that can be held accountable. The solution was simple: the robot was treated like a human being. When a fine is imposed, the company pays the fine in the same way a person pays, and in the same way the company fulfills its obligations by paying its bills, for example. The legal entity may be sentenced to the penalty of dissolution or prevention from performing its function. The main question for demanding amendments to the penalties that can be imposed on a robotic entity is the same as the penalty in relation to a human being. **Would that importance serve the same purpose for a robotic entity? How do these sanctions affect artificial intelligence**?

The death penalty for humans is intended to deprive a person of life, and to ensure that he does not commit a crime in the future (David, 1980). The life of an artificial system consists of its existence as an independent entity, such as a robot or a program installed on a computer. If the death penalty is imposed on an artificial entity, this can be applied by deleting a program that controls a robot. In this case, the system is unable to commit any other crime, so it is considered a death penalty.

Likewise, the prison sentence aims to deprive a person of his freedom, and the freedom of a robotic entity is the freedom to act as an entity, such as a robot that participates in factory work or in performing surgical operations. A prison sentence can be implemented by putting it out of service for a specific period, and then it is Restricting his freedom.

A final question arises about determining the applicable law as to place regarding the crimes of artificial intelligence technologies. An opinion responds to this by saying that the domicile of the legal personality of artificial intelligence may be where the artificial intelligence systems are registered, such as the system of legal companies. Several legal procedures are imposed to register the artificial system and the natural persons who legally represent it. This is the case for the company director who represents it in proceedings before the law (Al-Desouki, 2022)

Regarding the aforementioned, some may object that these ideas cannot be implemented in any way, and that this is not compatible with the rules of criminal law. However, imagining this is not far-fetched, especially since the biggest and most important legal challenge facing the future of artificial intelligence is the recognition of legal personality and legal regulation of this new creature. In addition, if the legal

personality of artificial intelligence can be established, and its ability to fulfill rights and assume obligations can be proven, it can thus be granted the right to exercise the right to ownership, conclude contracts, create, possess, and control intellectual property, and own bank accounts. The question will remain as to how the framework is conceived. The appropriate legal framework for dealing with these synthetic tools is still in place (Swinson, 2023)

In addition, the widespread use of artificial intelligence technology in various fields faces another challenge, which is protecting data and ensuring information security. Some legislation has attempted to confront this type of challenge, by establishing special legal frameworks to ensure a high level of protection, as we will see later.

Section II: Legislative Attempts to Establish Legal Systems

Governing AI: The need for legal regulation of artificial intelligence:

Subjecting A. I to the law was first invoked by Amnesty International in the first conference on artificial intelligence and the law in Boston in 1987, which was the first step to creating a legal status for artificial intelligence systems. This conference attempted to come up with a legal definition of the term artificial intelligence, and many discussions about the need for legal procedures to regulate the field of artificial intelligence, but at this time it did not provide anything linking artificial intelligence to the law, and the legal features of artificial intelligence remained unclear until recent years.

With the rapid developments witnessed in the field of artificial intelligence, countries are rushing to take many legal initiatives, in an attempt to regulate the legal status of A.I and this indicates the need to control the negative consequences that the world of information technology can produce and its use on a large scale.

In 2016, France adopted a law granting the National Commission for Computer Technology and Liberties to study the social and ethical behaviors of the digital technologies that are newly produced. China is the first leading country in the use and development of artificial intelligence and is working on developing a plan to regulate the next generation of artificial intelligence by 2030 AD. Among the strategies it has developed for that plan is the establishment of a legal and regulatory framework for the use of artificial intelligence, in addition to setting ethical standards and a system through which it can evaluate the security and capabilities of artificial intelligence systems.

The United States of America is making the greatest effort to regulate research in the field of artificial intelligence with the Artificial Intelligence Initiative Law of 2020. As for Brazil, in September 2021, the Brazilian House of Representatives approved a draft law regulating the use of artificial intelligence, taking into account that it establishes liability on the basis that human entities governed by public or private law and providing public services are responsible for the damages caused by their agents, which guarantees the right Recourse to the responsible person in cases of intentionality or error (responsibility for things). This draft law approved several principles, including:

- Ensuring that artificial intelligence systems seek to achieve results that are beneficial to humans, as well as respecting human dignity and privacy and protecting their personal data and basic rights. And work to reduce the use of artificial intelligence systems for discriminatory or abusive purposes, meaning ensuring non-discrimination.

- Ensuring the pursuit of neutrality, safety, prevention, and transparency when communicating with artificial intelligence systems. That is, defining the general standards that guide its operation.

As for the objectives of the Brazilian draft law on artificial intelligence, with regard to ensuring and protecting the rights of artificial intelligence, they are as follows:

(a) Guaranteeing the freedom to express thought and the free expression of intellectual, artistic, scientific, and communication activity.

(b) Security, privacy and protection of personal data.

(c) Ensuring information security.

(d) Maintaining the stability, security, resilience, and functionality of artificial intelligence systems through technical measures consistent with international standards.

In Europe, in April 2021, the European Commission adopted the "European Union Regulation for the Artificial Intelligence (AIA) Act. It proposed developing a regulatory and legal framework for the uses of artificial intelligence, especially with regard to service providers of artificial intelligence systems, defining their responsibilities, and the entities that benefit from them in a way that does not harm humans. The European Parliament adopted its position on June 14, 2023. There were 499 affirmative votes, 28 negative votes, and 93 abstentions. Thus, recommendations of some amendments to the proposed regulations were introduced (Tambiama, 2023).

It appears that the proposed European Artificial Intelligence Law attempts to take precautionary measures to prevent harm that may result from the use of artificial intelligence systems. It places the greatest responsibility on service providers without placing any responsibility on the AI entities themselves as independent entities capable of bearing responsibility. This regulation included regulating three types of uses of artificial intelligence as follows:

(1) **Prohibited use of artificial intelligence:**

The bill on Artificial Intelligence Law prohibits the use of artificial intelligence systems that perform any of the following:

-Uses subconscious techniques to manipulate a person's behavior, in a way that may cause psychological or physical harm.

- Exploits the weaknesses of some people due to their age or physical or mental disability in a way that may result in psychological or physical harm.

- Provides real-time remote biometric identification of places that can be accessed by law enforcement, except in cases of public safety, emergencies, and specific times.

(2) **High-risk use of artificial intelligence:**

This qualification exists when the use of AI constitutes a significant threat to the health or safety as well as the fundamental rights of persons. This must be evaluated by the service or product provider before putting artificial intelligence systems on the market. Future AI products will be assessed as having a high risk to health, safety, or fundamental rights, as they impact many people.

This law requires organizations that develop or use high-risk artificial intelligence systems to adhere to a set of technical and regulatory requirements, including establishing safeguards against certain types of artificial intelligence systems. These safeguards verify their outputs throughout the system's life cycle, and the necessary human supervision of the system in general. European Artificial Intelligence law places

liability, in the event of damages, on the party that places the system on the market (the "provider"), whether it is a third-party provider, or a company developing the artificial intelligence itself.

In the case where distributors, importers, and users place on the market a high-risk artificial intelligence system in their name or make fundamental modifications to it, they must meet certain requirements. They must submit to the obligations of the supplier, and in the event that they do not comply with this, causing in this way prejudice to humans, the original supplier is exempted from responsibility and full responsibility falls on them.

In addition, this law imposes regulation after high-risk systems are put on the market. The law creates legal and mandatory obligations on the part of distributors, as accidents or serious errors occurred in artificial intelligence systems that violate safety laws or basic rights. These defects must be reported to the National Supervisory Authority. The regulator may forcefully withdraw high-risk systems that violate the law from the market.

(3) Artificial intelligence systems with limited risks:

The limited-risk artificial intelligence systems are placed under transparency requirements, especially intelligence systems that interact with people. They face obligations similar to the European General Data Protection Regulation (GDPR), including notifying users that they are interacting with an artificial intelligence system, and inform them of the personal data it collects. Persons must be informed of the specific purpose of collection and the time for collection and processing and whether users are classified into specific categories such as gender, age, or ethnicity. All non-high-risk AI systems must comply with safety legislation and preserve the fundamental rights of EU citizens.

Finally, the proposed European Artificial Intelligence Law imposes penalties in the event of violating it, as is also the case regarding the violations of the provisions of the European Data Protection Regulation, which are as follows:

First: These rules apply extraterritorially to service providers and users outside the European Union, if the system output is used in the European Union.

Second: Failure to comply with prohibited uses and data governance obligations is punishable by a fine of up to 30 million euros or 6% of the total annual sales worldwide (whichever is higher).

Third: For high-risk AI systems, the maximum fine is 20 million euros or 4% of the annual turnover.

Fourth: In the event that incorrect, incomplete, or misleading information is provided to the competent bodies, the penalty shall be a fine of up to 10 million euros, or 2% of the annual sales volume.

This law has not been issued in its final form yet, noting that it exempts currently existing artificial intelligence systems from being subject to its provisions, unless they witness a change in purpose or design in the future. The legislative movement is still ongoing, in order to provide guarantees to protect the uses of smart systems, which have become a challenge to humanity. Rather, we may imagine that they precede human capabilities and represent a tool that may harm them rather than benefit them.

Results

- Artificial intelligence has a role that overlaps with human work or works alongside it. At present, artificial intelligence is not criminally accountable for its work. The responsibility falls entirely on the human element behind it, whether the designer, the operator, or... the programmer as well as the user.

- Opinions differed about the possibility of granting artificial intelligence an independent legal personality, and opinions still differ about the foundations upon which that personality is based. Is it treated like humans, like a legal person, or is it an independent person?
- Many concepts of criminal liability of artificial intelligence could be imagined, such as the responsibility of the moral actor, the responsibility for potential risks, and finally the direct responsibility of artificial intelligence itself. Each of these concepts had foundations that could be accepted in establishing a criminal responsibility of artificial intelligence.
- Artificial intelligence can conceivably commit a crime when it acts in contravention with the law or fails to act when obligated to do so. We must consider all perspectives because artificial intelligence systems operate according to the programming prepared in advance by the programmer or operator.
- Many legislations have taken proactive steps regarding the risks that artificial intelligence may pose, by establishing regulatory and legal frameworks for the uses of artificial intelligence (without recognizing independent legal personality). These regulations considered the services provided by artificial intelligence systems and contemplated their responsibilities, and the parties that benefit from them in a way that does not harm humans.

Conclusion

After our research, we reviewed the legal challenges facing those in charge of the legislative industry, with regard to the future of artificial intelligence technologies, especially the urgency and challenge that these new entities impose on legislators. In developing legal frameworks and rules that suit the special nature of this artificial intelligence. In addition, we discussed the difficulties that may be associated with the possibility of creating an independent legal personality for artificial intelligence systems. The research reached several results and recommendations as follows:

Recommendations:

(1) The principle of appropriateness and legal necessity imposes the necessity of resolving the problems concerning the legal personality of artificial intelligence, as artificial intelligence systems are developing very rapidly, especially regarding their capabilities to act consciously and independently from their programmer or operator.

(2) Given that artificial intelligence will create new entities in addition to natural or legal entities, legislators - especially in our Arab countries - must accelerate the development of systems that determine the nature of dealing with these entities. Whether it concerns the rules of law or the rules of ethics, it is important to imagine a unique personality, whether in terms of the limits of this personality or the type of rights granted to it. Thu the AI is distinguished from other natural or legal persons, as a guarantee to protect artificial intelligence itself, and protect humanity from its dangers.

(3) At present, we find that it is most appropriate to determine criminal liability for artificial intelligence, which the responsibility is borne by the person who programmed or developed the artificial intelligence, due to which harm occurred, whether this was done intentionally or accidentally.

(4) We see that for artificial intelligence to be tried, it must possess awareness, which requires its transition from the stage of artificial intelligence to the stage of artificial perception, on which technical scientists are working at the present time.

(5) If it is envisaged to impose a punishment on artificial intelligence systems, it will be in accordance with contemporary criminal policy, especially regarding the purposes of punishment, and the evolution from the

criminal philosophy from causing pain to the offender to reforming and rehabilitating him. This can be applied to artificial intelligence, especially since it has so far been characterized by a lack of awareness.

(6) It is necessary, when creating, designing, or programming artificial intelligence systems, to subject them to experimental periods for a specific period, which allows studying their efficiency and its performance.

References

Al-Desouki, Mona Muhammad Al-Atris, "Crimes of Artificial Intelligence Technologies and Independent Electronic Legal Personality, A Comparative Study" Journal of Legal and Economic Research, Faculty of Law, Mansoura University, Egypt, Issue 81, September 2022.

Al-Khatib, Muhammad Irfan "Artificial Intelligence and the Law - A Critical Comparative Study in - French and Qatari Civil Legislation - in Light of the European Rules in the Civil Robotics Law of 2017 and the European Industrial Policy for Artificial Intelligence and Robotics of 20172019." BAU Journal - Journal of Legal Studies -Vol. 2020- Article 4, Available at: https://digitalcommons.bau.edu.lb/lsjournal/vol2020/iss2020/4

Al-Lami, Yasser Muhammad, "Criminal Liability for Artificial Intelligence Acts: Reality and Expectations, A Prospective Analytical Study." Paper presented for the Conference on Legal and Economic Aspects of Artificial Intelligence and Information Technology. May 23-24, 2021 AD. Journal of Legal and Economic Research, special issue of the (twentieth annual international conference) Faculty of Law, Mansoura University.

Anthony M. Dillof, Unraveling Unknowing Justification, 77 NOTRE DAME L. REV. (2002), p 1547.

Bishr, Aisha Bint Butti, "Principles and Guidelines for the Ethics of Artificial Intelligence, Smart Dubai, Ethics", United Arab Emirates, 2019 AD, pp. 5-6.

David J. Rothman, "For the Good of All: The Progressive Tradition in Prison Reform, HISTORY AND CRIME". James A. Inciardi & Charles E. Faupel eds., 1980, p 271.

David Levy, The Ethical Treatment of Artificially Conscious Robots, I INT'L J. SOC. ROBOTICS. (2009) p 215.

Edward D. Hoedemaker, "Irresistible Impulse" as a Defense in Criminal Law", 23 WASH. L. REV. 1, 7 .1948.

Hallevy, Gabriel (2010), "The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control". Akron Intellectual Property Journal: 4(2), p 9.

Hosni, Mahmoud Naguib, "Explanation of the Penal Code, General Section, General Theory of Crime and the General Theory of Punishment and Precautionary Measures," eighth edition, Dar Al-Nahda Al-Arabi, year 2018, p. 602.

Lima, G. et al. Explaining the punishment gap of AI and Robots. 2020. Available in: https://www.researchgate.net/publication/339972166_Explaining_the_Punishment_Gap_of_AI_and_Robots.

McKinney, David, "Alice: Tumbling Down the Rabbit Hole of Software Patent Eligibility," UMKC Law Review, Vol. 84, 2015, p. 261.

Minsky, M., "Steps Towards Artificial Intelligence," Proceeding of the IRE, January 1961.

Richard E. Susskind, "Expert Systems in Law: A Jurisprudential Approach to Artificial Intelligence and Legal Reasoning", 49 MOD. L. REV. (1986). P 168

Stela Enver Mecaj stela. "ARTIFICIAL INTELLIGENCE AND LEGAL CHALLENGES", Centro Universitário Christus. 24 February 2022. https://www.redalyc.org/journal/6338/633875004009/html/#B11

Swinson N, J.; Slater, R.; Fouracre, K. "AI Guides /Facial Recognition".2020. Available in: https://www.lexology.com/library/detail.aspx?g=ed57828c-8e53-4977-a5be-043ca446d935.

Tambiama Madiega; Graphic: Samy Chahri. Members' Research Service. "Artificial Intelligence Act", European Parliamentary Research Service. PE 698.792 – June 2023.

Terry Winograd, Thinking Machines: Can There Be? Are We? THE FOUNDATIONS OF ARTIFICIAL INTELLIGENCE. Derek Partridge & Yorick Wilks eds., (2006). P 167.

Laws and regulations:

- French Civil Code.
- The American Artificial Intelligence Initiative Act of 2020.
- EU Regulation Artificial Intelligence Act 2023 (AIA).
- European Regulation No. 2016/679 issued by the European Union on April 27, 2016, regarding the protection of individuals with regard to the processing of personal data and the freedom to transfer this data. This entered into force on May 25, 2018.