



International Journal of Artificial Intelligence Governance and Human Rights

ISSN online: 2977-604X - ISSN print: 2977-6031

<https://www.inderscience.com/ijaighr>

Artificial intelligence in line with the provisions of international law: risks and challenges

Sarah Al-Arasi, Ola Ghazi Abbasi, Hisham Al-Kasasbeh, Wasan AlRawashdeh, Randa Alsayed El-bheery

DOI: [10.1504/IJAIGHR.2025.10072081](https://doi.org/10.1504/IJAIGHR.2025.10072081)

Article History:

Received:	22 January 2025
Last revised:	01 April 2025
Accepted:	02 April 2025
Published online:	14 April 2026

Artificial intelligence in line with the provisions of international law: risks and challenges

Sarah Al-Arasi

Faculty of Law,
Al-Zaytoonah University of Jordan,
Amman, 11733, Jordan
Email: Dr.arasi@yahoo.com

Ola Ghazi Abbasi

Department of Comparative Law,
Sheikh Nouh Al-Qudah Collage for Sharia and Law,
The World Islamic Science and Education University,
Amman, 11947, Jordan
Email: ola.g.abbasi@hotmail.com

Hisham Al-Kasasbeh

Faculty of Law,
Al-Zaytoonah University of Jordan,
Amman, 11733, Jordan
Email: hish_kasasbeh@yahoo.com

Wasan AlRawashdeh

Judge, Jordanian Judicial Council,
Amman, 11118, Jordan
Email: Wasan_alrawashdeh@yahoo.com

Randa Alsayed El-bheery*

Legal Researcher,
Amman, 11593, Jordan
Email: randa.rafat55@gmail.com

*Corresponding author

Abstract: This study showed the great importance of addressing the risks of artificial intelligence and its technologies in light of its continuous developments within the rules and provisions of international law, as the international community has begun to suffer from many challenges and moral, and legal risks as result of this development, which had to address the civil and criminal liability resulting from the absence of its legal personality that makes them eligible for litigation. Accordingly, the researcher reached a number of results, the most important is that the criminal liability is to be limited to the individual and not the artificial entity, and then she recommended the necessity

of introducing special penalties for smart machines such as destroying or preventing them from working under the penalty of punishment if this rule was violated.

Keywords: artificial intelligence; civil liability; criminal liability; human rights; international law.

Reference to this paper should be made as follows: Al-Arasi, S., Abbasi, O.G., Al-Kasasbeh, H., AlRawashdeh, W. and El-bheery, R.A. (2026) ‘Artificial intelligence in line with the provisions of international law: risks and challenges’, *Int. J. Artificial Intelligence Governance and Human Rights*, Vol. 1, No. 1, pp.5–24.

Biographical notes: Sarah Al-Arasi has held several academic and leadership roles, including Deputy Dean and Head of the Law Department at Al-Zaytoonah University of Jordan. They currently serve as a Chief Editor of the University’s Journal for Legal Studies and are a Member of both the Center for Leadership and Innovation and the Scientific Research Council. Previously, they were Director and Deputy Director of the Center for Migration and Refugee Studies at Sana’a University and served on its Human Rights Center board. They also held the position of Dean of Law and Student Affairs at the University of Applied and Social Sciences in Yemen.

Ola Ghazi Abbasi began her academic career as a full-time Lecturer at Al-Isra University, Jordan (2012–2013), then served as an Assistant Professor at the Same university (2013–2015). They continued as an Assistant Professor (2015–2021) and later Associate Professor (2021–present) at the World Islamic Sciences and Education University. Professionally, they worked as Director of the Administrative and Legal Department at Arab Orient Insurance Company in 2002, and as a legal consultant at the American University in Madaba (2011–2012). Since 2015, they have also served as a Faculty Member at the World Islamic Sciences and Education University.

Hisham Al-Kasasbeh served as Dean of the Faculty of Law at Jordan Zaytoonah University from February to October 2017, and as Vice-Dean from October 2015 to February 2017. Concurrently, they headed the Law Department during that same period. They have been a member of the Law Department Council since 2013 and served on the Faculty Council from 2014 to 2017. Additionally, they were a member of the University’s Discipline Committee during the academic years 2013/2014 and 2015/2016, contributing significantly to academic leadership and governance at the Faculty of Law.

Wasan AlRawashdeh’s experience bridges legal practice, academia, and legal reform. From 2006 to 2008, she practiced law, gaining skills in dispute resolution, legal drafting, and courtroom advocacy. In 2023, she became a Lecturer at The General Secretariat of the Judicial Council, reflecting her commitment to legal education. She has published research on judicial reform, human rights, and modern legal frameworks. Additionally, she contributed to the profession through active membership in prominent committees, including the Arab Women’s Legal Network (supported by Queen Rania), the Danish Dignity Project, and the First Prosecution Conference Committee, promoting justice and legal development. Now as a judge and legal professional, she has always prioritised integrity, fairness, and excellence in every aspect of her work.

Randa Alsayed El-bheery holds a Master's degree in International Criminal Law and a Bachelor's degree in Law, both from Al-Zaytoonah University, with distinction. Her academic focus is complemented by research contributions in international and comparative law. She has published two peer-reviewed papers: one on franchise contracts in Jordanian legislation and another on the governance of artificial intelligence under international law. A third paper is currently under review. Her work reflects a strong commitment to legal scholarship and a deep interest in the evolving intersection of law, technology, and global legal standards.

1 Introduction

The outcomes of the Fourth Industrial Revolution, also known as the Digital Revolution, have impacted various aspects of life, it was the initial spark for the massive expansion of modern and intelligent information systems; which have enabled the entire international community to embrace the tools of artificial intelligence, considering that provided nations with the opportunity to reformulating their strategies and outputs, creating the way for competition locally and internationally. Artificial intelligence and its technologies were developed to simulate the human mind and its functions, facilitating the replacement of human labour with industrial alternatives, with reservations about the possibility of such technologies causing programming errors, which are sometimes unavoidable.

Due to the superior technological advancements, and urgent need to adopt these alternative technologies and mechanisms, it has become imperative for the law to establish a legislative framework and integrated legal provisions that keep move with both domestic and international developments related to artificial intelligence tools. From that point of view artificial intelligence has become a top priority that requires clarity on its legal nature, criminal liability, and the establishment of international agreements to regulate its uses. Such measures aim to eliminate or limit misuse, especially since these technologies' most prominent and widespread applications include smart weapons used in armed conflicts. These weapons may violate the principles of international law and international humanitarian law, blatantly infringing on the most basic human rights in ways unacceptable to any human conscience or governing state, particularly within the context of the international community governed by these laws.

The development of artificial intelligence technologies has progressed rapidly, making it difficult for both local and international laws to keep up, as artificial intelligence technologies have presented challenges in applying existing legal rules to all the issues and cases that artificial intelligence introduces. Whether artificial intelligence should be granted legal personality has been a subject of debate and criticism, making confining the process of these technologies within a legal framework a difficult and complex task, but, it remains necessary due to the varying benefits and harms that it entails.

The importance of this study is reflected in the fact that artificial intelligence continues to intersect with the provisions and principles of international law, both positively and negatively, to highlight the urgent need to strike a balance between advancing these technologies on the one hand and preserving the integrity and sovereignty of international law on the other. Thus, it has become imperative for the

international community to regulate artificial intelligence and its technologies by establishing legal frameworks that align with the nature of artificial intelligence while respecting the rules of international law, which is referred to as the governance of artificial intelligence from the perspective of upholding of international law.

This study aimed to identify the relationship between the principles of international law and artificial intelligence by addressing the concept of artificial intelligence and its connection to the provisions of international law. Thus, seeks to propose a legal framework to govern artificial intelligence technologies; while also identifying the challenges they create to the international community and its legal systems, in order to establish a governance framework that aligns with international law.

Therefore, the main research problem mentioned above branches into the following sub-questions:

- What is the stance of international law on artificial intelligence technologies?
- What are the legislative and legal frameworks governing the applications of artificial intelligence?
- What types of legal liability arise from errors in artificial intelligence technologies under the rules of international law, and who bears responsibility for them?

As for the methodology, the study will employ descriptive research and an inductive analytical approach, by examining the relationship between artificial intelligence technologies and the sovereignty of international law, including legal regulation, and civil, and criminal liability. Also, the study will review and analyse legal texts and international agreements that could potentially regulate the use of artificial intelligence in a manner that safeguards the principles of international law from any violation or infringement.

The study plan will be divided into two main sections, each containing two subsections. Section 1 will address the nature of artificial intelligence and its relationship with international law. This section will be further divided to discuss the stance of international law on artificial intelligence applications in the first subsection, and the legislative framework for artificial intelligence applications in the second subsection.

Section 2 will focus on the liability of artificial intelligence applications, it will cover civil liability for damages caused by artificial intelligence errors and its scope in the first subsection, and criminal liability arising from artificial intelligence errors and its scope in the second subsection.

2 The nature of artificial intelligence and its relationship with international law

Artificial intelligence and its technologies, which have demonstrated their ability to mimic the human mind, have gained significant importance as one of the forms of modern technology, and despite transcending the technical field, there is no universally agreed-upon definition of artificial intelligence. Some define it as “*a branch of computer science aimed at designing intelligent systems that simulate human thinking and behaviour*” (Alfaqi, 2012), while others describe it as “*a field of computer science that explores the application of technology based on computer simulation of human intelligence traits*” (Abd Alsattar, 2012). Despite the diversity and differences in

definitions, they all converge on a single essence: its immense capacity to parallel the human mind and make decisions independently of human intervention (Alrai, 2023).

It can be argued that the emergence of artificial intelligence necessitated the creation of harmony and balance between its technologies and national as well as international legal frameworks. This is because these technologies have posed significant challenges due to their autonomy and ability to make decisions that can be entirely decisive on their own (Masoud et al., 2021). With the increasing number of producers of intelligent machines, it is natural for the international community to adopt whatever is within its reach to achieve international interests in general. Consequently, the use of these technologies is growing rapidly, spanning economic, service, military, and even pharmaceutical fields.

Some pharmaceutical companies have utilised artificial intelligence to employ neural networks to analyse images of cells tested with new types of drugs or to use intelligent machines to diagnose and discover rare diseases, enabling them to propose new drug formulas for treatment (Barqawi, 2023). This has highlighted the necessity of regulating the development of artificial intelligence, particularly at the international level, especially since the use of smart weapons in armed conflicts has become a necessity in warfare. These technologies inevitably risk violating the rules and conventions of international law in one way or another.

2.1 The stance of international law on artificial intelligence applications

Artificial intelligence systems are more closely linked to international human rights law than other areas of law, primarily because these systems are most prominently used in smart weapons deployed in armed conflicts. This makes human rights, above all else, a focal point for the international community to ensure that intelligent technologies are deterred from violating human rights in any form.

In this regard, Michelle Bachelet, the United Nations High Commissioner for Human Rights, emphasised in her report to the UN in September 2021 – based on her framework on technology and human rights – the importance of halting the sale and use of AI systems that pose a serious threat to human rights until appropriate measures and safeguards are implemented. She also called for a ban on AI applications that are inconsistent with international human rights laws (United Nations, 2021).

The report highlights that the rapidly at which countries and companies have integrated artificial intelligence applications has often failed to ensure due diligence. This has led to numerous instances where individuals were treated unfairly due to reliance on these technologies. Examples include being denied social security benefits because of flawed artificial intelligence tools or being arrested due to errors in facial recognition systems. Your observations provide a thoughtful perspective on the challenges and opportunities associated with artificial intelligence.

Bachelet emphasised the urgent need to strike a balance between harnessing the benefits of artificial intelligence technology for humanity and protecting human rights. This requires states and societies to take appropriate measures to ensure that the use of artificial intelligence aligns with human rights principles and is properly regulated, with necessary oversight and boundaries in place to prevent ongoing violations. This is the direction many international organisations and entities are striving toward, aiming to ensure that artificial intelligence serves the interests of everyone and does not pose a threat to human rights.

The three legislative institutions – the European Commission, the European Parliament, and the Council of the European Union – are still engaged in negotiations regarding the proposed European Union Artificial Intelligence Act, which is expected to be finalised before the end of 2023. Additionally, the Council of Europe is negotiating an international convention titled the Framework Convention. This convention aims to design, develop, and implement artificial intelligence systems in a manner consistent with the Council of Europe's standards for human rights, democracy, and the rule of law. Notably, this convention will include non-European countries, reflecting its ambition to become a global instrument for setting artificial intelligence standards (Fanouchi and Conoli, 2023).

2.2 The legislative framework for artificial intelligence applications

Artificial intelligence has firmly established itself in both local and international communities, creating a pressing need to develop a regulatory system that addresses the requirements for dealing with artificial intelligence technologies. In response, some legislative bodies have introduced new laws capable of addressing these developments, while others have revised their legal stances to better understand and effectively regulate artificial intelligence systems. This approach aims to enrich future generations, who may encounter artificial intelligence and its phenomena in their entirety.

It is worth noting that UNESCO has shown interest in exploring the ethical dimensions of the information society and digital technology since 1977. In 2018, UNESCO hosted a series of meetings focused on harnessing artificial intelligence for the benefit of humanity, emphasising the values, principles, and ethical frameworks necessary for the appropriate use of intelligent machines. Also, UNESCO worked on creating a code of ethics outlining the rules for ethical practices in the field of artificial intelligence, based on predefined standards (UNESCO, 2019).

The United Nations highlighted in its 1975 General Assembly Resolution the declaration on the use of technological progress for the benefit of peace and humanity emphasised the international community's interest in fostering cooperation among nations to understand artificial intelligence and utilise it for development, creativity, and innovation. Furthermore, in 2018, the UN held a meeting addressing the diverse activities of artificial intelligence and its potential uses in achieving public good both nationally and internationally (Ibrahim, 2022).

In 2017, the European legislature issued a specific law for robots, eliminating the description of robots as 'objects' and replacing it with the term 'electronic agent'. In the same year, the European Union worked on enacting the European Civil Law on Robotics by forming a group of experts and officials under the European Commission to study and provide recommendations on the legal and ethical challenges arising from the rapid development of robots and artificial intelligence. Thus, the report submitted by this group included several recommendations on various issues, such as establishing a registration system for advanced robots, enhancing the civil liability of robots, and advocating for adherence to ethical principles in the design and use of artificial intelligence technologies (Mohammad, 2021).

Subsequently, in 2019, the European Union issued a set of guidelines outlining how to develop artificial intelligence applications. As for USA, it enacted a law in 2017 focused on understanding artificial intelligence systems, titled the "Artificial Intelligence Future and Its Global Prospects Act" (Ali, 2022).

Regarding the stance of Arab legislation, the Emirati legislator introduced Law No. (4) of 2020 on Drones, which serves as a permit to operate this type of aircraft in UAE airspace. This law was enacted due to the inadequacy of traditional aviation laws in addressing artificial intelligence-powered drones. Consequently, regulatory and executive bylaws, along with other related laws, were established. These include provisions for compensation in the event that such drones cause harm to others in the future (Ibrahim, 2022).

Similarly, the Egyptian legislator addressed artificial intelligence applications by issuing Law No. (216) of 2017 on Remotely Piloted or Autonomous Aircraft. This law includes a set of rules and regulations that aircraft owners and pilots must adhere to, aiming to ensure the safety of passengers, pilots, and society as a whole. It mandates the implementation of safety measures and procedures to prevent accidents and protect against potential risks. Additionally, the law emphasises compliance with international aviation laws and recognised international standards.

As for the Jordanian legislator, the Ministry of Digital Economy and Entrepreneurship presented a draft of the Jordanian Artificial Intelligence Strategy and its Executive Plan for 2023–2027. This draft was prepared in collaboration with the European Union and the United Nations Economic and Social Commission (ESCWA). The draft calls for the development and activation of artificial intelligence strategies, as well as the creation of a timeline for implementing projects that will emerge from this plan. The Ministry of Digital Economy and Entrepreneurship announced that it has set five main objectives for the AI strategy in Jordan. The first four objectives focus on developing the artificial intelligence support system by building capacities, enhancing Jordanian skills and expertise in this field, encouraging scientific research and development, promoting investment and entrepreneurship, and ensuring a legislative and regulatory environment that supports the safe use of artificial intelligence. The fifth objective focuses on using artificial intelligence tools to improve the efficiency of the public sector and priority sectors.

Given the importance of data as a key resource in developing and adopting artificial intelligence solutions, the draft includes a chapter explaining the role of data in achieving economic development, improving government performance, and supporting decision-making processes through the analytics and predictions provided by artificial intelligence systems.

For the significant autonomy of artificial intelligence applications, there has been considerable debate and disagreement over whether artificial intelligence systems should be classified as ‘persons’ or “objects” – in other words, whether they can acquire legal personality. The foundation of natural legal personality lies in the ability to acquire rights and bear obligations, considering that intelligent machines are now capable of making decisions independently, this grants them a degree of autonomy separate from human involvement. These differing opinions have sparked significant controversy over the legal nature of artificial intelligence and whether it can be granted legal personality.

This issue has posed a legal challenge for nations worldwide, leading to varying approaches in regulating the legal nature and personality of artificial intelligence. Countries have adopted different legislations defining the rights and responsibilities of intelligent machines. In this context, the European Union issued the General Data Protection Regulation (GDPR) in 2016, which addresses issues of AI liability in cases where artificial intelligence causes harm to individuals, whether physical or financial. The regulation requires organisations using artificial intelligence to take measures to

mitigate risks and provide clear explanations for decisions made by these technologies (Badri, 2022).

In 2019, the Canadian government introduced new legislation known as the “National Artificial Intelligence Framework”, or “Artificial Intelligence Framework”. This framework aims to promote trust, transparency, and accountability in the use of artificial intelligence in Canada. It includes a set of guiding principles and core values that organisations must adhere to when utilising artificial intelligence, such as transparency, accountability, legal protection for individuals, diversity, and inclusion (ESCWA, 2020).

In USA, local governments are adopting generative AI technologies, focusing on minimising risks and enhancing efficiency in public service delivery. It recommends a phased approach, starting with low-risk pilot applications and developing a comprehensive long-term plan for scaling AI adoption. emphasising and identifying tasks that can be improved with generative AI, creating detailed implementation plans, and considering the impact on workflows and employees. It also highlights the need to balance risks and benefits while developing regulatory and training strategies to ensure the responsible and effective use of generative AI in the public sector (Mckinsey and Company, 2024).

Thus, it can be said that the extensive local and international efforts to regulate and standardise artificial intelligence systems, ensuring their alignment with the provisions and rules of international law and other national laws, continue to emerge consistently. This indicates that artificial intelligence holds significant importance, compelling the international community and its members to take a firm stance toward intelligent machines as one of the modern innovations that will eventually be granted certain rights and obligations inherent to legal personality. This is due to the prominent position artificial intelligence has achieved across various sectors, both locally and internationally.

In any case, researchers argue that it is difficult to grant artificial intelligence systems legal personality. Granting them such status would imply their ability to bear obligations and acquire rights, which does not align with their nature unless they surpass stages of autonomy and achieve everything a natural person can acquire. Without this, artificial intelligence cannot be granted the right to express opinions, vote, or exercise similar rights. Moreover, even if artificial intelligence systems can surpass human cognitive limits, they cannot fully replace humans. Therefore, it is possible to enact appropriate legislation for artificial intelligence without granting it the legal personality inherent to natural persons.

3 Liability of artificial intelligence applications and their implications

The development of intelligent machines is closely intertwined with the law, as the legal system is fundamentally based on protecting the public interest from violations. While artificial intelligence is one of the modern technological fields that has permeated various aspects of life, its role in enhancing service, military, economic, and even political sectors cannot be denied. However, the complete autonomy of artificial intelligence systems from human intervention and their ability to act independently without programming – coupled with their high level of perception – makes them susceptible to civil or criminal liability for their actions.

The replacement of human labour with artificial intelligence does not exempt it from adhering to the legal frameworks governing the local or international communities in

which it operates. Therefore, this study will address both the civil and criminal liability arising from errors caused by artificial intelligence technologies.

3.1 Civil liability for damages arising from artificial intelligence errors and its scope

Civil liability is defined as the obligation of the responsible party to compensate for the damage caused, provided that the elements of such damage are met. This is in accordance with Article 256 of the Jordanian Civil Law No. 43 of 1976, which states: "Any harm caused to others obligates the perpetrator, even if unintentional, to compensate for the damage." Based on this, the researcher can assert that compensation for damages resulting from civil liability is based on personal accountability, stemming from the principle that each individual is responsible for their own actions. Consequently, the study will address the civil liability arising from errors caused by artificial intelligence technologies and the extent to which artificial intelligence systems can be held accountable. To explore whether artificial intelligence technologies can bear liability for harmful actions, the researcher must first examine their legal nature, as this will facilitate the clarification of the basis for their civil liability.

Researchers have briefly discussed the permissibility of granting legal personality to intelligent machines. In this regard, it can be said that the debate and divergence of opinions have been relatively extensive, ranging between opponents and proponents of the idea. The purpose and aim of granting legal personality to artificial intelligence machines lie in providing them with rights that protect them from external infringements and imposing obligations that pave the way for holding them accountable for the damages they cause as a result of their actions.

An example that illustrates this issue occurred in USA in 2022, when a modern technology company faced civil liability after one of its artificial intelligence machines, operating with an autonomous driving system, caused a car accident. During its first trip, the system failed to recognise a red traffic light, leading to a collision with another vehicle and resulting in injuries to the driver and passengers.

The manufacturer of the system justified the incident by stating that the accident was the result of an unexpected technical error in the programming. However, local authorities decided to hold the company civilly liable for the accident. The injured driver and passengers filed a lawsuit against the manufacturer, claiming that the faulty intelligent system was the direct cause of the accident. Therefore, the company had no choice but to bear responsibility for the injuries caused by its intelligent system (Washington, 2022).

In another incident that occurred in (2021) in USA, specifically on Wall Street in New York, an artificial intelligence system was used to analyse data and make automated decisions in the stock market. This system was programmed to make investment decisions based on data analysis and financial forecasts. However, a programming error led to incorrect decisions, resulting in significant financial losses for investors.

A lawsuit was filed against the company responsible for developing the artificial intelligence system, accusing it of negligence in programming the system and failing to adhere to ethical standards and financial regulations. The company was held civilly liable for the financial losses incurred by investors as a result of the system's incorrect actions. Consequently, the company was held accountable for the damage caused by the

intelligent system and was required to compensate investors for their financial losses (Alarbia.net, 2023).

From here, disputes arose regarding the possibility of granting intelligent machines legal personality. Traditional standards of legal personality are insufficient and cannot fulfil the purpose if applied to artificial intelligence technologies. Consequently, it can be said that granting them such personality is highly challenging, as these systems and industrial entities cannot be granted rights that conflict with fundamental freedoms and international charters and treaties concerned with human rights. They cannot be granted rights such as citizenship, dignity, or others. The justification for granting legal personality to legal entities lies in the fact that the latter is subject to the directives of those who represent it, which is not applicable to intelligent machines. Granting them legal personality would inevitably lead to the evasion of responsibility by whoever represents them or is accountable for them in any way for the errors they commit (Wahba, 2020).

In this context, French jurisprudence has concluded that legal personality is granted to the physical entity of a human being regardless of their understanding or perception. Therefore, linking legal personality to legal responsibility is not entirely accurate. Not everyone who is granted legal personality is legally accountable for their actions. A person lacking legal capacity is a prime example of this, as they possess legal personality and independent financial liability but are not civilly responsible for their actions. Instead, their guardian or representative is held accountable in such cases. Applying this concept to intelligent machines, it can be stated that such machines cannot be held civilly liable. Instead, the responsibility for compensating damages lies with the human being behind the machine, who is responsible for its operation (Barak, 2022).

The disagreements among jurists regarding granting legal personality to artificial intelligence applications were not limited to the aforementioned issues. Instead, they were divided into four approaches (Aldweikat, 2022):

First approach: Proponents of this view argued that intelligent machines, despite demonstrating significant capabilities in decision-making and replacing human involvement in many fields, particularly intellectual ones, do not warrant the granting of legal personality. No matter how advanced they become, they will remain classified as ‘objects’ from a legal perspective. Consequently, compensating for damages caused by these technologies should be addressed through the establishment of a mandatory insurance system specifically covering robot-related incidents or through a fund designated to cover such damages in the absence of insurance.

Second approach: Advocates of this approach argued that the actions of intelligent machines are nothing more than tasks delegated to them by their human agents. Therefore, any harm caused by these technologies would be the responsibility of their principal – the human agent. However, this approach faced significant criticism based on the fact that an agency relationship, in principle, can only exist between two legal persons, which is something that artificial intelligence and its applications lack.

Third Approach: This approach opposed the previous ones and leaned towards the possibility of granting legal personality to intelligent machines, but only as moral persons. The independence that these machines possess enables them to carry legal personality. Thus, once the necessary registration procedures are completed, they would

be granted a name, nationality, independent financial liability, and legal capacity, similar to other legal entities.

Fourth Approach: Supporters of this approach took a relatively neutral stance compared to the previous ones. They argued that while intelligent machines have replaced human elements in certain areas, they cannot fully replace humans. Therefore, there is no urgent need to grant them legal personality at this time. However, if these machines continue to evolve and gain further independence, it will be inevitable to grant them legal personality sooner or later.

The researchers believe that the third and fourth approaches are the most reasonable and logical. If artificial intelligence technologies do not exceed their current level of independence, even though they are capable of making decisions on their own, they can only be granted a legal personality of an entity. This is because they have not yet reached the level of human independence. At the same time, it can be argued that if AI continues to evolve and surpass the natural limits of independence to the point of resembling the human mind to the extent that no distinction can be made between the two, granting them legal personality will become inevitable. Consequently, this would eliminate the classification of AI as an object under the law and elevate it to the status of a natural person, not by granting full human rights, but by determining the responsible party for causing harm and compensating for it.

To establish civil liability for the party causing harm, it is necessary to prove both the harmful act, the damage, and the causal relationship between the two. The harmful act consists of two important elements: trespass and intent. Trespass is based on two criteria: the first is the objective criterion, which is formed by negligence or failure to provide the necessary care – care that would be expected from an ordinary person – when committing the act. The second is the subjective criterion, which is the individual's deliberate wrongdoing that infringes upon the rights of others with full awareness and caution (Aljuboori, 2011). As for intent or deliberate harm, it can be described as the intention to cause harm, meaning that the individual's will is directed at intentionally causing harm through their actions. Intent cannot be said to exist if the act causes harm unintentionally. Therefore, researchers argue that intent must be based on the commission of an unlawful act against another person, an act that can only lead to harm, and the individual must be aware and capable of distinguishing the harm they are causing.

Damage is defined as anything that causes harm or disrupts an individual's interest or rights, whether it affects their body, property, or honour (Alzarqa, 1988). Based on this definition, it can be said that damage is divided into physical damage that affects the individual in non-financial interests, financial damage that impacts their financial liability either partially or entirely, and moral or emotional damage that affects their feelings, reputation, honour, or dignity. Civil liability for harm to others can only be established under certain conditions, such as when the damage is real, direct, and affects the legitimate interest of the other party. Responsibility for the damage is only established when these three conditions are met.

As for the causal relationship between the harmful act and the damage, it is considered the connecting link between the committed act and the harm it caused, determining the connection between each of them. Therefore, the absence of this relationship negates the establishment of liability for compensating the damage. Consequently, if it is proven that the damage did not result from the act directed at the

harmful party, the establishment of liability becomes irrelevant, as the absence of the causal link negates their connection.

Based on the above, this responsibility poses a challenge regarding intelligent machines, as they must be subjected to a legal system that can hold them accountable for the damage they cause. This responsibility may fall on those who are responsible for or involved in designing and programming them, considering that these machines are not capable of bearing that responsibility on their own. Because applying traditional responsibility to intelligent machines is highly challenging, there have been some opinions – such as in French jurisprudence – calling for the application of the responsibility for the custody of things to artificial intelligence applications. This is based on the idea that the person responsible for the machine is not only liable for the damage it causes in a personal capacity but also bears the consequences of damage caused by objects under their custody or control (Mowafy, 1992). A custodian is someone who has actual authority over the object, directing and overseeing it. However, researchers argue that it is difficult to apply this theory to artificial intelligence machines because they possess a high degree of autonomy, enabling them to make decisions based on their surroundings without any instruction from their owner. This makes them not subject to the supervision or control of their custodian. Therefore, it is not possible to determine liability based solely on traditional legal provisions, as intelligent machines still present unforeseen challenges due to the conflict between traditional legal texts and practical realities, making it difficult to reconcile the two because of the vast difference in their legal nature.

In terms of international responsibility, two key elements are required for the establishment of traditional international responsibility: the first is the commission of an internationally wrongful act by a state, meaning an act that involves a clear violation of international law, which provides the element of fault (the objective element). The second is the ability of the injured state to prove that the wrongful act by another state or international legal person has violated its rights, which is the personal element based on the damage and causal relationship (Abd Alnabi, 2013).

When considering artificial intelligence and its various, continuously evolving applications that impact the international community due to the potential harms faced by other states, the matter moves beyond traditional responsibility and into a different form of international responsibility. The researcher believes it is important to briefly reference international responsibility based on risk, which disregards fault. This type of responsibility is based on two elements only: damage and causal relationship. It is defined as: “Responsibility that falls on a state due to the harm caused by the use of lawful activities that involve multiple risks, regardless of the state’s negligence, omission, or error. In other words, it is responsibility for the damage caused by hazardous activities without considering fault” (Abu Alwafa, 2004).

The relationship between artificial intelligence and this responsibility shows that, due to the emerging capabilities of smart machines, which will inevitably play a role in influencing economic, security, military, political, and other fields, these machines will serve the interests and objectives of states both domestically and internationally. Consequently, these machines will generate competition, primarily driven by technological companies across all states, which will increase the likelihood of potential harm occurring during this process. Therefore, it can be argued that states are constrained by a limitation that requires them to adopt the principle of good faith in their actions, to

avoid causing harm to other foreign states. Failure to comply with this principle would expose them to sanctions and penalties for breaching it.

3.2 Criminal responsibility arising from artificial intelligence errors and its scope

Intelligent machines and robots can be seen as more than just mechanical devices performing specific tasks; they surpass human capabilities in many aspects and fields, which makes them exceed human potential and go beyond their mechanical role. However, the issue of accountability for their mistakes remains a complex problem, as it can incentivise exemption of those responsible for undesirable actions resulting from these entities. Despite their resemblance to individuals in many ways, they lack the eligibility and intent inherent in humans, which makes them not subject to legal accountability in the same manner as individuals. Given that artificial intelligence has not been granted the personality that would enable it to bear obligations, including legal responsibility, it can be said that these machines are incapable of distinguishing in many cases, especially if used in military contexts. It is difficult to differentiate between civilians and military personnel since they are merely machines performing tasks based on the programming and information they have been fed. While they surpass human abilities in many areas of life, they are, ultimately, not equivalent to a complete human being.

Since criminal responsibility consists of the obligation to bear legal consequences resulting from the commission of acts prohibited by law, it can be said that it requires the presence of two elements: one is factual, represented by the criminal act, and the other is mental, represented by the general intent in the crime, which consists of knowledge and awareness. Therefore, there can be no criminal responsibility arising from the act alone without the presence of intention or awareness during its commission. In other words, if the criminal intent is absent, criminal responsibility for the act is also absent.

Criminal responsibility is characterised by being personal, meaning it does not extend to others. In other words, the essence of criminal responsibility lies in holding accountable the person who committed the unlawful act. It is unreasonable to hold someone else accountable for an act they did not commit. Furthermore, the determination of this responsibility requires the presence of criminal capacity, including awareness and intention to commit the criminal behaviour. If that intention or awareness is absent, the responsibility is incomplete, similar to the actions of a minor who lacks discernment. If their mental faculties are absent, they are not held responsible (Almala, 2021).

Applying all the above to artificial intelligence machines, strong opposing and supporting trends have emerged regarding the imposition of criminal responsibility on these machines. Researchers believe that determining this responsibility requires an individual to be free and aware of the criminal behaviours they are committing in order to be held criminally accountable. Therefore, it is impossible to direct blame toward something that is not considered human, as it lacks the capacity to bear responsibility under the laws and regulations designed for this purpose (Shams Aldein, 2012). This view generally aligns with the opposing stance on attributing criminal responsibility to artificial intelligence applications, as seen in Arab and French legislation (Pardel, 2016). Due to the lack of criminal capacity and the inability of artificial intelligence to perceive or choose, it can be said that the possibility of imposing criminal responsibility on these machines is non-existent. This is because the basic conditions required for someone to

bear responsibility are absent, and thus, the path to subjecting smart machines to criminal responsibility remains blocked. While these machines may demonstrate a significant degree of autonomy, they cannot replace the essential conditions that are required in humans.

As for the supporting side for the establishment of criminal responsibility on artificial intelligence applications, they argue that the tremendous development of these machines, which constitute what is called artificial cognition, obligates legislation to initially recognise their legal personality. Following that, the stage of determining whether criminal responsibility should be imposed for their actions arises. This is based on the idea that legal personality is granted to open the path for assuming obligations and rights and is not tied to human characteristics. Therefore, criminal responsibility cannot be established without legal personality (Bin Tarya and Shahida, 2018). The purpose of establishing a legal personality is the pressing need for it, noting that a legal person was not initially granted such a personality. However, the urgent need to grant it became essential, especially due to the growing role of these entities in local and international communities. This eventually led to granting them a certain degree of legal personality and criminal responsibility, by their nature.

One of the main arguments put forth by the proponents of this principle is the possibility of replacing artificial intelligence with artificial cognition, which is based on complete autonomy that grants it a form of awareness in decision-making, independent of its creators (Barak, 2022). This means that the machine makes decisions on its own, based on the nature of the situation it encounters or its surrounding environment, using a new way of thinking that relies on data and information, rather than solely relying on what is stored in its pre-programmed software (Masoud et al., 2023). Therefore, it can be said that this advancement in smart machines will inevitably lead to criminal acts, whether intentionally or by mistake. This is evident in the ongoing Russian-Ukrainian conflict, where the use of autonomous weapons, drones, and lethal robots, which possess enough independence to identify and attack targets without any human intervention, has been prominent. This conflict has essentially become a tragic testing ground for various forms of smart weaponry.

Accordingly, it can be said that, at present, criminal responsibility can be attributed to one of these parties regarding the applications of artificial intelligence and its actions:

3.2.1 First: responsibility of the artificial intelligence manufacturer

AI manufacturers are held accountable for any harm caused by their products, whether due to negligence, design flaws, or misuse as one crucial aspect of product safety. Therefore, the responsibility of the artificial intelligence manufacturer is considered one of the first issues raised when these machines engage in actions or behaviours that cause harm to others. In order for the manufacturer to remain within the safety zone, avoiding any legal responsibility, he must adhere to certain standards when designing and launching the smart machine. This includes compliance with the laws and regulations of the manufacturing state in this regard, ensuring that no laws are violated in the design of the machine and that safety rules are not neglected. If the manufacturer fails to take the necessary precautions to prevent the artificial intelligence machine from causing significant harm, he exposes himself to legal accountability for the negligence shown in that regard (Dahshan, 2020).

This incident serves as an example of this. In 2016, in USA, a self-driving car collided with another vehicle, resulting in the death of the driver and injuries to the passengers in the other vehicle. As a result, the manufacturer of the artificial intelligence system in the car was held criminally responsible because the accident occurred due to a malfunction in the intelligent system that managed the car. The manufacturer failed to take the necessary measures to ensure the safety of the system and prevent similar accidents. It is also worth noting that any manipulation of the car's data by the manufacturer or any violation of the laws and regulations governing the manufacturing of self-driving cars exposed him to the same liability due to his intentional or negligent failure to perform his duty.

Crimes such as violations of personal data and cybercrimes that are carried out through artificial intelligence devices specifically designed for these purposes are common offenses that expose their manufacturers to the responsibility resulting from these illegal acts. These include cyberattacks, hacking, electronic fraud, and other actions that undoubtedly constitute criminal acts based on the manufacturing and design of the perpetrators.

Therefore, it is possible to say that the implementation of AI mechanisms in the field of cybersecurity and surveillance AI application could pave the way for new cyberattacks and threats in the face of national security, based on the vulnerability inherent in the nature of the data feeding into it. Whether that data is flawed or biased, it could lead AI systems to make incorrect decisions, opening up gaps that attackers could exploit, especially those based on distorted or unreliable data. These systems may become vulnerable to hacking, manipulation of security systems, or even the distortion of sensitive data. Moreover, attackers could develop more advanced AI tools to create new capabilities, allowing them to analyse patterns or predict security measures to bypass them (Osoba and Welser, 2017).

In this regard, the USA Intelligence Agency has expressed concern that an AI system was potentially breached during the 2016 USA election cycle by an external party, where cyberattacks could have leaked sensitive information that might have impacted voter behaviour in that election. Although the origin of the attack could be traced if the right environment was available, the use of more efficient and advanced systems by the attackers could weaken the detection process of the attacking entity (Paletta, 2016).

As the USA also pointed out in a report it issued in 2021 about cybersecurity, that engaging legislative and regulatory bodies is essential for shaping effective cybersecurity policies, while integrating cybersecurity into organisational risk management ensures a proactive approach to threats. Bridging the gap between physical security and cybersecurity strengthens overall defence mechanisms, enhancing cyber resilience across all levels. Developing regulatory frameworks for compliance and accountability, alongside leveraging oversight mechanisms, fosters stronger governance and enforcement. A robust cybersecurity culture must be instilled from leadership downward, adopting a holistic, organisation-wide strategy that positions the workforce as the first line of defence. Optimising resource allocation and investing in specialised cybersecurity professionals are critical to sustaining long-term resilience. By taking these measures, organisations can anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises affecting cyber-enabled systems (United Nations, 2021).

3.2.2 Second: responsibility of the artificial intelligence programmer

The question of AI accountability remains legally complex, particularly regarding the role of programmers and manufacturers, that's why when applying the concept of granting artificial intelligence machines legal personality, making it possible to hold them accountable for their actions, it becomes evident that practical accountability remains unfeasible due to the absence of awareness and intent in these machines, despite them operating based on the software or designs of their manufacturers. Given their ability to make independent decisions, it has been proposed that at least the manufacturing companies bear responsibility for the civil losses and damages resulting from their errors and actions (United Nations General Assembly Resolution, 2013). After a thorough investigation, it is clear that no national or international law has been put in place to define the responsibility of artificial intelligence so far. In cases of non-deliberate negligence, it is challenging to hold manufacturers or programmers accountable, as manufacturers often point to the potential for accidental errors by robots, which absolves them completely from any responsibility for these mistakes (Alfalasi, 2021). It can be said that manufacturers and programmers of artificial intelligence machines take advantage of this situation to avoid bearing any responsibilities regarding the performance of these machines. This behaviour suggests that robots enjoy a high degree of independence, which helps in avoiding legal accountability. While the programmers and manufacturers of these machines are not a single entity, researchers believe the most suitable policy for holding them accountable is to divide responsibilities and implement laws that criminalise evading accountability comprehensively.

In this regard, the case of Sandra Saltzer (2024) which happened in UK is a great example, a lawsuit was filed against Intuitive Surgical, the manufacturer of the da Vinci system, following the death of 78-year-old Sandra Saltzer. During a surgical procedure, the robot allegedly caused a perforation in her small intestine, leading to a fatal internal leak. The lawsuit claims that the malfunction of the robot directly resulted in her death. Various reports have highlighted instances where patients experienced severe complications post-surgery involving the da Vinci system. These complications have sometimes led to legal actions against healthcare providers and the manufacturer, focusing on issues like inadequate training, device malfunctions, and insufficient disclosure of potential risks, and ethical challenges, questioning the institutional oversight and the manufacturer accountability and it's obligations to provide reliable equipments associated with the device held accountable (Almashad, 2024).

3.2.3 Third: responsibility of the user of artificial intelligence

The types of artificial intelligence devices vary depending on their uses, and it can be said that when linking artificial intelligence applications to their users, smart weapons serve as a prime example for explaining the responsibility of those who use these machines. It is reasonable to consider a military leader responsible for the actions of artificial intelligence entities if they deploy smart weapons with the intent to commit a crime. These machines are capable of committing war crimes, distinct from ordinary crimes. However, military leaders may attempt to avoid responsibility by claiming that the incident was an unforeseen mistake or an error made by the artificial intelligence machine. Therefore, it is just that the military leader using robots as weapons be prosecuted in the same manner as they would be if they issued orders violating

international humanitarian law. The execution of these unlawful decisions leads to the same outcome: exceeding the provisions of the law of war and violating its rules (Mekki, 2017).

3.2.4 Fourth: responsibility of the state using artificial intelligence

The responsibility for artificial intelligence machines lies with the state that manufactures them, similar to the case with aircraft and ships, with the notable difference being these machines' characteristics. It should be noted that holding the state legally responsible for the actions of artificial intelligence usually exempts the programmer and user from responsibility unless the machines are used by non-governmental entities. However, it cannot be said that there are no concerns regarding the use of robots and their independence in decision-making, which makes it difficult to define the legal framework for criminal responsibility for unlawful actions and compensation for damages resulting from the use of these entities (Harqous, 2018).

4 Conclusion

At the completion of this study, the importance of developing artificial intelligence technologies while considering ethical values and respecting international law and human rights cannot be denied. It is essential to attempt to govern artificial intelligence technologies based on the principles of international law and international humanitarian law, which should be part of national and international policies for their regulation. The way forward involves unifying the international community around guiding principles for organising artificial intelligence technologies, when necessary, by establishing technical committees that include independent experts, scientists, and representatives from companies and institutions involved in artificial intelligence. Manufacturers and innovators also have the responsibility to consider the social and security implications of their technologies, ensuring that new technologies contribute to creating a safe and stable society for all, free from any disruption to international peace and security.

Therefore, the study concluded with a set of findings and recommendations:

5 Findings

- The lack of a comprehensive, conclusive, and inclusive definition of the concept of 'artificial intelligence systems' could lead to varying interpretations and understandings of this concept by scholars and legislators, due to the differences and expansion in the fields of artificial intelligence, thus resulting in varied definitions according to its different domains.
- Criminal responsibility is limited to individuals only and cannot be attributed to an artificial entity; hence, there is no possibility of punishing it, as criminal responsibility is exclusive to humans.
- Scholars have disagreed on granting legal personality to artificial intelligence machines, with both supporters and opponents presenting their arguments. However, there is still no consensus on whether artificial intelligence should be granted legal

personality, as it lacks some of the conditions stipulated by traditional legal rules, making it difficult to easily grant it such a personality.

- Granting legal personality to artificial intelligence applications is not sufficient to resolve the issue of criminal or civil liability, as artificial intelligence remains a machine operated based on pre-stored data.
- The international community is still working on creating an integrated system to regulate artificial intelligence according to the rules and guidelines of international laws and covenants, as there is no avoiding the impact of artificial intelligence developments on societies in various forms.
- The current international community is in a state of balance regarding AI organisations, especially in the effort to establish an international society based in security and global peace without any disruption.

6 Recommendations

- The need to introduce penalties for robots that cause harm or crimes, by either destroying the responsible robot or preventing it from functioning under the threat of punishment for those who violate this, and not only imposing fines or compensation on the person who controls the smart machine. This would serve as a deterrent to prevent machines from causing various harm locally and internationally.
- The need to establish rules and regulations that obligate the manufacturers of artificial intelligence machines to follow, and to specify their liability and penalties for violations of those rules. This is to ensure compliance with safety standards, regulations, and safety protocols during the development of artificial intelligence machines, making it clear that manufacturers cannot escape responsibility for damages caused by their mistakes.
- A call for the international community to increase its efforts to keep pace with artificial intelligence developments at the same pace, to enhance the preservation of international peace and security from being affected.
- The need to establish a set of local and international ethical standards that govern the manufacturing of artificial intelligence machines, and determine their specifications and guidelines, to reduce unethical manufacturing violations, which will inevitably lead to varying degrees of harm.
- The need to legislate new local laws that are tailored to the nature of artificial intelligence applications, to facilitate defining the rules of civil and criminal liability resulting from errors made by artificial intelligence machines.
- The need to decisively address the issue of legal personality for smart machines, to free oneself from the uncertainties about whether or not they should be granted such a personality, thus clarifying the standards for liability arising from artificial intelligence errors, making it easier to apply.

Conflicts of interest

All authors declare that they have no conflicts of interest.

References

- Abd Alnabi, E. (2013) *International Liability for Damages Resulting From Non-Prohibited Acts by International Law (International Liability and Objectivity)*, Unpublished Doctoral Thesis, Menofia University, Egypt.
- Abd Alsattar, M. (2012) 'The legal liability related to artificial intelligence', *Journal of Law and Political Sciences*, Vol. 10, No. 2.
- Abu Alwafa, M. (2004) *The Intermediary in Public International Law*. 1st ed., Al-Nahda Al-Arabia for Publishing and Distribution, Egypt.
- Alarbia. net (2023) *Artificial Intelligence Flips the Table on Wall Street*, Retrieved from <https://www.alarabiya.net/>
- Aldweikat, N. (2022) 'Tort liability for damages of artificial intelligence robots in the Jordanian civil law', *Al-Zaytoonah University of Jordan Journal for Legal Studies*, Vol. 3, No. 3, pp.232–252.
- Alfalasi, A. (2021) 'Criminal liability arising from artificial intelligence errors', *Legal Studies*, Vol. 9, No. 8, pp.2838–2900.
- Alfaqi, A. (2012) *Artificial Intelligence and Expert Systems*. 1st ed., Dar Al-Thaqafa for Publishing and Distribution, Jordan.
- Ali, K. (2022) 'Artificial intelligence legal framework', *Jil Journal of Legal Depth Research*, Vol. 54, pp.53–66.
- Aljuboori, Y. (2011) *The Concise Explanation of Jordanian Civil Law*, 3rd ed., Dar Al-Thaqafa for Publishing and Distribution, Jordan.
- Almala, M. (2021) 'The historical dimensions of the development of criminal liability theory and the dialectic of its application in the era of artificial intelligence: an analytical and prospective study', *Kuwait International Law School Journal*, Vol. 8, No. 1, pp.83–132.
- Alrai, A.F. (2023) 'Investigating and inferring crimes through artificial intelligence systems', *Al-Zaytoonah University of Jordan Journal for Legal Studies*, Vol. 4, No. 1, pp.156–175.
- Alzarqa, M. (1988) *Liability for Harm and Warranty in It: A Legal Study and Formulation Based on Islamic Jurisprudence Texts in Accordance with the Provisions of the Jordanian Civil Law*, 1st ed., Dar Al-Qalam for Publishing and Distribution, Syria.
- Badri, J. (2022) 'Artificial intelligence: a legal approach to research', *The Journal of Algerian Legal and Political Sciences*, Vol. 59, No. 4, pp.173–190.
- Barak, A. (2022) *Towards the Legal Regulation of Liability Rules for Artificial Intelligence Technologies*, 1st ed., Dar Wael for Publishing and Distribution, Jordan.
- Barqawi, L. (2023) 'The impact of using artificial intelligence in pharmaceutical companies', *Al-Zaytoonah University of Jordan Journal for Legal Studies*, Vol. 4, No. 1, pp.217–236.
- Bin Tarya, M. and Shahida, K. (2018) 'Damages caused by robots and artificial intelligence technologies: a new challenge to current civil liability law', *University of Algeria Annals Journal*, Special Issue, pp.119–142.
- Dahshan, Y. (2020) 'Criminal liability of artificial intelligence crimes', *Journal of Sharia and Law*, Vol. 82, No. 82, pp.101–144.
- European Union (2016) *General Data Protection Regulation*, Retrieved from <https://data.consilium.europa.eu/>
- Fanouchi, F. and Conoli, K. (2023) *What is the Law of Artificial Intelligence and the Council of Europe Convention*, Retrieved from <https://www.stopkillerrobots.org/>

- Harqous, H. (2018) *About a Soulless War Where Robots Can Kill You*, Retrieved from <https://www.mohe.gov.jo/>
- Ibrahim, M. (2022) 'The legislative regulation of artificial intelligence applications', *Legal and Economic Research*, Vol. 12, No. 81, pp.1025–1137.
- Masoud, M., Jaradat, Y., Rababa, E. and Manasrah, A. (2021) 'Turnover prediction using machine learning: empirical study', *International Journal of Advances in Soft Computing and Its Applications*, Vol. 13, No. 1, pp.194–207.
- Masoud, M.Z., Manasrah, A., Jaradat, Y. and Shaban, N.A.A. (2023) 'How data can mislead machine learning prediction process: case study of building cooling and heating loads', *2023 International Conference on Information Technology (ICIT)*, August, IEEE, pp.709–714.
- Mekki, O. (2017) *International Humanitarian Law in International Armed Conflicts*, International Committee of the Red Cross.
- Mohammad, A. (2021) 'The legal framework for smart robots equipped with artificial intelligence technology (United Arab Emirates as a model), analytical comparative study of the civil law regulations for robots issued by the European union in 2017 and the Korean ethical charter for robots', *Legal and Economic Research*, Vol. 7, No. 2, pp.1–130.
- Mowafy, Y. (1992) 'Liability for objects in light of jurisprudence and judiciary: a comparative study, 1st ed., Mansha'at Al-Ma'arif for Publishing and Distribution, Egypt.
- Osoba, O. and Welser, W. (2017) *The Risks of Artificial Intelligence to Security and the Future of Work*, Rand Corporation. Retrieved From <https://www.rand.org/pubs/perspectives/PE237.html>
- Paletta, D. (2016) 'U.S. blames Russia for recent hacks; intelligence agencies believe hacks are meant to 'Interfere with the U.S. election process'', *Wall Street Journal*, Retrieved from <http://www.wsj.com/articles/u-s-blames-russia-for-recent-hacks-1475870371>
- Pardel, J. (2016) *Droit pénal comparé (4e édition)*. Agrégé des Facultés de droit Professeur émérite de l'Université de Poitiers Membre titulaire de l'Académie internationale de droit compar.
- Shams Aldein, A. (2012) *Legal Formulation of Criminal Procedure Law*, 2nd ed., Al-Nahda Al-Al-Arabia for Publishing and Distribution, Egypt.
- UNESCO (2019) *The Preliminary Study of the Technical and Legal Aspects Related to the Adequacy of Establishing a Regulatory Document on the Ethics of Artificial Intelligence*, p.206.
- United Nations (2021) *Cybersecurity in the United Nations System Organizations*, Retrieved from https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf
- United Nations (2021) *The Risks of Artificial Intelligence That Threaten Privacy*, Retrieved from <https://www.ohchr.org/>
- United Nations Economic and Social Commission for Western Asia (ESCWA) (2020) *Developing a Strategy for Artificial Intelligence, a National Guide*, Retrieved from <https://archive.unescwa.org/file/110400/download?token=r8bYBIra>
- United Nations General Assembly Resolution (2013) 'Promoting and protecting all human rights, the specific mandate concerning cases of extrajudicial, summary or arbitrary executions', *Universal Human Rights Index*, Vol. 23, No. 3, pp.1–28.
- Wahba, A. (2020) 'Civil liability of damages caused by artificial intelligence: an analytical study', *Jil Journal of Legal Depth Research*, Vol. 43, pp.11–45.
- Washington, A.F.P. (2022) *Tesla Facing a Lawsuit Related to the Self-Driving Capabilities of It's Vehicles*, Retrieved from <https://www.emaratayoum.com/>