Pak. j. life soc. Sci. (2025), 23(1): 37-52 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences

www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2025-23.1.004

RESEARCH ARTICLE

Authenticity of Using Artificial Intelligence Systems in Proving Electronic Evidence

Murtada Abdalla Kheiri[1*], Nizar Qashta[2], Dorgham Issa Aljaradat[3]

[1,2]Associate Professor of Civil Law at A'Sharqiyah University, Ibra, Oman

[3]Assistant Professor of Islamic Jurisprudence, College of Islamic Sciences, Palestine

ARTICLE INFO

Received: Apr 30, 2024

Accepted: Aug 28, 2024

Keywords

Artificial intelligence

Electronic evidence

Electronic proof

Evidentiary weight

Algorithmic bias

***Corresponding Author:**

murtadha.kheiri@asu.edu.om

ABSTRACT

The digital age has brought a surge in technological advancements, impacting every facet of life. The emergence of artificial intelligence technologies and the achievements and radical changes they offer have led to the emergence of new types of crimes characterized by the use of electronic evidence and the use of machines to commit them. This has prompted governments, police and judicial authorities to use artificial intelligence technologies to help detect these crimes and reduce their occurrence. However, employing AI in the courtroom raises significant questions. Expand more Concerns surrounding the validity, weight in court, and proper limitations of evidence extracted using AI This research delves into the role of AI in evidence extraction and its admissibility within the legal system. The research focuses on the contemporary legal landscape, particularly regarding electronic evidence and its weight in court. It addresses the challenges posed by AI, such as relying solely on AI for crime investigation and prosecution, and the resulting legal complexities. The research aims to:

- Define AI and electronic evidence.
- Identify the different types and characteristics of electronic evidence.
- Explore areas where AI can be applied in judicial evidence analysis.
- Examine the weight given to electronic evidence in court.

The research utilizes a combined scientific approach, employing both descriptive and analytical methods. It found that AI excels in data analysis, facial/eye recognition, and multimedia analysis, surpassing traditional computer programs. However, legal and legislative hurdles remain, along with challenges related to the weight of evidence, algorithmic bias, and deep fakes (manipulated videos). The research recommends a balanced approach. It suggests allowing AI use in courts with strict safeguards to protect liberties and ensure justice. These safeguards include upholding the presumption of innocence, carefully evaluating the weight of digital outputs, and thoroughly discussing them in court proceedings. Additionally, the research emphasizes the need for:

- Updating laws and regulations to keep pace with AI advancements.

- Educating law enforcement and judicial personnel on AI technologies.
- Continuously seeking solutions to address algorithmic bias and other emerging challenges. By implementing these recommendations, we can leverage AI's potential while ensuring its ethical and responsible use in the judicial system

INTRODUCTION

All praise is due to Allah, who taught by the pen, taught man that which he did not know; peace and blessings be upon our greatest Prophet, Muhammad, peace and blessings be upon him.

After that, in light of the enormous digital and technological revolution witnessed in various fields of modern life, along with the emergence of artificial intelligence technologies and the radical changes and achievements they bring across different fields, new types of crimes have appeared, characterized by the use of electronic evidence and the exploitation of machines in committing them. This development has prompted governments, law enforcement agencies, and judicial authorities to adopt artificial intelligence technologies to assist in detecting these crimes and reducing their occurrence.

The use of these technologies in the judicial field, particularly in proving the occurrence of crimes and attributing them to their perpetrators, raises significant questions about the validity of evidence derived through artificial intelligence means, the extent of its authenticity in legal proof, the permissible limits for using these methods in the judiciary, and the perspective of law and legislation on this matter.

For these reasons and others, this research is titled: "Using of Artificial Intelligence Systems in Proving Electronic Evidence."

Research Importance

The research's importance lies in its keeping pace with contemporary electronic issues and modern legal trends in using artificial intelligence technology. The research sheds light on the role of artificial intelligence in proving and extracting evidence, its focus on proving electronic evidence, and the extent of its authenticity in the judiciary.

Research problem

The research problem emerges from the legal problematics that need to be addressed in light of the risks posed by artificial intelligence technologies. These problematics raise many questions, including:

- Can artificial intelligence be relied upon to detect crimes? Can it be used to prove the occurrence of crimes and attribute them to their perpetrators? What are the difficulties and challenges that may result from this?
- What are the legal solutions to the problems resulting from using artificial intelligence in proving evidence? How can artificial intelligence be controlled without compromising the judicial system and the basic guarantees for properly administrating justice?

Research Objective

1. To define artificial intelligence, electronic evidence, and electronic proof.
2. To outline the types and characteristics of electronic evidence.

3. To explain the areas in which artificial intelligence can be used in judicial evidence.
4. To examine the authenticity of electronic evidence and the problematics of using artificial intelligence in Proving electronic.
5. To highlight the difficulties and challenges that may arise from using artificial intelligence in electronic evidence and to propose legal solutions to these issues.

RESEARCH METHODOLOGY

The research adopts an integrative scientific approach that combines descriptive and analytical methods. It involves describing and defining the issue and presenting various opinions on it. The research also resorts to the comparative approach in presenting different legal perspectives. The research then analyzes the data and opinions to arrive at conclusions.

Research plan

The research consists of three chapters conclusions, and the chapters are divided as follows:

Chapter One: The nature of artificial intelligence and electronic evidence

- First requirement: The concept of artificial intelligence.

- Second requirement: The concept of electronic evidence and electronic proof.

Chapter Two: Electronic evidence, its types and characteristics, and areas of proof by artificial intelligence.

First requirement: Electronic evidence, its types, and characteristics.

Second requirement: Areas and mechanisms of proof using artificial intelligence for electronic evidence.

Chapter Three: The authenticity of proving electronic evidence by artificial intelligence.

First requirement: The authenticity of proving electronic evidence.

Second requirement: Proving electronic evidence by artificial intelligence and its problems.

Conclusion: It contains the most important results and recommendations.

Chapter One: The Nature of Artificial Intelligence and Electronic Evidence:

First requirement: The concept of artificial intelligence:

Artificial Intelligence (AI) is a branch of computer science and a fundamental pillar of the technology industry in the present era (Artificial Intelligence in Education, 10/062024). The term “artificial intelligence” consists of two words: “intelligence” and “artificial.”

In linguistics: “Intelligence” (dhakaa) comes from the Arabic root (dhaka), clever heart, and a clever boy; if he is quick-witted, intelligence is quick-witted (Ibn Manzur, 1994). The term (dhaki) indicates someone who is clearly intelligent, with the plural form being (adhkiyaa). Its origin relates to the concepts of brightness and flame. This is also the name of the sun (Ibn Sidah, 1996). The person was intelligent: he was quick to understand and quick-witted, and his mind was intelligent: his intelligence was sharp (Mukhtar, 2008).

As for “artificial,” the word's root is derived from the verb (sana’a), which means to make or manufacture. The term (masnoo’) means something that is made or manufactured, and (saneea) refers to something that has been crafted or created. Also, he made it: he took it and made something. He called for its manufacture, and the manufacture is what you manufacture of a matter (Ibn Sidah, 2000). The root of the verb is ifta`ala from daraba and sana`a, so the ta` was changed to a ta (Ibn Iyad, no date), and the ta` here is a replacement for the ta` of ifta`ala (Ibn Iyad, no date).

Artificial: a singular noun derived from artificiality, meaning what is made unnaturally, i.e., made by man, including artificial silk and artificial heart (Mukhtar, 2008).

From the definitions of the two terms, it is clear that “intelligence” implies quickness and precision of understanding, while “artificial” refers to something that is manufactured or made. Therefore, “artificial intelligence " is a form of intelligence created or simulated, designed to mimic human intelligence. An artificial system is not inherently intelligent or unintelligent on its own unless it has some of the characteristics of the human mind.

In programming terminology, the essence of intelligence is the integration of information representation with the abilities and skills of information processing. It refers to mental processes that lead to innovation, brilliance, and control of movement, senses, and emotions (Izz Al-Din, 2007).

Intelligent programs are computer programs that simulate human mental abilities and working patterns, such as the ability to learn, infer, and react to situations that were not programmed into the machine (Artificial Intelligence article, 03/06/2024).

As for the term artificial intelligence, a group of researchers defined it similarly: “The study and design of intelligent agents, or it is: the science and engineering of making intelligent machines. It is a specific behavior and characteristics that characterize computer programs that make them imitate human mental abilities and work patterns. The most important is the ability to learn, infer, and react to situations that were not programmed into the machine (Artificial Intelligence article,13/06/2024). Another definition is: The science related to the creation of machines and the design of software that performs activities and tasks that would require intelligence if carried out by a human (Musa & Habib, 2019). Or: The science aimed at creating machines and developing computers and software that acquire intelligence, enabling them to perform recently exclusive tasks to humans (Adel, 2005; Khawaled,2019). Or: The science of computing that focuses on computer systems possessing characteristics related to human intelligence and the ability to make decisions in a manner somewhat similar to human behavior across various fields (Arnous, 2007).

Generative AI Models: It refers to a type of AI technology capable of generating various forms of content, including text, images, and synthesized data, from simple commands and contexts (Generative Artificial Intelligence, 2023).

The word “istana’a” contains the word “ifta’al” from “istana’a” and “ifta’ala”. It means that it is based on a request for a craft, and perhaps the term “generative intelligence” was taken from it. It generates words and sentences based on the user’s request.

So, generation here is not just the transfer of stored information but rather the presentation of new information generated from several sources. This is the meaning of craftsmanship, a mixture of several materials and efforts to produce a new form.

It is noted that all the aforementioned definitions agree on several things: that artificial intelligence is a simulation of human intelligence and that no definition of artificial intelligence does not depend on linking it to human intelligence. The goals of artificial intelligence include learning, reasoning, and perception, as well as the ability of artificial intelligence to think, act, and make decisions. Artificial intelligence is used in various areas of life (Alai & Abdul Majeed, 2023).

Based on the above, artificial intelligence can be defined as the capability of machines and digital computers to perform specific tasks that mimic and resemble human abilities. These include thinking, learning from previous experiences, and other cognitive processes such as natural language learning, performing practical tasks with coordinated precision, or using perceptual images and forms to guide physical behavior. Artificial intelligence aims to create intelligent systems that behave the same way as humans, providing their users with various services such as education, guidance, and interaction. At the same time, they can store accumulated human experiences and knowledge and use them in the decision-making process (Muhammad & Muhammad, 2020; Artificial Intelligence in Education, 10/062024).

Artificial intelligence has become an umbrella term for applications that perform complex tasks that previously required human input, such as communicating with customers online. Data science is an interdisciplinary field that uses scientific methods to extract value from data. It combines statistics skills and computer science with scientific knowledge to analyze data collected from multiple sources (Cybersecurity & Artificial Intelligence, 2024).

Based on the above, it becomes clear that the science of artificial intelligence is based on two basic principles:

Data representation: It is how to represent data or a problem in a computer so that the computer can process, output, and analyze the data (Jihad, 2014).

Decision-making: This is considered thinking in itself, as the computer searches for the options available to it and evaluates them according to criteria set for it or deduced by it itself, then decides on the best solution (Al-Asyuti, 2020).

Artificial intelligence consists of three basic components:

Knowledge base: It includes absolute facts and describes the logical relationships between elements and concepts, a set of experience-based facts, problem-solving methods, and mathematical formulas rules.

The inference mechanism system is programmed procedures that lead to the required solution by linking the relevant facts and rules to form deduction and reasoning.

The user interface: The procedures provide the user with appropriate tools to interact with the system during the development and use phase (Al-Asyuti, 2020).

Second requirement: The concept of electronic evidence and electronic proof:

Digital or Electronic Evidence is defined as information with evidential strength or value that is stored, transmitted, extracted, or obtained from computers, information networks, and similar sources. It can be collected and analyzed using specialized devices, software, or technological applications (Egyptian Law No. 175 of 2018)

Some researchers have defined it as: “Evidence obtained from computers in the form of magnetic or electrical fields and pulses, which can be collected and analyzed using specialized software, applications, and technology (Abdul Muttalib, 2020).”

The definitions appear to use the term digital evidence because data within a virtual medium is represented in binary code (0 and 1). When displayed, these binary numbers are converted into a visual format, such as images, documents, or recordings.

Digital evidence is a digital component that presents information in various forms, such as symbols, written text, images, sounds, shapes, and graphics. It represents thoughts and statements. Digital writing, which includes writing done through modern communication means, is broadly referred to as digital evidence (Al-Matradi, 2012).

Others have defined electronic evidence as: “Information that is accepted by logic and reason and relied upon by science, obtained through legal and scientific procedures by translating stored computational data from computers, their peripherals, and communication networks. It can be used at any stage of investigation or trial to prove the fact of any action or entity related to a crime, an offender, or a victim (Abdul Muttalib, 2020)”.

From the previous definitions, it can be inferred that digital evidence is information extracted from computers or other devices that rely on digital technology for operation. It can be read or interpreted by individuals with skills in reconstructing information using computer programs (Ibrahim, 2020).

Digital forensic evidence includes all digital data that can prove a crime has been committed, establish a connection between the crime and the offender, or a relationship between the crime and the victim (Hijazi, 2004).

Thus, digital forensic evidence is a type of forensic evidence that adheres to the same characteristics and conditions for use. However, digital evidence is distinguished by three qualitative characteristics: First, it is intangible; second, it is considered technical or scientific evidence (derived from machines); and third, understanding the content of digital evidence relies on using devices to collect and analyze it to serve as proof (Al-Jaradat, 2022).

In legal terminology, evidence is defined as the legally accepted means used by parties in a dispute to convince the judge of the validity of the facts they claim (Al-Nadawi, 1976).

Electronic proof is the establishment of evidence or proof before the judiciary using an electronic means or one or more electronic data formats (Al-Jaafari, 2013).

Electronic documents are information or data created, processed, transmitted, stored, or retrieved using electronic, optical, or similar means. They can be linguistic, non-linguistic, readable, audible, or visible. They may include contracts, promises, commitments, notifications of obligations, agreements, or other forms. These documents can be exchanged in either digital or analog formats (Al-Mahdi, 2007).

Chapter Two: Electronic evidence, its types and characteristics, and areas of proof by artificial intelligence.

First requirement: Electronic evidence, its concept, and types.

Judicial evidence: Judges use judgment methods to prove the occurrence of judicial rulings, such as admission, testimony, oath, refusal, or other things. These methods are also called arguments (Al-Qarafi, 1973; Ibn Abd al-Salam, 1991).

In general, evidence can be categorized into two types: evidence that is stated (direct evidence), such as testimony, oaths, and admissions, and evidence that is not stated, such as circumstantial evidence.

Jurists have differed regarding the methods of proof and judicial ruling. Are they limited, and only what is stated is acceptable, or are they absolute? There are two opinions (Ibn Abidin, 1966; Majmoo' al-Fatawa). The most correct of which is that they are absolute. Every method that indicates the establishment of a judicial fact and its stability in the event of a dispute must be acted upon and is not limited to what is stated (Al-Khanin, 2003).

This is what is known in civil law as free proof or restricted proof (Nasser, 2024; Abdul Latif, 1992; Marqus, 1981)

Contemporary electronic evidence often falls under what is called circumstantial evidence, and it follows free evidence. Contemporary means of evidence are many and varied, the most prominent of which are three categories:

First: Methods derived from physicochemical analysis: Includes seven fingerprints, which are fingerprints and voice prints, through which sounds can be distinguished from each other. This will become clear when discussing the application of artificial intelligence to verify voice recordings, eye prints, ear prints, smell prints, teeth prints, and lip prints.

Second: Scientific methods derived from some biological tests, Such as genetic fingerprinting (DNA) and blood fingerprints (Al-Jazzar, 2024)

Third: Modern means derived from electronic evidence: Such as computer-written texts and digital images, which are the subject of this research.

Electronic evidence can be divided – in general – into three types:

First: Digital images: They represent the visual facts about the crime and present the image on paper or visually via a computer or phone screen.

Second: Audio recordings stored by digital devices, including audio conversations on the Internet, computer, phone, and similar platforms.

Third: Written texts: This includes texts written by digital machines, including messages via e-mail and mobile phones, and data recorded by computers (Al-Jamali, 2009).

This type is represented in three forms:

First form: Records saved on the computer, phone, or tablet, which are written and saved documents, such as email, word processing program files, and chat program messages.

Second: Records created by the computer or phone and considered as its output and not touched by humans, such as log files, phone logs, and ATM bills.

Third: Records that contain a part saved by input and another part created by the computer or phone and processed electronically, such as student grade tables where the template is an Excel program. The teacher inputs the grades, and the program performs a calculation to produce the results (Ibrahim, 2020).

Characteristics of electronic evidence:

Electronic evidence is technical, invisible, or intangible and is not perceived by man's normal senses. No digital evidence exists outside its digital environment (Al-Bishri, 2002).

Electronic evidence is scientific evidence, meaning that it needs the technical environment in which it is formed. It must not deviate from its rule of not contradicting sound scientific rules. Scientific evidence must not deviate from what digital science has reached; otherwise, it will lose its meaning (Ben Younes, 2004). It is from the category of what is known as evidence derived from machines (Hamouda, 2003).

Second requirement: Areas and mechanisms of proof using artificial intelligence for electronic evidence.

Artificial intelligence plays a crucial role in data analysis, particularly in analyzing big data, due to its advanced features and ability to gather, organize, and infer. Analyzing data stored on digital devices and media now primarily relies on AI technologies (Yasser, 2019).

One of the areas where artificial intelligence is used is in forensic analysis of electronic evidence. This refers to the process of retrieving and analyzing content from digital devices such as computers, tablets, smartphones, and similar devices. It is a set of practices aimed at collecting, analyzing, and reporting digital data in a legally acceptable manner, with the goal of detecting or preventing crime.

Artificial intelligence techniques are used to inspect devices and detect crimes by analyzing computer files, whether they are present, deleted, or damaged, as well as advanced technologies such as facial recognition or iris analysis (Al-Sayed, 2016).

Electronic evidence is extracted through electronic processing, which refers to the technical operations carried out to write, compile, record, store, retrieve, or replace electronic data and information. This is done using media, computers, other devices, or newly developed media (Shams El-Din, 2021). The process of extracting digital evidence involves several key stages: evaluation, followed by collection or acquisition, then identifying and preserving the electronic document, performing the necessary technical analysis, and finally, presenting the evidence in a legally acceptable manner (Ali, 2023).

Artificial intelligence can play a crucial role in national security by assisting systems in scrutinizing vast amounts of data captured through surveillance. It helps analyze this data and alert analysts to any unusual or suspicious activities, indirectly aiding in crime prevention before it occurs (Yasser & Al-Babli, 2019).

Facial recognition technologies have proven to be significant in the field of forensic evidence. They support security through identity verification software and provide a reliable and efficient mechanism for verifying individuals' identities quickly and accurately (Alai & Abdul Majeed, 2023).

With the use of AI algorithms in voice analysis, accuracy and speed have significantly improved, reducing errors considerably. These technologies have demonstrated high effectiveness compared to traditional software programs, which do not match the capabilities of artificial intelligence (Sayed, 2021).

However, many concerns could theoretically limit the use of artificial intelligence in various fields, particularly regarding the evidence and legal responsibility associated with it. The issue of granting robots legal personality has sparked significant debate. While humans control robots, the advanced development of robots, their self-learning abilities, and problem-solving skills have led some legal experts to consider the possibility of granting legal personality to robots. The European Parliament proposed in its statement issued on 16/2/2017 the creation of an independent legal personality for advanced robots, referring to it as (electronic personality). This proposal was based on the anticipated benefit, especially in the field of civil liability. So, the most advanced autonomous robots would bear compensation for the damage they cause by themselves.

Chapter Three: The authenticity of proving electronic evidence by artificial intelligence.

First requirement: The authenticity of proving electronic evidence.

Evidence is defined in legal terminology as the legally acceptable means that the parties to a dispute use to persuade the judge of the validity of the facts they claim (Al-Nadawi, 1976).

This definition corresponds to what Islamic jurists refer to as proofs), legal evidence, or judicial methods, which are the means relied upon by the judge in their adjudication and upon which the judge bases their ruling (Kuwaiti Jurisprudence Encyclopedia, 1404 – 1427 AH).

Artificial intelligence and data analysis techniques contribute to the previous concepts in reaching evidence of the crime, whether proving or disproving it. Law enforcement agencies can use them in their work in the event of a crime, whether in the stages prior to initiating the criminal case or within the framework of the criminal case. They can also be used to predict criminal behavior, which enhances the opportunity to prevent crimes before they occur and to impose certain preventive measures, as some studies have concluded (Ali, 2023).

There has been a disagreement among contemporary legal schools regarding the authenticity of electronic evidence, regardless of its type. Legal perspectives on accepting evidence derived from computers and their peripherals can be divided into three main trends:

The first trend is the one that supports the acceptance of evidence derived from electronic devices. Some of the key foundations of this perspective include:

First: The principle of proof freedom, where most international laws state that crimes can be proven by any means of evidence. This serves the interest of the accused, who is granted the legal right to defend themselves using all available methods. It also benefits society, as this principle enables the identification of criminals and their presentation to the court using all available means of proof.

Freedom of proof necessitates protecting individual liberty from arbitrariness and oppression and avoiding wrongful accusations that result in injustice to the innocent. It also ensures that no offender escapes justice due to the lack of evidence of a particular type or quantity (Atiq, 2005).

Second: Computers and smartphones greatly affect proving and reducing crime. As long as criminals rely on scientific methods in committing their crimes, trying to escape justice, it has become necessary for justice agencies to use everything that would prove the facts and determine the nature of the crime. Limiting criminal evidence to specific types of proof makes the tools used to commit the crime precede the evidence proving it. This can reduce the effectiveness of achieving justice (Mish'sha', 2013).

Third: Relying on evidence derived from these devices prioritizes the public interest over individual rights. Although the exploitation of modern technology in criminal evidence might sometimes impact individual rights and freedoms, the public interest takes precedence over absolute individual freedom (Al-Hussaini, 2014). This aligns with the jurisprudential principle that individual harm can be tolerated to prevent greater public harm.

Fourth: The value of evidence often arises from the judge's conviction of its strength. Most legislations recognize the principle of the judge's personal conviction, which results in two main things: First, the judge's freedom to accept evidence that has a basis or relevance to the case file. Second, the evidence is subject to the judge's assessment after it is presented for public oral discussion (Bin Khalifa, 2014). Accordingly, the judge may rely on electronic evidence if it has risen to the level of considered evidence. He may also assess its probative value and issue a ruling based on that.

The second trend is a trend that rejects evidence derived from electronic devices. The most important pillars of their rejection are:

First, relying on evidence derived from devices violates the sanctity of private life, which is one of the most important basic human rights. Eavesdropping on private conversations and viewing films and photos recorded on the phone without the person's knowledge or consent is a clear assault on privacy. Legislations and laws have guaranteed the protection of personal privacy for all individuals (Mish'sha', 2013; Ben Mashri, 2018). For instance, prohibiting the use of mobile phones, considering it a repository of secrets, including recordings, photos, memories, video clips, calls, and private messages, from the principle of absolute protection of personal freedoms and privacy (Al-Hussaini, 2014).

Second, Crimes may only be proven by lawful means, even if that leads to the accused escaping, because preserving privacy is more important than using an unlawful means of proof (Al-Hussaini, 2014).

Third: Evidence derived from these devices is not conclusive. Electronic evidence, particularly from phones, is susceptible to forgery and manipulation due to significant advancements in software and applications that can alter or fabricate audio, images, and documents. Therefore, such evidence cannot be relied upon as long as it remains within the realm of uncertainty. Some laws have stated that it is not permissible to rely on audio evidence derived from recordings as independent evidence. It is considered a means of deception and fraud (Al-Hussaini, 2008).

The third trend is the mixed or conciliatory approach. This trend accepts this type of evidence as valid for criminal proof but establishes a set of criteria for accepting evidence derived from phones. These criteria include both legal and technical aspects.

As for the legal criteria:

1. Evidence must be used with the knowledge and supervision of the judicial authorities, with justification for the recording or extraction. This includes a statement of the evidence presented against the accused and its sufficiency and a statement of the benefit expected from the procedure.
2. The use of evidence must adhere to the legality controls and not deviate from them.
3. It should only be utilized in cases of serious crimes.
4. This evidence must be obtained by the person's free will, without deception, trickery or coercion (Al-Hussaini, 2014).

As for the technical criteria:

1. Ensure that the recording or image has not been altered.
2. The image must be clear.
3. The evidence must represent a complete picture of the incident or call without interruption from beginning to end. It must not have been exposed to factors of damage or poor preservation (Al-Hussaini, 2014; Al-Jaradat, 2022).

The Egyptian legislator recognized in Article (11) of Law (175) of 2018 the authenticity of digital evidence, as stated in the article: "Evidence derived from or extracted from devices, equipment, media, digital storage, information systems, computer programs, or any information technology means shall have the same value and admissibility as physical forensic evidence in criminal proof, provided that it meets the technical conditions stipulated in the executive regulations."

The second requirement Is providing electronic evidence of artificial intelligence and its problems.

Using AI techniques in this field is like using a technical expert in something he is proficient in. This means that evidence obtained through these technologies is considered indirect, as it often lacks direct evidence of the individual's commission of the crime or direct indication of the fact to be proven.

Proving a crime related to electronic evidence through artificial intelligence faces the same problems related to the authenticity of electronic evidence itself. Additionally, it introduces another problem related to the legal weight of evidence obtained through AI techniques and data analysis.

Some researchers argue that artificial intelligence techniques conflict more with privacy than other forms of evidence. This is because AI and data analysis often rely heavily on monitoring and tracking individuals' activities and detecting changes in their lives, usually without the person's consent or knowledge, which constitutes a violation of privacy.

Using artificial intelligence in data analysis can encroach on personal freedom and privacy, and its outcomes may conflict with digital privacy. Therefore, its use should be restricted by requiring a judicial order that specifies the reasons for employing this method. It must be subject to oversight and the reasons on which it was based by the court of subject matter. Thus, it is consistent with the guarantees guaranteed by constitutions and included in-laws (Ali, 2023).

Some legal experts believe that the authorities may use artificial intelligence techniques to extract sufficient evidence to prove the occurrence of a crime, limited only by the guarantees stipulated by general rules, such as not violating the sanctity of private life or personal freedom. Many countries have adopted the use of artificial intelligence techniques to detect crimes and track down their offenders (Al-Sharif, 2021).

Others argue that the legitimacy of using highly intelligent robots for evidence is not significantly different. There is no dispute about the permissibility of using modern technology in crime detection and evidence establishment, especially when robots are employed to analyze voiceprints from recorded data or retinal scans with greater speed and accuracy than traditional forensic lab methods (Sayed, 2021).

Some researchers argue that the issue at hand is not the legitimacy of using artificial intelligence techniques in proof but rather the legitimacy of allowing a robot to conduct inference or investigation independently without human intervention. They believe that this requires the intervention of the procedural legislator to solve this problem or frame it (Sayed, 2021).

Accordingly, is using artificial intelligence techniques to prove or disprove a crime permissible?

"The answer depends on the previously mentioned dispute regarding electronic evidence. Those who rely on the principle of freedom of criminal proof and the judge's personal conviction allow consulting experts in artificial intelligence to extract evidence of the crime's occurrence or disproving it."

Regarding basing a judgment on evidence derived from artificial intelligence techniques, some legal scholars believe that it is permissible for the court to use these methods, especially if it is impossible to obtain other supporting evidence (Ali, 2023).

The impact of the development of artificial intelligence technologies on trust in electronic evidence.

While artificial intelligence has positively impacted electronic evidence, there are also negative effects that may weaken its reliability. This is particularly true with the rise of deep fake technologies (Abdel Mola, 2023), which can replicate voices through voiceprints in a way that appears to be from the actual person. They can also superimpose a face on another person in a way that is very difficult to detect, leading to more caution when using these technologies and relying on them to detect audio or video recordings.

While some reports have noted that the results of artificial intelligence analysis are inconclusive. The analytical results are based on the database and algorithms that feed these results, and this data may be weak or biased (Al-Jabour, 2024), leading to inaccurate results (Al-Sharif, 2021)

One risk that may weaken the authenticity of evidence using artificial intelligence is that artificial intelligence systems are electronic programs that may be hacked, manipulated in programming, or manipulated in a biased manner to reach specific results (Al-Ahwal, 2013; Risks of Artificial Intelligence, 2017).

Some researchers have suggested ways to avoid deep fakes, including educating legal professionals and improving the efficiency of forgery detection methods by developing technologies that can detect forgeries before the evidence reaches the court. Also, supporting electronic evidence with additional proof, such as witness testimonies from those who observed the recorded event. Alternatively, technical evidence like verifying calls or recordings with telecommunications companies, allowing the defense to prove falsification in electronic evidence, imposing strict penalties for using fakes, and enhancing international cooperation to combat this phenomenon (Abdel Mola, 2023).

As for algorithmic bias, The RAND Corporation has confirmed that these algorithms have become a reality that cannot be ignored. There are other options available to deal with the current data deluge, especially in the field of crime prediction and investigation. The transparency of these algorithms requires instilling more awareness among users who are able to absorb artificial intelligence technologies and their capabilities to understand and comprehend their results (Al-Ajmani, 2023)

In short, despite the differences in schools of evidence, there are controls that govern evidence resulting from computers and their outputs – including evidence derived from artificial intelligence

– that the judiciary must adhere to to avoid misconduct and to support and protect the parties' rights. These controls center on the principle of innocence and its related consequences, which necessitate certain conditions for digital outputs. This ensures that the judge can verify that the digital evidence has not been tampered with before making a ruling of acquittal or conviction.

The principles governing the acceptance of digital outputs can be summarized in three principles:

1. Principle of Certainty of Digital Outputs: The Supreme Court of Oman supports this principle, which affirmed the principle of innocence in its ruling on Decision No. (50) in Appeal No. (22/2004) on 2/3/2004.

It stated: "It is sufficient for an acquittal to have reasonable doubt about the accuracy of the accusation against the defendant or due to insufficient evidence because the basic principle of human beings is innocence, and a crime is a form of abnormal behavior that deviates from the norm. Therefore, according to this fundamental principle, caution must be exercised in attributing it to a specific person (Al-Balushi, 2008)."

2. Principle of Requirement to Discuss Digital Outputs: This principle was adopted by the Supreme Court of Oman in its ruling on Decision No. (51/2004) on 13/4/2004.

It stated: "Every piece of evidence relied upon by the court in its judgment must have been presented orally in the session and subjected to oral discussion. The judge's conviction should be derived from the outcome of these oral discussions, not from written records. These rulings apply to digital evidence, meaning that digital outputs must be discussed and analyzed, whether printed or displayed on a computer screen, phone, or other devices (Ahmed, 2022)."

3. Principle of Legitimacy of Digital Outputs: This principle states that obtaining digital evidence must be lawful, including not violating the defendant's fundamental rights (Al-Nawafleh, 2010).

The executive regulations of the Information Technology Crimes Law No. 175 of 2018 in Egypt stipulate: "Digital evidence must be collected, extracted, preserved, and secured by judicial officers authorized to handle such types of evidence or by experts appointed by the investigating or judicial authorities. Additionally, the seizure reports or technical reports must specify the types and specifications of the programs, tools, devices, and equipment used. They must also document the code and algorithm resulting from extracting a duplicate copy of the original digital evidence in the seizure report or technical examination report, ensuring that the original remains unaltered (Article 1, Law No. 175 of 2018)".

CONCLUSION

Artificial intelligence has demonstrated remarkable progress in many fields, so it has become necessary to benefit from it in the field of crime and uncovering its circumstances. The development of artificial intelligence has significantly impacted providing new data that would help prove many crimes in which electronic evidence is used. Therefore, it is necessary to shed light on this revolution through study, research, legislation, and codification. The research has reached several results and recommendations, the most important of which are:

RESULTS

Artificial intelligence: It is the ability of a machine to simulate human behavior and perform functions and tasks that require experience and intelligence.

Electronic evidence: Any evidence derived from a machine, computer, or the like, whether it is documents, images, audio or visual files, or otherwise.

Artificial intelligence plays an advanced role in big data analysis. It has demonstrated remarkable progress in detecting facial and eye prints, and analyzing audio and visual media. This matter has become more accurate, speedy, and less risky than traditional computer programs.

There are concerns in many legal and legislative sectors about granting legal personality to robots.

Legal researchers are divided into three directions regarding the issue of using artificial intelligence techniques in proving evidence: absolute acceptance, absolute rejection, restricted acceptance, or the conciliatory direction.

Using artificial intelligence systems in electronic evidence may be considered as using a technical expert in a matter that he is proficient in.

Proving a crime using artificial intelligence techniques has the same ruling as proving a crime using traditional technical evidence. However, the problem lies in the weight of the evidence extracted through artificial intelligence techniques.

The research tends towards the conciliatory trend that sees the possibility of using artificial intelligence to prove electronic evidence, taking into account the general legal controls and rules for the course of justice and without infringing on freedoms and the private life of human beings.

The revolution in the development of artificial intelligence has had negative effects that may undermine confidence in electronic evidence. These include the spread of deep fake technologies, which create digital content that is difficult or impossible to distinguish from the original content. This includes the problematic issue of algorithmic bias.

If these technologies are adopted, there will be a set of controls based on the origin of innocence. The effects that follow are related to the weight of digital outputs in terms of certainty and legitimacy and the necessity of discussing them in court sessions.

Recommendations

The research recommends the following:

Develop comprehensive definitions for artificial intelligence applications used in the judiciary and the evidence derived from them.

Keep laws and legislations in line with the revolution in the use of artificial intelligence, in a way that achieves the interest and ensures the proper administration of justice.

Educate and train police and judicial personnel on the optimal use of these technologies and address their risks, especially in detecting deep fake techniques.

Continue research and work to find more effective solutions to the problems resulting from artificial intelligence technology, including the problem of algorithmic bias, which is considered a major challenge in this field.

REFERENCES

Abdel Mola, Muhammad Al-Sayed, 'The Negative Impact of Artificial Intelligence Developments on the authenticity of Electronic Evidence in Criminal Matters,' research published on the Electronic Encyclopedia of Protectors of Rights, December 26, 2023 (https://jordan-lawyer.com/2023/12/26).

Abdul Latif, Muhammad, Law of Evidence in Civil Matters, Modern Printing House for Printing, Publishing and Distribution, 1992. p. 6.

Abdul Muttalib, Mamdouh Abdel Majeed, Using TCP/IP Protocol in Researching and Investigating Computer Crimes, published on the Internet (Dpolice. Maktoobblog), accessed on: 12/12/2020.

Adel, Abdel Nour, Introduction to the World of Artificial Intelligence, 1st edition King Abdulaziz City for Science and Technology, Saudi Arabia 2005.

Ahmed, Amal Fawzy, Electronic Discovery & Digital Evidence Authority In proof between The Challenges of Acceptance and Information Security, Arab Democratic Center for Strategic, Political and Economic Studies, Berlin, Germany, First Edition, 2022.

Al-Ahwal, Ayman, and Al-Desouky, Ahmed, Contemporary Security Challenges of New Phenomena, Police Thought, Police Research Center, Sharjah Police General Command, Volume 22, Issue 86, July 2013.

Alai, Ammar Rashid, and Abdul Majeed, Muhammad Nour Al-Din. Using Artificial Intelligence Applications in Crime Prediction and Prevention, University of Sharjah Journal of Legal Sciences, Volume 20, Issue 37, 2023.

Al-Ajmani, Ahmed Abdel Wahid, and Said, Muhammad Noor El-Din, 'Legitimacy of Using Artificial Intelligence Techniques in Crime Investigation and Detection,' Sharjah University Journal of Legal Sciences, Vol. 20, No. 4, December 2023.

Al-Asyuti, Ayman Muhammad, Protect and Prove Legal Actions through the Application of Artificial Intelligence, Al-Baheth Al-Arabi Journal, Volume 1, Issue 1, 2020.

Al-Balushi, Rashid bin Hamad, 'Authenticity of Digital Outputs in Evidence,' a paper presented at the First International Conference on 'Protecting Information Security and Privacy in Internet Law,' sponsored by the International Association for Cybercrime Prevention in France, held from June 2 to 4, 2008, Cairo, Arab Republic of Egypt.

Al-Bishri, Muhammad, Digital Forensic Evidence: Its Concept and Role in Proof, a study in the Arab Journal of Security Studies and Training, Volume (17), Issue (33), Riyadh, April 2002.

Al-Hussaini, Ammar Abbas, 'The Legality of Mobile Phone Recordings as Evidence in Criminal Proceedings: A Comparative Study,' Al-Ahl al-Bait Journal, Faculty of Law, University of Babylon, Issue 8, 2008.

Al-Hussaini, Ammar Abbas, Visual Imaging and its Evidence in Criminal Evidence, Journal of the College of Law, University of Nahrain, Volume 16, Issue 1, 2014.

Ali, Rizk Saad, Using Artificial Intelligence and Data Analysis Techniques in Detecting Crimes, Journal of Legal and Economic Studies, A Refereed Scientific Journal, Faculty of Law, Sadat City University, Volume 9, Issue 3, 2023.

Al-Jaafari, Badr bin Abdullah, The Validity of Electronic Evidence in Commercial Disputes, Evidence Means Forum, Al-Ahsa Chamber of Commerce and Industry, 2013.

Al-Jabour, Ridwan Saleh, 'Algorithmic Bias and Favoritism in Artificial Intelligence,' article on LinkedIn. Accessed on June 27, 2024 (www.linkedin.com).

Al-Jamali, Tariq, Digital Evidence in Criminal Evidence, a working paper submitted to the First Maghreb Conference on Information Technology and Law held on 28-29-10/2009.

Al-Jaradat, Dhurgham Issa, Jurisprudential Rulings Related to the Use of Smartphones, Dar Al-Bashir, Emirates, 1st ed., 2022.

Al-Jazzar, Saadia, The Extent of Considering Audio Recording as a Modern Method of Proof: A Jurisprudential Study in Light of the Use of Artificial Intelligence Technology, Al-Azhar University Journal, Research Extracted from the First Issue 2/3 – Issue 39, 2024.

Al-Khanin, Abdullah bin Muhammad, Description of Judiciary in Islamic Law, 1st edition, no publisher, 2003.

Al-Mahdi, Hussein bin Muhammad, 'The Evidentiary Power of Electronic Transactions,' Judicial Research Journal, Republic of Yemen, Issue 7/200, 2007.

Al-Matradi, Miftah Abu Bakr, Electronic Crime and Overcoming Its Challenges, a research paper presented to the Third Conference of the Presidents of the Supreme Courts in the Arab Countries in the Republic of Sudan, held from 23 to 25 September 2012.

Al-Nadawi, Adam Wahib, 'Explanation of Evidence Law,' Al-Qadisiyah Press, Baghdad, Iraq, 2nd edition, 1976.

Al-Nawafleh, Youssef Ahmed, Digital Evidence, PhD Dissertation, Faculty of Law, Alexandria University, 2010.

Al-Qarafi, Ahmad bin Idris, Sharh Tankeh Al-fusool, United Technical Printing Company, First Edition, 1973.

Al-Sayed Muhammad, Hassan Abdel Fattah, 'Electronic Facial Recognition as a Means of Evidence from an Islamic Jurisprudential Perspective,' Annual of the Faculty of Islamic and Arabic Studies for Girls in Zagazig, Al-Azhar University, Egypt, 2016, Issue 6.

Al-Sharif, Mahmoud Salama Abdel Moneim. The Legal Nature of Predicting Crime Using Artificial Intelligence and Its Legitimacy, Arab Journal of Forensic Sciences and Forensic Medicine, Naif Arab University for Security Sciences, Saudi Arabia, Vol. 3, No. 2. 2021.

Arnous, Bashir, Artificial Intelligence, Dar Al-Sahab Publishing, Cairo, 2007.

Article 1 of the Definitions in the First Chapter of Law No. 175 of 2018 on Combating Information Technology Crimes.

Artificial Intelligence article, on the Nokta website of the Arab Scientific Community. (https://nok6a.net/categoryA), accessed on 14/6/2024. An article entitled Artificial Intelligence, Royal Care and Bahraini Leadership towards the Future, Haifa Adwan, was published on the Bahraini Al-Watan newspaper website. (https://alwatannews.net/article/859995/Opinion), accessed on: 3/6/2024.

Artificial Intelligence article, on the Nokta website of the Arab Scientific Community. See the article on artificial intelligence on the Tumoohi website for universities. https://www.tumoohi.org/ar/majors), accessed on: 13/6/2024. Al-Hussaini, Osama, Logo Language, Ibn Sina Library, Riyadh, 1st ed., 2002.

Artificial Intelligence in Education, an article on the Mabarrat website. (http://www.mabarrat.org.lb/Blog/4268). Accessed on: 10/6/2024.

Atiq, Al-Sayed Muhammad Saeed, 'General Theory of Scientific Evidence in Criminal Proceedings,' PhD Thesis, Faculty of Law, Cairo University, Egypt, 2005.

Ben Mashri, Abdel Halim, The Reality of Human Rights Protection in the Algerian Penal Code, Legal Forum Magazine, Faculty of Law, University of Mohamed Belkheder, Biskra, Issue 5, 2018.

Ben Younes, Omar, Crimes Arising from the Use of the Internet, PhD Thesis, Faculty of Law, Ain Shams University, Egypt, 2004.

Bin Khalifa, Ilham Saleh, The Role of Fingerprints and Other Physical Traces in Criminal Evidence, Dar Al Thaqafa for Publishing and Distribution, Amman, Jordan, 2014.

Cybersecurity and Artificial Intelligence Study in Saudi Arabia, article on Easy Uni website: (https://www.easyunime.com/advice/A9-2817), accessed on: 25/6/2024.

Egyptian Law No. 175 of 2018 on Combating Information Technology Crimes. Abdul

Generative Artificial Intelligence, Concept, Opportunities and Risks, Article on Argaam– Reuters – Tech Target – Forbes, published on: 7/6/2023. (https://www.argaam.com).

Hamouda, Ali, Evidence Obtained from Electronic Means within the Framework of the Evidence Theory, presented in the proceedings of the First Scientific Conference on the Security and Legal Aspects of Electronic Operations, organized by the Dubai Police Academy on 4/26/2003.

Hijazi, Bayoumi, Criminal Evidence and Forgery in Computer and Internet Crimes, Dar Al-Kotob Al-Qanuniyah, 2004.

Ibn Abd al-Salam, Izz al-Din Abd al-Aziz, Qawaid Al-ahkam , Al-Azhar Colleges Library – Cairo, 1991.

Ibn Abidin, Muhammad Amin, Hashiyat Radd al-Muhtar, ala al-Durr al-Mukhtar: Sharh Tanwir al-Absar, Mustafa Babi Halabi Library and Sons Press, Egypt, 2nd edition, 1966.

Ibn Iyad, Iyad bin Musa, Mashariq al-Anwar Ala Sihah Al-Athar, Al-Maktaba Al-Atiqah and Dar Al-Turath, No edition, No date.

Ibn Manzur, Muhammad bin Makram, Lisan al-Arab, Dar Sadir, Beirut, 3rd edition, 1994.

Ibn Sidah, Ali bin Ismail, Al-Muhkam wa Al- muhit Al-a'zam, Dar Al-Kotob Al-Ilmiyyah- Beirut, 1st edition, 2000.

Ibn Sidah, Ali bin Ismail, Al-Mukhassas, Dar Ihya' Al-Turath Al-Arabi, Beirut, 1st edition, 1996 AD.

Ibrahim, Khaled Mamdouh, Electronic Evidence in Criminal and Civil Matters, Dar Al Fikr Al Jami'I, Alexandria, 2020, an article published on his official website (https://kenanaonline.com/users/KhaledMamdouh/posts/77859), accessed on: 6/6/2024.

Izz Al-Din Ghazi, Artificial Intelligence: Is it a Symbolic Technology? Journal of Thought in Humanities and Social Sciences, Faculty of Arts – Fez, vol 6, 2007.

Jihad, Ahmed Afifi, Artificial Intelligence and Expert Systems, 1st ed., Amjad Publishing and Distribution House, Amman, Jordan, 2014, p. 14.

Khawaled, Abu Bakr, et al., Artificial Intelligence Applications as a Modern Trend to Enhance the Competitiveness of Business Organizations, Arab Democratic Center for Strategic, Political and Economic Studies, 1st edition, Berlin-Germany, 2019.

Kuwaiti Jurisprudence Encyclopedia, Ministry of Awqaf, Kuwait, Edition: (1404 – 1427 AH).

Majmoo' al-Fatawa (35/394-395), I'lam al-Muwaqqi'in (1/90), al-Turuq al-Hukmiyyah (pp. 15-32-302).

Marqus, Suleiman, Principles of Evidence and its Procedures in Civil Matters in Egyptian Law Compared to the Techniques of Other Arab Countries, Alam Al-Kutub for Printing, Publishing and Distribution, 1981.

Mish'sha', Moatasem Khamis, Proving Crime with Scientific Evidence, a research paper in the Journal of Sharia and Law, College of Law, United Arab Emirates University, Year 27, Issue 56, October 2013.

Muhammad, Asmaa Al-Sayed Muhammad, and Muhammad, Karima Mahmoud, Artificial Intelligence Applications and the Future of Educational Technology, Egyptian National Library, 2020.

Mukhtar, Ahmed Abdel Hamid Omar, with the assistance of a work team, Lexicon of the Modern Arabic language, Alam Al-Kutub, 1st edition, 2008.

Musa, Abdullah, and Bilal, Ahmed Habib, Artificial Intelligence: A Revolution in Modern Technologies, Arab Group for Training and Publishing, Cairo, 1st ed., 2019.

Nasser bin Abdullah, an article on the Omani electronic newspaper, published on 6/2/2017 (https://www.omandaily), accessed on 6/17/2024.

Risks of Artificial Intelligence on Security and the Future of Work: An Analytical Perspective, published by RAND Corporation, 2017, p. 6. (https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE237/RAND_PE237z1.arabic.pdf).

Sayed, Muhammad Nour El-Din, Security Challenges in Using Artificial Intelligence and Digital Systems for Security Work and Ways to Confront Them, Police Sciences Academy, Sharjah Police General Command, 2021.

Shams El-Din, Ashraf Tawfiq, Electronic Criminal Evidence, Dar Al Nahda Al Arabiya for Publishing and Distribution, Egypt, 1st ed., 2021.

Yasser, Ammar, and Al-Babli, Zuhair, 'The Role of Artificial Intelligence Systems in Crime Prediction,' Police Thought Journal, Sharjah Police General Command, Police Research Center, Vol. 28, No. 3 (July 31, 2019).