Artificial Intelligence and Combating Cybercrime: Technical Opportunities and Legal Challenges

الذكاء الاصطناعي ومكافحة الجريمة الإلكترونية: فرص تقنية وتحديات قانونية

Amina BOUTALEB *
Faculty of Law and Political Sciences, University of Bejaia, Algeria
amina.boutaleb@univ-bejaia.dz

Date of send:29/09/2025 **Date of acceptance**:21/11/2025 **Date of publication** ;11/06/2026

Abstract:

Cybercrimes currently pose a direct threat to the security and safety of individuals, institutions, and states. The open nature of cyberspace has facilitated the escalation of cybercriminal activities both in scale and complexity, including system intrusions, money laundering, data theft, cyberterrorism, as well as threats and extortion through electronic means, among other serious crimes that take cyberspace as their arena. This situation necessitates advanced mechanisms to confront such threats. Among modern technologies, artificial intelligence emerges as an effective tool in combating cybercrime due to its highly advanced technical capabilities in big data analysis, threat prediction, detection of suspicious activities, and accurate identification of the sources of cyberattacks.

However, the use of artificial intelligence in the fields of investigation and surveillance raises numerous legal challenges related to privacy violations, the legitimacy of algorithmically obtained evidence, and issues of criminal liability. These challenges call for precise legal frameworks that balance the requirements of cybersecurity with the protection of rights and freedoms.

Keywords: Artificial intelligence. cybercrime. cybercriminal. Legal.Challenges.

* ***Corresponding author***

Introduction

In light of the remarkable technological progress witnessed worldwide today, artificial intelligence has permeated various fields, particularly that of cybersecurity, which has recently experienced a surge in cybercrimes and electronic threats. Consequently, there has arisen an urgent need to adopt more advanced and effective technical mechanisms to counter this form of crime, characterized by its dynamic nature, complexity, and difficulty of traceability. Among such technologies, artificial intelligence stands out for its immense technical capabilities, including the analysis of big data, threat prediction, monitoring and detecting suspicious activities, as well as accurately identifying the sources of cyberattacks. However, the deployment of artificial intelligence in combating cybercrime raises numerous legal challenges, particularly regarding the protection of individual freedoms and privacy, the legitimacy of evidence obtained through algorithms, and the difficulty of determining criminal liability for acts or decisions made by intelligent systems. These challenges necessitate the establishment of precise legal frameworks that strike a balance between the imperatives of cybersecurity and the safeguarding of rights and freedoms.

The importance of this study lies in shedding light on a dual-faceted topic that intertwines the technical and legal dimensions. It emphasizes the necessity of keeping pace with digital transformations by establishing legal frameworks that balance technical efficiency with legal safeguards.

In general, the study aims to assess the effectiveness of artificial intelligence, as a technological application, in confronting cybercrime, while also identifying the key legal challenges associated with its use in combating this type of crime. This will be explored through the following points:

- ✓ Identifying the concept of artificial intelligence and cybercrime.
- ✓ Examining the role of artificial intelligence in addressing cybercrime.
- ✓ Highlighting the main legal challenges that hinder the fight against cybercrime through artificial intelligence.

To examine the subject in depth, the following central research problem is posed: Is artificial intelligence an effective tool for combating cybercrime, and what legal challenges does its use in this field raise?.

To answer this research problem, the study adopts a descriptive method, suitable for outlining legal concepts and realities, as well as an analytical method for examining the legal provisions relevant to this topic.

Firstly: The Conceptual Framework of Artificial Intelligence and Cybercrime

Artificial intelligence (AI) is closely related to cybercrime, particularly in its reliance on computers and digital environments. AI applications are often employed in committing or advancing cybercrimes, but conversely, they can also be harnessed to combat them. To highlight the strong link between the two, it is first necessary to define the conceptual framework of both artificial intelligence and cybercrime.

1. The Conceptual Framework of Artificial Intelligence

Artificial intelligence addresses the intellect, as it is one of the most prominent modern technologies simulating human thought through its ability to reason. This can be clarified by examining the emergence and development of AI, its definition, importance, and key characteristics.

1.1 Emergence and Development of Artificial Intelligence

The term artificial intelligence first appeared in the 1950s, specifically in 1956, at Dartmouth College in Hanover, United States, during a summer research workshop led by four American scholars: John McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude Shannon. At that time, AI was defined as the science and engineering of making intelligent machines. Since then, its historical trajectory has been marked by alternating phases of growth and decline until it witnessed significant flourishing during the early decades of the 21st century. The advancement of computing power and communication technologies has greatly contributed to the progress of artificial intelligence technologies[1].

1.2 The Concept of Artificial Intelligence

Although AI currently dominates technological innovation, there is no universally agreed-upon definition of the concept. AI is more a broad field of study than a term that can be easily defined, and definitions often vary depending on the discipline in which it is studied[2].

- **Definition of AI:**

AI has been defined as "the manner in which a computer becomes capable of intelligent thought."[3] Another definition states: "Artificial intelligence is the field of computer science concerned with systems that exhibit characteristics associated with human intelligence, with the ability to make decisions in a manner similar to human behavior in various domains. AI systems aim to develop computers to perform tasks requiring human intelligence by enabling machines to replicate human cognitive activities in practice."[4]

From this perspective, AI consists of designing automated systems that allow computers to mimic human reasoning, with nearly equivalent capacities, either through self-learning or by being fed with vast amounts of data[5]. Based on the above, AI does not have a single unified definition: some scholars emphasize its objectives, others liken it to the human mind, but all agree on the ability of machines to act like humans.

In the Algerian legal system, and particularly in the regulation of electronic transactions, no explicit definition or recognition of artificial intelligence and its applications has yet been introduced.

- **Characteristics of Artificial Intelligence**

AI has distinctive characteristics that differentiate it both from human intelligence and from traditional software. These include its advanced predictive, analytical, and adaptive capabilities, making it an essential tool in combating cybercrime. The most notable features include:

✓ **Predictive capacity:** One of AI's most prominent traits across various fields is prediction, particularly the prediction of crimes. By mining and analyzing past and present data, AI systems can generate forecasts about future outcomes using machine learning or deep learning algorithms. In this way, AI can anticipate criminal events[6], predict high-risk areas, and even forecast the occurrence of cybercrimes, given that both crimes and AI share the same complex digital environment.

✓ **Reasoning and problem-solving abilities:** AI systems possess a high capacity for reasoning and problem-solving, providing immediate and effective solutions without human supervision or intervention, thanks to the vast amount of data stored in their memory[7].

✓ **Data storage, analysis, and autonomous execution:** AI applications rely on extensive memory reserves to store vast amounts of information. This allows them to learn, analyze, and execute processes independently, equipping them to provide adequate solutions to encountered problems[8].

✓ **Learning and adaptation:** Learning is a defining characteristic of intelligent systems. AI applications employ unique learning strategies that surpass human capacity[9], not only enabling them to learn but also to improve, refine, and reuse acquired knowledge to address new challenges.

1.3 The Algerian Legislator's Position on Artificial Intelligence

In practice, the Algerian legislator has not explicitly addressed artificial intelligence or its applications in legal regulations, including those related to electronic transactions. However, implicit recognition of AI can be inferred from certain references. For instance, Law No. 18-05[10] on electronic commerce allows reliance on modern technologies, including intelligent software, for electronic contracting. Additionally, Presidential Decree No. 21-323 established the National Higher School of Artificial Intelligence[11], a scientific advisory body tasked with developing AI applications across various fields.

2. The Conceptual Framework of Cybercrime

Technological advancements have impacted numerous domains, offering services and conveniences to humanity. However, cyberspace has simultaneously become a stage for criminal activity. Criminals exploit the digital environment to execute illicit schemes, leveraging its unique characteristics, particularly the difficulty of detection and traceability. This distinctiveness defines cybercrime, which can be explored through the following points:

2.1 Definition of Cybercrime

The definition of cybercrime has been subject to considerable debate among scholars. Some adopt a narrow perspective, defining it as "an unlawful act involving the use of a computer," or "various forms of criminal conduct committed through automated data processing."[12] This restrictive approach identifies cybercrime solely by the tool used: the computer.

Proponents of a broader approach define cybercrime as "any deliberate act or omission arising from the unlawful use of information technology, aimed at

infringing upon tangible or intangible property"[13] Another definition describes it as "an act or omission carried out by a person to harm computer components or communication networks, protected by criminal law, with penalties prescribed for such violations."[14]

The U.S. Office of Technology Assessment also supports this broader approach, defining cybercrime as "a crime in which computer data and software play a central role"[15] Thus, the broader perspective does not confine cybercrime to its technical tools but encompasses any unlawful use of information technologies, extending to its digital environment and associated mechanisms.

2.2 The Algerian Legislator's Position on Cybercrime

The Algerian legislator has not explicitly defined cybercrime but uses the term "crimes related to information and communication technologies" in Law No. 09-04 on special rules for preventing and combating such crimes. Article 2 of this law defines them as "offenses against automated data processing systems as defined in the Penal Code, and any other crime committed or facilitated by an information system or electronic communications network."[16]

Accordingly, Algerian law recognizes both the intangible components of information systems as crime targets and the use of electronic communication as a means of committing offenses. The Penal Code was amended by Law No. 04-15 of November 10, 2004[17], to criminalize "attacks on automated data processing systems" under Articles 394 and 394 bis 1–7.

Furthermore, Law No. 18-05 on electronic commerce addresses cybercrimes in Chapter II, Section III (Crimes and Penalties), specifically in Articles 37 to 48.

Thus, Algerian law approaches cybercrime from two angles: the **subject matter** (attacks on data processing systems) and the **means of commission** (electronic communication or information systems). Importantly, it extends beyond attacks on systems to encompass even traditional crimes when committed through electronic means.

2.3 Characteristics of Cybercrime

Cybercrime is a product of the digital age, granting it particular traits that differentiate it from traditional crimes:

✓ **Dependence on computers and technical expertise:** Computers are both the main tool and target of cybercrimes, involving acts such as destruction, theft, tampering, or manipulation of software and stored data. Cybercrime also demands technical proficiency in computing and information systems, whether for committing or investigating the crime. Investigators may even unintentionally destroy digital evidence due to its fragility[18].

✓ **Transnational nature:** Cyberspace transcends geographical boundaries, allowing offenders and victims to be located in different countries and involving multiple parties. This raises issues of jurisdiction, applicable law, and prosecution procedures, common to all transnational crimes[19].

✓ **Difficulty of detection and proof:** Because cybercrimes occur in an intangible, virtual space, they are inherently difficult to uncover and investigate. Offenders often possess advanced technical skills, making them more elusive compared to traditional criminals.

✓ **Nonviolent nature:** Unlike traditional crimes typically associated with physical force (e.g., assault, theft), cybercrimes rely on intellectual and technical skills, consisting of the alteration or deletion of digital data. Nonetheless, some institutions, such as the FBI, liken them to violent crimes due to the similarity of offenders' motivations[20].

✓ **Insufficient international cooperation[21]:** Despite their transnational nature, cybercrimes lack adequate international legal frameworks and cooperation, complicating efforts to trace, investigate, and prosecute offenders across jurisdictions.

2.4 Types of Cybercrimes

Although classifications vary depending on legal and technological contexts, the most recognized types include[22]:

✓ **Crimes against information systems:** Targeting data integrity and confidentiality, such as illegal access and data destruction.

✓ **Crimes against property:** Including online fraud, money laundering, cryptocurrency theft, and offenses related to electronic payment cards.

✓ **Crimes against individuals:** Such as identity theft, online grooming, defamation, cyber harassment, and violations of privacy.

✓ **Crimes against state security:**

- **Cyberterrorism:** Using electronic communication to spread extremist ideologies, organize, and promote terrorist activities.
- **Cyber espionage:** Involving individuals or groups spying on a state by accessing confidential data, often targeting sensitive sectors such as politics, defense, or industry.

Secondly: The Role of Artificial Intelligence in Combating Cybercrime

Cybercrime is intrinsically linked to artificial intelligence, as both belong to the same digital environment, which is often characterized by ambiguity and complexity. Modern technologies, including AI, can act as a double-edged sword: while criminals exploit AI in cyberspace to execute their schemes and commit offenses, AI can also serve as an effective tool in combating this specific type of crime. Thanks to its immense technical capabilities, AI can detect, trace, and neutralize criminal activity through advanced methods applied across various domains.

1. The Role of Artificial Intelligence in Investigating and Preventing Cybercrime

AI assists digital police forces in the field of digital forensics, expediting the identification of cyber-offenders through their private messages, phone numbers, or other identifiers, while uncovering digital evidence and analyzing criminals' data to place them under surveillance. This enables highly accurate predictions regarding the time and place of potential future crimes, allowing law enforcement units to be

alerted in advance to prevent criminal activity, Advanced countries also employ technologies such as brain fingerprinting, which scans the suspect's brain before interrogation to determine whether they possess knowledge related to a specific crime. This method prevents criminals from lying or resorting to deceitful techniques to avoid responsibility[23], AI further contributes to digital forensics by facilitating the uploading of digital files for use by judicial authorities. An essential step in this process is the activation of digital identities, which enable more effective crime detection and perpetrator identification, simplifying analysis and reducing the time required to resolve cases. Investigations cover any type of computing device, including desktops, laptops, tablets, smartphones, digital cameras, networking equipment, and data storage devices[24], Accordingly, the integration of AI into police systems represents a significant step forward in equipping law enforcement agencies to confront modern forms of cybercrime, potentially preventing crimes before they occur.

2. The Role of Artificial Intelligence in Combating Financial Cybercrimes

AI plays a crucial role in addressing financial crimes targeting assets by employing encryption systems designed to prevent eavesdropping on data transmitted over networks. These systems secure information by converting it into unintelligible codes, thus protecting it from unauthorized access. Encryption techniques include digital fingerprints, electronic signatures, and password protections. Any attempt to tamper with encrypted data triggers alerts, allowing companies and financial institutions to detect criminal activities in time to take necessary preventive measures, Moreover, AI strengthens electronic protection systems by eliminating unnecessary files, ensuring the absence of spyware, and monitoring for malicious intrusions, thereby reinforcing the security of financial transactions and assets[25].

3. The Role of Artificial Intelligence in Combating Cyberterrorism

Cyberterrorism is among the most dangerous emerging crimes, prompting states to dedicate significant resources to combating it. Most preventive strategies focus on thwarting attacks before they occur, making predictive capabilities particularly vital, AI contributes to this effort by analyzing vast amounts of data to identify suspicious patterns and behaviors indicative of potential terrorist activity. Machine learning algorithms enhance this capacity by predicting the location and timing of terrorist attacks while tracking extremist activities through facial recognition technologies and image analysis to identify perpetrators or individuals prone to radicalization, AI also monitors websites and social media platforms containing extremist content[26], such as posts promoting terrorist ideologies or encouraging the adoption of radical beliefs. This surveillance facilitates swift intervention by security authorities, enabling them to shut down suspicious pages and websites and to pursue those responsible for disseminating extremist propaganda.

Thirdly: **Legal Challenges Arising from the Use of Artificial Intelligence in Combating Cybercrime**

Despite the technical efficiency offered by artificial intelligence in addressing various forms of cybercrime, its practical adoption—particularly in Algeria—still raises numerous questions and presents several legal challenges, including the following:

1. The Absence of a Legislative Framework Governing the Use of Artificial Intelligence

The integration of AI into different areas of life, especially in combating cybercrime, directly impacts the legal system. This raises debates concerning the extent to which existing legal frameworks regulate such emerging technologies, and whether legislation is comprehensive enough to encompass them[27]. Unfortunately, most legal systems—including Algerian law—still lack explicit provisions governing the use of AI in the criminal justice field, For instance, Algerian criminal law, including the Code of Criminal Procedure, contains no provisions addressing tools based on machine learning, big data analytics, or algorithms. Even the recently enacted laws related to the digital environment, such as those concerning the prevention of ICT-related crimes and electronic commerce, have proven insufficient to deal with AI systems. The absence of a clear legislative framework thus creates legal loopholes that can be exploited, as is widely recognized.

2. The Problem of Criminal Liability for AI Actions

Advanced programming has endowed AI-driven machines with the ability to develop a degree of autonomy, enabling them to make independent decisions in response to specific circumstances, similar to human behavior. When such applications are employed in combating cybercrime, a major issue arises: Who bears criminal liability for the actions and decisions made by AI systems, particularly in the absence of legal codification defining the scope and nature of such liability?

Under Algerian law, criminal liability is defined by the principle of legality, as enshrined in Article 1 of the Penal Code: “There is no crime, penalty, or security measure without a law.” Moreover, criminal responsibility requires both the material element and the mental element, While the material element may be established through an AI system’s actions, the mental element is inconceivable, as AI lacks legal personality and cannot form intent to commit a crime, Some scholars propose treating AI as a legal person, akin to corporations, which are recognized as juridical persons under the law. On this basis, AI systems could be granted certain constitutional rights similar to those enjoyed by corporations. The rationale is that, as AI advances, liability should not rest solely on programmers or owners; smart systems themselves could be held accountable for damages caused by their actions. This would imply granting AI an independent financial liability to compensate victims directly, By contrast, another perspective holds that criminal liability belongs exclusively to natural persons, and cannot extend to AI systems, since most criminal sanctions cannot meaningfully apply to machines. The central purpose of criminal law—

general and specific deterrence—cannot be achieved with AI[28]. Nevertheless, some suggest recognizing AI as a juridical person, enabling accountability through monetary fines, while also holding developers, operators, or companies liable for harmful outcomes.

3. The Problem of Privacy Violations

AI presents a serious challenge to privacy, as it relies on the collection and analysis of massive amounts of personal data, including private messages, communications, and browsing histories. These data are processed through algorithms and models to generate new information, which helps improve system performance, adapt to surrounding environments, and support autonomous decision-making, The wider the deployment of AI applications, the greater the risk of privacy violations[29], especially in the absence of specific legal frameworks governing the use of personal data by AI systems. AI-driven tracking and surveillance mechanisms raise concerns about the **legality of data collection**, as well as the proportionality of such practices when justified by public security, public order, and the protection of individuals in cyberspace. This underscores the urgent need for tailored legal safeguards to protect the right to privacy in the context of AI applications.

4. The Problem of the Legitimacy of Electronic Evidence

Electronic evidence refers to data or proof existing in the virtual world, often extracted from computers or other devices used in the commission of a crime. Such evidence is highly technical and requires expert knowledge for its retrieval and analysis[30], The use of AI systems during investigation or surveillance may occur without sufficient judicial oversight, raising doubts about the **legitimacy of procedures** and, consequently, the admissibility of evidence obtained, Furthermore, judicial bodies in many legal systems often lack the technical expertise necessary to assess the validity or accuracy of AI-generated evidence, which complicates its effective use in criminal proceedings.

Conclusion

Artificial intelligence is distinguished by its advanced capabilities in ensuring cybersecurity and combating cybercrime. It provides sophisticated techniques for detecting suspicious activities, analyzing big data, and predicting cyber threats, while also enhancing the ability of cyber police to respond rapidly to attacks. However, the integration of AI applications into the fight against cybercrime also generates several legal challenges. Chief among these are the inadequacy of current legislation to keep pace with rapid technological developments, the difficulty of determining criminal liability for actions carried out by AI systems, and issues related to privacy and the admissibility of AI-derived evidence in ensuring fair trials.

Based on the foregoing, the study reached the following key findings:

✓ Artificial intelligence is an effective mechanism for analyzing data and predicting patterns of criminal behavior in cyberspace.

✓ The absence of clear legislative provisions regulating the use of AI systems limits the effective legal benefits of this technology.

✓ The lack of a legal framework addressing liability for AI-related errors raises significant challenges regarding criminal accountability.

✓ The use of AI in criminal investigations may infringe upon the right to privacy and raises questions concerning the admissibility of evidence before judicial authorities, particularly in the absence of legislation regulating AI applications.

In light of these findings, the study proposes the following recommendations:

✓ Ensure the effective use of AI systems in combating cybercrime, given their efficiency and the fact that both AI and cybercrime emerge from the same digital environment.

✓ Draft specific legislation tailored to the unique nature of AI systems, while amending existing laws to align with these particularities.

✓ Encourage the use of AI in security, research, and crime detection, both in general and specifically in the digital domain.

✓ Train technical and legal experts capable of understanding the intersection between AI and cybercrime to ensure the proper implementation of relevant laws.

✓ Strengthen international cooperation and promote the exchange of information and expertise among states and international organizations specialized in combating cybercrime.

Margins:

[1]Salima Qazlan & Younsi Hafidha. "Defining the Conceptual Framework of Artificial Intelligence.".Al Tourath Journal, University of Djelfa,Vol. 14, No. 03, September 2024, pp.99.

[2] Ghufran Mohamed Ibrahim, Yousra Mohamed Mahmoud Shaaban & Amal Mohamed Manour Najahi. "Artificial Intelligence Governance under International Human Rights Law.", Jordan Studies, University of Jordan, No. 04, 2022, pp. 128.

[3] Manal Mohamed Kurdi & Jalal Ibrahim Al-Eid, Introduction to Management Information Systems: Basic Concepts and Applications, New University House, Alexandria, 2003, p. 364.

[4] Ali Ahmed Ibrahim, Applications of Artificial Intelligence in Confronting Cybercrimes, Legal Journal, Cairo University – Khartoum Branch-, No. 08, 2020/2021, p. 2814.

[5] Mohamed Fathi Mohamed Ibrahim, Legislative Regulation of Artificial Intelligence Applications, Journal of Legal and Economic Research, Mansoura University, September 2022, p. 1033.

[6] Ammar Babbli & Yasser Mohamed Zuheir, The Role of Artificial Intelligence Systems in Crime Prediction, Journal of Security and Law, Vol. 29, No. 01, January 2021, pp. 125–126.

[7] Qennouz Fatiha, Legal Aspects of Using Artificial Intelligence, Algerian Journal of Law and Political Science, University of Tissemsilt, Vol. 09, No. 01, 2024, p. 1183.

[8] Sabrine Jaber Mohamed, The Problem of Applying the Rules of Criminal Liability to Artificial Intelligence Crimes, Journal of Legal and Economic Research, University Center Aflou, Vol. 08, No. 01, January 2025, p. 89.

[9] Omar Nafea Reda Al-Abbasi, The Legal System of Artificial Intelligence: A Comparative Study, 1st ed., Arab Center for Publishing and Distribution, Egypt, 2023, p. 38.

[10] Law No. 18-05 of May 10, 2018, on Electronic Commerce, Official Gazette, No. 25, issued May 16, 2018, p. 04.

[11] Article 17 of Presidential Decree No. 21-323 of August 22, 2021, establishing the National Higher School of Artificial Intelligence, Official Gazette, No. 65, issued August 30, 2021, p.19.

[12] Tarek Ibrahim El-Dessouki Atiya, Globalization of Crime: The Global Partnership in Criminal Practices, New University House, Alexandria, 2010, p. 208.

[13] Saliha Boujadi, The Conceptual Framework of Cybercrime, Journal of Comparative Legal Studies études juridique comparées, Universityof Hassiba Ben Bouali Algaria, Vol. 07, No. 01, June 2021, p. 2529.

[14] Abdelhadi Drar, Mechanisms for Confronting Digital Crime in Algerian Legislation, Modern Journal of Legal Studies, Al-Asriya University College, Ramallah, Palestine, Vol. 01, No. 02, 2023, p. 250.

[15] Mohamed El-Saghir Messeka, The Concept of Emerging Crimes and Their Legal Nature (Cybercrimes), Journal of Legal and Political Studies, University of Laghouat,/ Vol. 08, No. 01, January 2022, p. 135.

[16] Article 02 of Law No. 09-04 of August 05, 2009, on Specific Rules for the Prevention and Combating of Crimes Related to ICT, Official Gazette, No. 47, of August 16, 2009, p.05.

[17] Law No. 04-15 of November 10,2004, amending the Penal Code, Official Gazette, No. 71, of November 10,2004, p.08.

[18] Mouna Meqlani & Radia Mouchri, Cybercrime: The Meaning of the Concept and the Effectiveness of Legal Treatment, Journal of Legal and Political Research, University of Jijel, Vol. 06, No. 01, June 2021, pp. 497–498.

[19] Yasmine Bounara, Cybercrime, El-Mieyar Journal, University of Constantine, Vol. 20, No. 39, June 2015, p. 281.

[20] Naima Douadi, Cybercrime: Its Characteristics, Areas of Application, and Main Means of Combating It, Mahd Al-Lughat Journal, University of Chlef, Vol. 02, No. 01, August 2020, pp. 48–49.

[21] Abdelmoumen Si Hamdi & Souad Qeira, Cybercrime and Mechanisms for Confronting It in Algerian Law, EL Bibane Journal of Legal and Political Studies, University of Bordj Bou Arreridj, Vol. 07, No. 01, June 2022, p. 63.

[22] Mohamed Rahmouni, Characteristics of Cybercrime and Its Areas of Application, Al-Haqiqa Journal, Adrar University , No. 41, January 2018, p. 444 ff.

[23] Mourad Mohamed Ghaleb Mohamed Qasem, The Role of Artificial Intelligence in Combating Cybercrime – A Comparative Study, Modern Journal of Legal Studies, Al-Asriya University College, Ramallah, Palestine, Vol. 02, No. 02, June 2024, pp. 103–104.

[24] Noura Amina Al-Akhnach & Mohamed Al-Idani, Artificial Intelligence as a Mechanism to Confront Cybercrime, Journal of Law and Environmental Sciences, University of Djelfa, Vol. 02, No. 02, September 2023, pp. 536–537.

[25] Abdelnour Abdelhaq & Omar Hamas, Artificial Intelligence between Committing Financial Crimes and Preventing Them, Journal of Legal and Social Sciences, University of Djelfa, Vol. 09, No. 03, September 2024, p. 502.

[26] Adel Abdel-Sami Awad, The Role of Artificial Intelligence in Predicting and Combating Terrorism, Moutoune Journal, University of Saida, Vol. 17, No. 01, p. 72.

[27] Mohamed Ali Abu Ali, Criminal Liability for Artificial Intelligence Damages, 1st ed., Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 2024, p. 51.

[28] Wafaa Mimouni & Nour-Eddine Amari, Artificial Intelligence between the Hammer of Law and the Anvil of Technological Innovation, Algerian Journal of Law and Political Sciences, University of Tissemsilt, Vol. 09, No. 02, December 2024, pp. 181–182.

[29] Abdallah Cheibani & Widad Ben Salem, The Right to Informational Privacy in Light of Artificial Intelligence, Journal of Legal and Economic Studies, University Center Barika, Vol. 06, No. 02, November 2023, p. 459.

[30] Yas Hassan Mohamed Othman, Digital Evidence and Its Impact on Criminal Proceedings, Journal of Legal and Social Sciences, University of Djelfa, Vol. 05, No. 03, September 2025, p. 318.