

## The Role of Artificial Intelligence in Criminal Investigation: Digital Evidence as a Model

### دور الذكاء الاصطناعي في التحقيقات الجنائية- الأدلة الرقمية نموذجاً -

HEMIS Maamar \*

University of Djillali Bounaama, Khemis Miliana (Algeria)

Civil Status System Laboratory

[maamar.hemis@univ-dbkm.dz](mailto:maamar.hemis@univ-dbkm.dz)

Date of Submission 02-04-2026 Date of Final Acceptance 12-09-2026 Date of Publication September 2026

#### Abstract:

The rapid development of artificial intelligence has brought about a qualitative transformation in criminal investigations, particularly with regard to digital evidence. Its technologies enable investigative authorities to analyze vast amounts of electronic data with high speed and accuracy. Artificial intelligence assists in detecting hidden criminal patterns and systematically linking digital facts and events. It also contributes to the analysis of images and videos and the tracking of suspicious online activities. Moreover, it has become an effective tool in combating complex cybercrimes. However, reliance on artificial intelligence raises legal issues concerning the evidentiary value of digital evidence. In addition, it poses ethical challenges related to the protection of personal data. This necessitates the establishment of a clear legal framework that ensures investigative efficiency while safeguarding fundamental rights and freedoms.

**Keywords :** Artificial Intelligence, Criminal Investigations, Digital Evidence, Cybercrime, Digital Forensic Analysis, Evidentiary Value.

#### ملخص:

أدى التطور المتسارع للذكاء الاصطناعي إلى إحداث نقلة نوعية في مجال التحقيقات الجنائية، ولا سيما في ما يتعلق بالأدلة الرقمية، إذ تُمكن تقنياته الجهات المختصة من تحليل كميات ضخمة من البيانات الإلكترونية بسرعة ودقة عاليتين، ويساعد الذكاء الاصطناعي في كشف الأنماط الإجرامية الخفية وربط الوقائع الرقمية ببعضها البعض بشكل منهجي، كما يساهم في تحليل الصور والفيديوهات وتتبع الأنشطة الإلكترونية المشبوهة، ويُعد أداة فعّالة في مواجهة الجرائم السيبرانية المعقدة، غير أن الاعتماد عليه يثير إشكالات قانونية تتعلق بحجية الأدلة الرقمية. إضافة إلى تحديات أخلاقية مرتبطة بحماية المعطيات الشخصية، مما يستلزم وضع إطار قانوني واضح يضمن فعالية التحقيق مع احترام الحقوق والحريات الأساسية.

**الكلمات المفتاحية:** الذكاء الاصطناعي، التحقيقات الجنائية، الأدلة الرقمية، الجرائم السيبرانية، التحليل الجنائي الرقمي، حجية الدليل الإلكتروني.

\* Corresponding Author: HEMIS Maamar

**Introduction:**

The rapid technological development has led to a qualitative shift in criminal justice mechanisms, especially with the emergence of **Artificial Intelligence (AI)**, which has become a pivotal element in collecting and analyzing evidence. Therefore, criminal investigation no longer relies solely on human expertise but now depends on intelligent systems capable of processing enormous amounts of digital information, deciphering complex codes, and extracting precise criminal indicators.

The contemporary world is witnessing rapid technological transformations that have imposed themselves on various areas of life, including criminal justice, which increasingly relies on **Artificial Intelligence (AI)** in data and evidence analysis. The latter has become an effective tool in crime detection and offender tracking, particularly amid the growing prevalence of cybercrimes that rely on the digital space either as a means or as an environment for committing the crime <sup>1</sup>

Among the most prominent applications of AI in this field is the analysis of **digital evidence** extracted from electronic devices or information networks, which today represents a major focus in modern criminal investigations.

This new reality raises the question of the extent to which AI can develop criminal investigation methodologies and the legal and ethical challenges it poses, particularly regarding the **legitimacy of digital evidence** and **protection of individual privacy**.

This research aims to achieve several scientific and practical objectives, most notably:

1. Analyzing the role of AI in developing criminal investigation methods.
2. Clarifying the concept of digital evidence and its importance in modern criminal proof.
3. Demonstrating AI applications in digital evidence analysis and how they are employed in crime detection.
4. Monitoring the legal and ethical challenges posed by AI technologies in the criminal field.
5. Proposing a balanced legal and ethical framework that ensures the benefit from technology without harming human rights.

In this context, the importance of this topic stems from its addressing of the interaction between criminal law and the digital revolution, which represents a major challenge for legal systems worldwide.

- **From a scientific perspective:** The research contributes to enriching legal studies related to AI, especially in the field of evidence and investigation.
- **From a practical perspective:** It provides modern insights for investigators and experts on how to employ intelligent systems to analyze digital evidence more effectively.
- **From a legislative perspective:** It helps formulate proposals to update national laws in line with technological developments while ensuring respect for fundamental rights.

This research relied on the **descriptive-analytical methodology**, through:

- Accurate description of the concept of AI and its applications in criminal investigation.
- Analysis of legal texts, jurisprudential references, and relevant international materials.
- The comparative method when necessary, to compare some international experiences (such as French and American) in using AI in digital evidence analysis.
- The inductive method was also adopted to infer results from practical applications and case studies.

The main research problem is summarized in the central question:

**To what extent has AI contributed to developing criminal investigation methodology through digital evidence analysis, and what are the resulting legal and ethical challenges?**

## **Section I: The Conceptual Framework of AI and Criminal Investigation**

This chapter is a fundamental theoretical introduction to understanding the relationship between AI and criminal investigation. It aims to clarify the basic concepts associated with both, including the nature of AI and its legal applications, then defining traditional and digital criminal investigation as a basis for understanding the new role of intelligent technologies in this field.

### **A) The Concept of AI in the Criminal Field**

AI is defined as: *“the ability of technical systems to perform tasks that usually require human intelligence, such as understanding, learning, and decision-making.”* <sup>2</sup>

This concept is among the most comprehensive in the digital revolution era, as it encompasses a wide spectrum of applications that simulate human thinking methods and rely on data, algorithms, and machine learning.

In the criminal field, AI refers to: *“the use of intelligent software and algorithms to analyze criminal data, extract patterns or indicators that contribute to crime detection or prediction.”*

Its applications include multiple areas, such as:

- Facial recognition systems.
- Analysis of digital texts and communications.
- Monitoring information networks.
- Examining digital evidence and extracting elements of investigative value.

The importance of these technologies lies in their ability to process huge amounts of data faster than humans, while maintaining high accuracy and objectivity in analysis <sup>3</sup>

AI allows analyzing massive information rapidly, enhancing the precision of investigation and accelerating the achievement of results.

Researchers confirm that integrating AI into investigative agencies' work is considered a *“qualitative transformation in modern criminal justice”*, as the role of technology has shifted from

simple technical assistance to participation in “*analytical decision-making*” in criminal processes, through reading patterns and inferring relationships between facts and individuals.

The significance of AI in the criminal field stems from its ability to enhance investigative accuracy, accelerate investigation pace, and improve the ability to detect criminal activities, especially amid the massive expansion and diversity of cybercrime.

However, its use remains conditional on respecting legal safeguards, particularly concerning privacy protection and algorithmic transparency, to prevent infringement on individual rights or deviation from justice.

## **B) Criminal Investigation in the Digital Environment**

Criminal investigation is defined as: “*a systematic process aimed at collecting, analyzing, interpreting, and presenting evidence before the judiciary.*”<sup>4</sup>

Investigation is one of the fundamental pillars of the criminal justice system, as it embodies the stage in which judicial truth is established by following a strict scientific methodology that combines respect for the legal guarantees of litigants with effective identification of the perpetrator.

With deep transformations imposed by modern technology, crime is no longer confined to physical space but has gradually moved into the digital environment, occurring via information networks, smart devices, or platforms and data-driven systems.

This shift to cyberspace has created a complex environment characterized by speed, encryption, and transboundary nature, forcing criminal justice agencies to reconsider traditional investigation methods and develop advanced technological capabilities to face cybercrime<sup>5</sup>

From this context, the concept of **Digital Forensics** emerged, defined as: “*a set of technical and legal procedures aimed at examining electronic devices, information systems, and digital data to extract legally admissible evidence that can be presented before the judiciary.*”<sup>6</sup>

This type of investigation relies on specialized techniques capable of recovering deleted data, analyzing system logs, tracing digital fingerprints, and identifying the source of cyber-attacks, while maintaining the integrity of digital evidence to ensure judicial acceptance.

Investigating digital crimes is not only technical but also requires deep legal understanding, due to the peculiarities of digital evidence and its susceptibility to rapid alteration or destruction. Hence, it is imperative for legislators and judicial authorities to develop laws and procedures compatible with the nature of such evidence, regarding collection, preservation, and presentation before the judiciary, ensuring a balance between protecting individual rights and effective crime fighting in a rapidly evolving digital world.

Digital criminal investigation differs from traditional investigation in that it deals with “*intangible evidence*” easily copied or destroyed, such as emails, encrypted files, browsing histories, and

metadata. Therefore, precise techniques are required to ensure evidence integrity and prevent tampering.

In this context, AI systems have become pivotal in analyzing such evidence, providing automatic classification, pattern recognition, and user behavior prediction, giving them a central position in the future of digital criminal investigations <sup>7</sup>

## **Section II: Artificial Intelligence as a Tool for Digital Evidence Analysis**

AI is considered one of the most prominent tools that have transformed criminal investigation methods in the digital era. It enables investigators to analyze massive amounts of data with speed and accuracy surpassing human capabilities. Its various applications have turned digital evidence from static data into effective criminal indicators that help detect crimes and identify perpetrators.

To understand this role, it is necessary first to identify the nature of digital evidence that can be analyzed and then clarify how AI contributes to processing it.

### **A) Types of Digital Evidence that Can Be Analyzed**

The digital environment has witnessed a significant expansion in the volume of data generated daily from various devices and information platforms, making digital evidence a core component of modern criminal investigations.

Digital evidence refers to any information extracted from an electronic device or system that can help uncover a crime, identify perpetrators, or reconstruct events.

Such evidence is intangible and highly mutable, requiring precise procedures for collection, analysis, and preservation.

Digital evidence includes any electronically stored or transmitted information that can be used to prove a factual or legal event. Its main types are as follows:

#### **1- Computer Data**

Includes information stored in desktop and laptop computers, such as:

- Text files, images, and documents
- Deleted files recoverable through forensic methods
- System logs
- Login and usage records <sup>8</sup>

These data are one of the most important sources of digital criminal evidence because they preserve technical traces that help determine the time and nature of the criminal activity.

## 2 - Smartphones and Mobile Devices Data

Smartphones contain large amounts of personal and professional data, including:

- Text messages and app-based conversations
- Call logs and contact lists
- Photos and videos
- GPS location data
- Installed applications and related files <sup>9</sup>

These data are highly valuable in cases involving communication, hacking, cyber harassment, or criminal coordination.

## 3 - Network-Based Evidence

Evidence generated from data traffic through local and global networks, including:

- a. Server logs
- b. Network traffic
- c. Firewall logs
- d. Router and switch logs <sup>10</sup>

Such evidence is used to detect cyber-attacks, hacking attempts, or trace digital communications.

## 4 - Multimedia Evidence

Includes:

- a. Digital images
- b. Video clips
- c. Audio recordings

This evidence requires specialized analysis focusing on authenticity verification and detecting any manipulation, using tools such as **Image Forensics** or **Audio Forensics** <sup>11</sup>

## 5 - Social Media Evidence

Platforms like Facebook, Instagram, WhatsApp, and Telegram generate huge amounts of data used in investigations, such as:

- a. Messages and conversations
- b. Interactions and posts
- c. Login records and user locations

This evidence is particularly important in cases of blackmail, online fraud, and defamation.

## 6 - Cloud-Based Evidence

Includes information stored on remote servers, such as:

- a. Shared files
- b. Backups
- c. Cloud system logs

Accessing such evidence is sometimes difficult due to differing jurisdictions and multiple service providers worldwide <sup>12</sup>

## 7 - Internet of Things (IoT) Evidence

With the proliferation of smart devices, evidence can be extracted from:

- a. Smart home cameras
- b. Fitness trackers
- c. Home automation devices
- d. Sensors

Such data contribute to reconstructing events or accurately locating individuals.

## B) The Role of AI in Analyzing Digital Evidence

AI has triggered a real revolution in **digital forensic analysis**, being used to detect patterns, identify suspicious behaviors, and classify data according to its criminal significance. Its practical applications include : <sup>13</sup>

### 1 - Machine Learning

This technique trains systems on massive datasets to autonomously detect criminal patterns and relationships.

It is especially used in analyzing hacking behavior, online fraud, and predicting repeated cybercrimes <sup>14</sup>

### 2 - Image and Audio Recognition

Computer vision and audio processing algorithms are used to analyze surveillance footage and audio recordings, enabling precise recognition of suspects' faces and voices <sup>15</sup>

This technology is also employed to detect tampered or digitally altered scenes and images.

### 3 - Text and Communication Analysis

AI systems utilize **Natural Language Processing (NLP)** to analyze conversations and emails to determine criminal intent or suspicious relationships between communicating parties. This analysis is crucial in cases of cyberterrorism, blackmail, and online incitement <sup>16</sup>

#### - *Text Content Analysis*

Focuses on processing digital texts to identify:

- Keywords with criminal significance
- Encoded or indirect phrases
- Linguistic style that may indicate the author's identity
- Indicators of threats, blackmail, or incitement
- Repetition patterns or distinctive vocabulary of a person or group

AI techniques such as NLP help convert texts into analyzable statistical or semantic data.

#### - *Digital Communication Analysis*

Examines metadata and communication structure, such as:

- Message timestamps
- Conversation duration
- Sender and recipient identity
- Device type
- Message location (if available)

This data helps track information flow, identify involved parties, or establish connections between suspects and victims or criminal networks <sup>17</sup>

#### - *Email Forensics*

Involves examining:

- Sender and recipient addresses
- IP addresses
- Email headers
- Attachments
- Suspicious links

Essential in cases of online fraud, phishing, and targeted cyberattacks <sup>18</sup>

#### - *Voice and Audio Message Analysis*

With frequent use of voice messages in apps, analysis includes:

- Voice characteristics
- Speaker tone
- Message content
- Verifying authenticity and ensuring no alterations

### - *Contextual and Behavioral Analysis*

Digital investigation considers not only words but also:

- Writing style (Stylometry)
- Typing speed
- Common mistakes
- Linguistic tendencies
- Social context of the conversation

These elements help determine whether a message is authentic, written by the original author, or fabricated, enhancing its legal admissibility <sup>19</sup>

## 4 - Criminal Network Analysis

AI techniques rely on **Social Network Analysis (SNA)** to uncover hidden links between perpetrators by tracing digital communications and identifying the most influential nodes in criminal networks.

These applications are effective tools for dismantling cyber gangs and transnational organized crime <sup>20</sup>

AI's role in digital evidence analysis now extends beyond technical aspects to support decision-making in investigations by providing **accurate probabilistic conclusions** that guide investigators toward realistic paths.

Criminal network analysis is defined as: *“a set of techniques used to uncover the internal structure of criminal groups by studying links between individuals and determining the degree of influence and connectivity among them.”*

It is particularly used in cases involving:

- Organized crime
- Terrorism and its financing
- Drugs
- Human trafficking
- Complex cybercrimes <sup>21</sup>

The analysis relies on social and mathematical sciences, especially SNA, and uses diverse data, including:

- Call Detail Records (CDR)
- Emails and digital chats
- Social media metadata
- App communication logs
- Geographical data of communicants
- Electronic financial transfers
- Closed group chat activities <sup>22</sup>

Thus, AI has transformed digital evidence analysis from limited human effort to an intelligent system capable of detection, inference, and prediction. Yet, its use poses **legal challenges** concerning evidence legitimacy and the limits of machine authority in judicial procedures.

### Section III : Legal and Ethical Challenges in Using AI with Digital Evidence

Despite AI's immense benefits in criminal investigation and digital evidence analysis, its deployment raises numerous complex legal and ethical issues, particularly regarding evidence legitimacy, privacy protection, and algorithmic error responsibility.

This chapter highlights the main challenges across three sections:

#### A) Legitimacy of Automatically Extracted Evidence

A central question arises regarding the **judicial admissibility of digital evidence produced by AI systems**, especially since such evidence is extracted through complex technical processes difficult for judges or defense attorneys to fully verify.

Some scholars argue that this evidence may lack a proper **chain of custody**, as in traditional criminal procedures, ensuring evidence integrity from collection to presentation before the judiciary.

Another issue concerns the possibility of judicial oversight of algorithms. Many codes are privately owned, creating a “**black box**” in interpreting technical results, threatening transparency and limiting the right to challenge scientific evidence.

#### B) Privacy and Individual Rights Protection

Protecting personal data is among the most prominent legal and ethical challenges in using AI with digital evidence. With the expansion of digital monitoring, algorithms can collect and analyze vast amounts of sensitive data without explicit consent, potentially violating procedural legality and privacy protection under national laws and international conventions <sup>23</sup>

This challenge intensifies without specialized legal frameworks regulating AI usage in investigations, data collection limits, storage, retention periods, and ultimately necessitates national legislation aligned with European and international standards <sup>24</sup>

**C) Algorithmic Bias and Legal Responsibility**

One of the most serious challenges is **algorithmic bias**, as AI systems rely on previously trained data that may contain human errors or biases, resulting in unfair outcomes, such as false suspicion or skewed behavior evaluation.

Studies have shown that algorithms may exhibit discriminatory tendencies when analyzing criminal data, particularly regarding gender, ethnicity, or social affiliation.

Legal responsibility is also debated: if a technical error occurs or an inaccurate result is issued, who is accountable—the programmer, the security authority using it, or AI itself? This issue remains controversial and reveals the urgent need to redefine legal responsibility concepts in the era of comprehensive digital transformation <sup>25</sup>

**Conclusion:**

This research has shown that AI is no longer a mere supporting technology but a core pillar in developing contemporary criminal investigation tools and methods, particularly amid widespread cybercrime and its complexity.

Conceptual and applied analysis demonstrates AI's pivotal role in **digital evidence analysis**, thanks to its ability to process large datasets, detect hidden patterns, and accelerate results that previously required arduous human effort.

Key conclusions include:

1. AI represents a qualitative leap in criminal justice, enhancing accuracy and efficiency, especially in complex cybercrimes.
2. Digital evidence has become a major component of criminal proof, and AI analysis is an effective tool to identify perpetrators and track activities.
3. Legal challenges, particularly evidence legitimacy, privacy protection, and algorithmic bias, pose obstacles to balanced and responsible AI use.
4. Current legal frameworks in most countries are insufficient to handle automatically extracted evidence or technical liability cases.

Practical and legislative recommendations:

1. Update criminal and procedural laws to include clear provisions on AI-extracted digital evidence and criteria for judicial acceptance.
2. Establish independent national bodies for technical and judicial oversight of intelligent systems in the criminal field to ensure transparency.
3. Enhance training programs for investigators, judges, and experts in AI and cybersecurity for precise understanding of digital evidence and analysis methods.
4. Establish ethical standards and professional guidelines defining AI usage limits in investigations while protecting individual privacy and fundamental rights.

5. Promote scientific research and international cooperation in criminal AI to exchange expertise and develop more precise and fair analytical tools.

In conclusion, the future of criminal investigation is heading toward **integrating AI as a core actor in criminal justice systems**, with successful integration contingent on balancing **technical efficiency** and **legal-human safeguards**, which form the essence of justice

#### Citations:

1. عبد اللطيف سامي، الذكاء الاصطناعي والتحقيقات الجنائية الرقمية، مجلة القانون والتكنولوجيا، العدد 5، 2023، ص 12
2. Russell Stuart J, & Norvig Peter, Artificial Intelligence: A Modern Approach (4th ed.). Pearson, 2021, p 5
3. عبد اللطيف، سامي ، الذكاء الاصطناعي والتحقيقات الجنائية الرقمية، مجلة القانون والتكنولوجيا، العدد 5، 2023، ص 14
4. Mike Maguire ,Criminal Investigation. Oxford University Press,2018, p. 33
5. <sup>1</sup> Casey Eoghan Patrick, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet , 4th edn, Academic Press 2019, P 12.
6. International Organization for Standardization. (2015). ISO/IEC 27043:2015 — Information technology—Security techniques—Incident investigation principles and processes, 2015
7. Casey Eoghan Patrick, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet ,4th edn, Academic Press, 2019, P 425.
8. Casey, Eoghan Patrick, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet , 4th edn, Academic Press 2019, P 78.
9. Casey Eoghan Patrick, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet , 4th edn, Academic Press 2019, P 112.
10. International Organization for Standardization, ISO/IEC 27043:2015 — Information technology—Security techniques—Incident investigation principles and processes (2015) , P 23.
11. Casey Eoghan Patrick, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet , 4th edn, Academic Press 2019, P 210.
12. United Nations Office on Drugs and Crime (UNODC), AI and Criminal Justice Systems , Vienna ,2021, P 48.
13. Casey Eoghan Patrick, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet , 4th edn, Academic Press, 2019, P 425.
14. Chen Chao Liu, Wei Zhang Xin, et al., ‘Machine Learning in Digital Forensics’ (2020) 8 IEEE Access, p. 12
15. Goodfellow, I, Bengio, Y, & Courville, A ,Deep Learning, MIT Press, 2016, p. 218
16. عبد المنعم كمال، الأدلة الإلكترونية في ظل الذكاء الاصطناعي، دار النهضة العربية، القاهرة، 2022، ص 33
17. Casey Eoghan Patrick, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet , 4th edn, Academic Press 2019, P 332.
18. <sup>1</sup> Casey Eoghan Patrick, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet , 4th edn, Academic Press 2019, P 310.
19. Casey Eoghan, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (4th ed.). Communication Analysis, Text Evidence, Messaging Artifacts , Academic Press, 2019, pp. 423–438
20. UNODC, AI and Criminal Justice Systems, United Nations Office on Drugs and Crime, Vienna, 2021, p 64

21. Álvarez-Hamelin José Ignacio, *Criminal Networks and Network Analysis* , Routledge, 2018, pp 45–63.
22. Borgatti Stephen P, Everett Martin G, Johnson Jeffrey C, *Analyzing Social Networks* 2nd edn, SAGE Publications, 2018, pp. 97–130.
23. Marr Bernard, *Artificial Intelligence and the Law* , Forbes Publications, 2022, p. 55.
24. European Data Protection Board, *Guidelines on AI and Data Protection*, Brussels, 2021
25. أبو طالب حسن، المسؤولية القانونية عن أخطاء الذكاء الاصطناعي، مجلة الحقوق، جامعة الكويت، المجلد 47، العدد 2، 2023، ص 77

## Bibliography :

### A- Books:

1. Russell Stuart J., Norvig, Peter, *Artificial Intelligence: A Modern Approach* , 4th edn, Pearson, 2021
2. Maguire Mike, *Criminal Investigation* , Oxford University Press, 2018
3. International Organization for Standardization, *ISO/IEC 27043:2015 — Information Technology—Security Techniques—Incident Investigation Principles and Processes* (2015).
4. Chen Chao Liu, Wei Zhang Xin, *et al.*, ‘Machine Learning in Digital Forensics’ (2020) 8 *IEEE Access*.
5. United Nations Office on Drugs and Crime (UNODC), *AI and Criminal Justice Systems*, Vienna ,2021
6. Marr Bernard, *Artificial Intelligence and the Law* , Forbes Publications, 2022
7. عبد المنعم كمال، الأدلة الإلكترونية في ظل الذكاء الاصطناعي، دار النهضة العربية، القاهرة، 2022.

### B- Articles:

8. Goodfellow Ian J, Bengio Yoshua, Courville Aaron, *Deep Learning*, MIT Press, 2016
9. Casey Eoghan Patrick, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 4th edn, Academic Press, ‘Communication Analysis, Text Evidence, and Messaging Artifacts’, 2019, pp. 423–438.
10. Álvarez-Hamelin José Ignacio, *Criminal Networks and Network Analysis*, Routledge, 2018, pp 45–63.
11. Borgatti Stephen P, Everett Martin G, Johnson Jeffrey C, *Analyzing Social Networks* 2nd edn, SAGE Publications, 2018, pp. 97–130.
12. European Data Protection Board, *Guidelines on AI and Data Protection* (Brussels 2021).
13. عبد اللطيف سامي، الذكاء الاصطناعي والتحقيقات الجنائية الرقمية، مجلة القانون والتكنولوجيا، العدد 5، 2023.
14. أبو طالب حسن، المسؤولية القانونية عن أخطاء الذكاء الاصطناعي، مجلة الحقوق، جامعة الكويت، المجلد 47، العدد 2، 2023.