ITJ | The International Tax Journal

# International legislative obstacles related to artificial intelligence

**Mr. Mentalecheta Chafik** [1]

[1] Lecturer "B", Faculty of Law and Political Science, University of Lounici Ali – Blida 02 (Algeria).
c.mentalecheta@univ-blida2.dz

**Abstract---**This study gains its importance from its approach to artificial intelligence from the perspective of the negative side related to cybercrime and its impact on the components of society. In the face of this new type of crime, current national penal laws do not appear as adequate or effective as required.

**Keywords---**international dimension, artificial intelligence crimes, comparative legislation.

## Introduction

To be sure, in addition to the peaceful or useful uses of computers, the incredible advances in artificial intelligence have led to crimes resulting from its various applications. These crimes may consist either in attacks on the computers themselves, or in criminal acts carried out using computers as a tool in the hands of the offender to achieve his criminal purposes.

Due to the high rate of AI-related crime, developed countries have begun to develop special criminal laws to counter this new phenomenon in criminology. These include the United States of America, France and other EU countries that developed a convention on computer crime in 2001. This Convention recommended that Members take all legislative or other measures as needed to make illegal access to computer systems or any part thereof a crime in accordance with domestic law. The Convention also included A set of general principles on international cooperation in criminal matters and established procedures for dealing with requests for mutual assistance between Member States in the absence of international conventions.

With this, the world has been transformed into a small village, and this village full of information has become the focus of attention of all legitimate and illegitimate interests. The effects of artificial intelligence are beginning to appear comprehensively on the administrative, economic, social, political,

**How to Cite**:
Chafik, M. (2025). International legislative obstacles related to artificial intelligence. *The International Tax Journal*, *52*(4), 1247–1261. Retrieved from https://internationaltaxjournal.online/index.php/itj/article/view/143

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370 © 2025

Submitted: 03 January 2025 | Revised: 17 June 2025 | Accepted: 18 July 2025

cultural and legal structure of states. Every scientific invention opens up new horizons and produces effects that did not exist before its emergence and spread. Therefore, it was necessary for the law to intervene, as it regulates with its various rules all aspects of life.

This study gains its importance from its treatment of artificial intelligence from a negative aspect related to information crimes and their impact on the components of society. In the face of this new type of crime, national penal codes in their current state do not appear as adequate or effective as required or hoped, as their texts and the legal theories and principles they contain or stand behind date back to the nineteenth century. Therefore, cooperation between States is an urgent necessity to combat this new type of crime that has crossed borders to affect several countries and societies, taking advantage of the great progress in modern technology for communication and transportation. This requires enhanced cooperation and effective measures to curb, eliminate and punish the perpetrators.

**What are the different mechanisms for the procedural and legislative aspects of Arab and international legal control against artificial intelligence crimes?**

**The first topic**: **General provisions for artificial intelligence crimes**

Cybercrime: Definition and Development Criminal jurisprudence traces its roots back to the 1960s. [1] As for AI crimes, it can be said that they began in 1988. The first Internet-related crimes were the crimes of aggression historically known as the first viral crime, known as the Morris worm, which occurred on November 2, 1988. Jurisprudence and comparative laws still have difficulty distinguishing between computer crime and those resulting from the use of the Internet, to the extent that the 1995 United Nations Crime Reduction Report adopted this comparative position. Released under the title "Computer Virus".

Therefore, we find that the concept of computer crimes in jurisprudence and legislation combines crimes that target the computer itself and those in which the computer is used as a tool for its implementation. According to this concept, crimes are seen as "illegal acts related to the computer system, whether the computer is the object of the crime, the means of its execution, or the source of evidence related to it". This definition derives from the most well-known definition of computer crime, presented by Professor Dot Berker, who stated that computer crime "requires accurate computer knowledge in order to The crime succeeds."[2]The European Convention on Cybercrime, dated 22 November 2001, did not provide a specific definition of cybercrime, only recognizing a certain type of crime that can be committed online.

**First: What is artificial intelligence?**

Without a doubt, AI applications continue to evolve and expand in aspects of our daily lives gradually. This can be seen through how our phones interact with images, or through artificial intelligence software such as Apple's Siri app, Samsung's Pixby, or even Alex and Google Voice Search and many other applications. There are also computers used in modern cars that use artificial intelligence applications to determine weather conditions, detect roads, and know how much fuel is left, as well as its uses in video games. All these applications represent examples of the remarkable global progress in the arena of artificial intelligence.[3]

---

[1] (SIEBER) Dr. Ulrich Computer and Other IT Crimes Rev. inter.de droit penal 1991 p. 1033

[2] Voir site : Temp (Royal Canadian Mounted Police) "Computer crime is any illegal act involving computer systems whether a computer is a crime crime, a tool used to commit a crime, or a response available on the Internet in the crime of February 2000." Relevant Guide http://www.rcmp.com (Mac D. Rush - Criminal Law and the Internet - Internet and Society. © Copyright 1996 by the Computer Law Association, in: Inc. p.6, donn parker of Sri , is necessary for the successful commission of crime.

[3] Abdel Razek Mukhtar Mahmoud, Applications of Artificial Intelligence, Introduction to the Development of Education in Light of the Covid-19 Pandemic, International Journal of Research in Educational Sciences, Vol. 3, No. 4, 2020, p. 207.

The words "intelligence and artificial" in language and terminology can be addressed as follows:

**1- The concept of intelligence language:**

- **In language and terminology**

Intelligence: Speed of discernment, from your saying: intelligent heart and intelligent boy: if he is quick to discern, and has intelligent - broken - intelligent intelligence. It is said: Zaki is intelligent, and Dhaka is intelligent.

- **Intelligence idiomatically:**

Al-Manawi said: Intelligence: "speed of perception, unity of understanding."[4]

- **Artificial language**

Synthetic common law: a name attributed to an artificiality which was made, unnatural artificial silk.[5]

**Artificial artificial roses idiomatically**

Artificial intelligence is the act of continuous effort with the aim of achieving certain results. If we consider AI to be nexus-based automation, here are three additional perspectives on what constitutes AI. It is important for education professionals to be aware of these divergent views when evaluating educational technologies involving AI. One useful list of AI terms for education is the AI Glossary for Teachers[6]. So, AI is not just one thing, it is an umbrella term that combines a growing set of modeling capabilities. [7]

The vast cultural awareness of artificial intelligence can be traced back to the extraordinary film "2001: Space Odyssey" – where the algorithm-programmed computer Hal communicates with astronaut Frank. Hal helps Frank guide the journey through space, a task Frank cannot accomplish alone. However, Frank ends up outside the spacecraft and Hal takes over, which does not yield positive results for Frank. Hull reflects human-like behaviors such as perception, speech and behavior as in all AI applications, It can be helpful to humans but it also carries unexpected risks – especially since the ways AI is perceived are different from those of humans.

The "human-like" concept is that computers now possess skills that may be very different from the capabilities of older educational applications. Educational applications can interact with students and teachers, participate in how activities develop in the classroom, and make decisions that affect both students and teachers broadly. There will be opportunities to do things in much better ways than we do today, and we will face risks that should be anticipated and dealt with. However, reducing it to "human-like intelligence" is not always beneficial, due to the nature of artificial intelligence. Information is processed differently than how people process information, and when we transcend the differences between individuals and computers, we may put in place AI policies in education that don't hit the target.[8]

AI is also an algorithmic view aimed at achieving a specific goal, as it relies on any computational method implemented independently."[9]

---

[4] Al-Durar Al-Sunni website Accessed 25-03-2025
%84%D8%A7%D8%AD%D8%A /2268/https://dorar.net/alakhlaq

[5] Dictionary of meanings available on the internet https://www.almaany.com/ar/dict/ar-a؟ Accessed November 20 , 2024.

[6] . Cardona, Artificial Intelligence and the Future of Education, USA, (2) Miguel Office of Educational Technology, May 2023, p.13

[7] A Regona, Massimo & Yigitcanlar, Tan & Xia, Bo & Li, R.Y.M. (2022). Opportunities and Challenges of Adoption in the Construction Industry: A PRISMA Review. Journal of Open Innovation Technology Market and Complexities, 8(45). https://doi.org/10.3390/joitmc8010045

[8] Miguel A. Cardona, Artificial Intelligence and the Future of Education, Reference, Reference, Reference, P13

[9] Friedman, L., Blair Black, N., Walker, E., & Rochelle, J. (November 8, 2021) Al in Education Secure Needs You. Association of Computing Machines https://cacm.acm.org/blogs/blog-cacm/256657-safe-ai-in-education- Blog, Need You/ Full Text

This definition highlights AI systems and tools that identify patterns and select actions to achieve a specific goal. These abilities will be used to recognize patterns and provide automated recommendations in ways that affect the learning process, including student learning and teacher decision-making. For example, current personalized learning systems may be able to detect signs of problems in a student and may recommend an alternative learning plan. Pattern recognition and automated recommendations will expand further.

To achieve goals, our human abilities are based on understanding multiple contexts. For example, a teacher may observe three students making the same mistake in mathematics, but realize that one is following an individual education program to treat vision problems, another understands the mathematical concept and the third suffers from frustration caused by unsuccessful interactions on the field, so the same educational decision is not suitable for everyone. However, AI systems often lack the data and judgment needed to adequately embed context as they detect patterns. and automate decisions. Furthermore, case studies indicate the ability of technology to quickly deviate from the safe path to the unsafe or from effective to inefficient even at a slight change in context. These and other reasons make people's involvement essential in setting goals, analyzing patterns, and making decisions. [10]
Augmented intelligence is a design style that involves collaboration between humans and artificial intelligence to improve cognitive performance, including learning processes, decision-making, and new experiences.[11]

AI models are similar to financial models. Realistic analysis is useful for identifying patterns, making predictions, or studying alternative options in a typical middle school math curriculum, where students use a mathematical model to compare the two cell phone purchase plans and which is better. Financial planners use these models to guide the composition of a retirement portfolio. At its core, AI is a sophisticated set of mathematical tools used to build models and use them practically. In well-known chatbots, complex articles are written word by word at a time, with the AI model predicting the next words that may follow the written text so far.

Smart chatbots use a huge statistical model to predict the next word every time, producing amazingly consistent articles..[12]

**Second: The evolution of the legislative structure for artificial intelligence crimes**
The US Department of Justice has expanded the link between computers and its technology, going to define computer crimes as "any aggression committed against any law that includes computer technology in its content and is subject to investigation and accusation."[13]

This was, of course, influenced by the trends of the American legislator in the 1996 amendment to the National Information Infrastructure Law, Section (10), which was inspired by criminalization from the link between the computer and its technology as a whole, and this trend resulted in the existence of three types of artificial intelligence crimes that enable the computer, according to the American curriculum,[14] namely:

---

[10] Russell, S. (2019). Compatible with human: artificial intelligence and the problem of control. Viking. ISBN978-0-525-55861-3 .
[11] Gartner (n.d.) Gartner Glossary: Augmented Intelligence. Gartner: https://www. Intelligence
gartner.com/en/informationtechnology/glossary/augmented-
[12] Miguel A. Cardona, Artificial Intelligence and the Future of Education, Reference, Reference, Reference, p20
[13] Scallion) Robert
Cybercrime, Fall 1996, p. 1. "Accountability offence is any violation of the law involving knowledge of computer technology to be committed, investigated or prosecuted" available online in February 2000 at:
http://wings.buffallo.edu/complaw/complawpapers/scalion.html
-THOUMYRE - VIOLATIONS IN CYBERSPACE, OP. CIT. p. 7
[14] It is noted that this division was developed by Prof. Dr. Jamil Abdel-Baqi in his book - Crimes arising from computers - a report submitted to the Sixth Conference of the Egyptian Society of Criminal Law - Dar Al-Nahda Al-Arabiya, Cairo, 1996.

**The first type:** crimes for which the computer is a target, which is a type of crime in which the goal of the criminal is to reach the theft of data from the computer or cause damage to it, its operating system, or the network through which it is committed.

**The second type:** crimes that the computer is a means of committing These forms of crimes occur when the offender exploits the computer to facilitate the implementation of some traditional crimes such as bank fraud. A bank employee used currency conversion software to his advantage, depositing transferred amounts into his account instead of putting them on track. He also prepared, transported or possessed a machine, including a computer, with the intention of using it to forge identity documents. Some laws have expanded the definition of "counterfeiting tools" to include computers, components, and software, if they are specifically designed for forgery purposes, as in New Jersey law.

**Type III:**
Crimes in which the computer is a tool for preserving evidence without being an intermediary in obtaining it, as is the case in drug dealers and illicit trafficking, as well as the producers of software that infringes on property rights, as well as electronic theft that is carried out as an infringement on copyright, placing their thefts, files and records in the computer. It should be noted that such a previous division is not inclusive of the expression of artificial intelligence crimes, as there are crimes that are committed By computer, it cannot be included in any of the three sections or forms, as[15] is the case with the crime of stealing computer time, for example, a crime defined by Section 641 of the US Code as an information crime[16]. It is possible that the previous expansion was the result of the lack of clarity of the computer's capabilities to the required amount. Much less we know about his capabilities than we know about the Internet's. The latter, frankly, did not take its share as it should, yet politicians and legal scholars addressed it The economy at the regional and international levels is passionately though it is still in its early stages, while the computer path seems calmer or naturaler. This situation had a clear impact in the European Convention on Cybercrime of 22-11-2001, where the first article of that Convention recognized the term "computer system" and not limited to the mere definition of "computer". Rather, this agreement defined this term as it includes any device or group of devices linked to each other, which by adding certain programs to one or more of them can process data automatically.[17]

Thus, some legal unionists tend to create discrimination in this context, in terms of defining AI crimes separately from computer crimes, as crimes resulting from the use of the Internet. The definition is based on a deep understanding of the nature of the case, including the need to distinguish between these two types of crimes. The Internet has produced new criminal images that were not known even within the context of computer-related crimes, as a result of the emergence of the Internet, it is not only about the coordinates of discrimination within the The scope of computer crime, but goes beyond the complexity (e.g., artificial intelligence crimes) as well as the details associated with computer crime and

---

[15] Jamil Al-Saghir - Crimes Arising from the Use of Computers, Cairo, Dar Al-Nahda Al-Arabiya, p. 23.

[16] UNITED STATES V. SAMPSONM, 6 COMP, L. SERV. REP. 879 (N.D. Cal. 1978)
In the present case, the Court considered that the unauthorized use of a computer in a government institution constituted an offence of aggression against government property as prescribed in section 641 sec referred to - see also in respect of section 641 cited:
18 USC and 641. See: United States v. Friedman. 445 F. 2d 1076, 1087 (9th Cir.) (The theft of grand jury minutes and the information contained therein was theft of government property.) The certificate was rejected. 404 U.S. 958 (1971) United States v. Morison, 604 F. Supp. 655, 663-65 (D. Md. 1985) ("theft" of confidential information supports a conviction for embezzlement); United States vs United States. DiGillo, 538 F. 2d 972 (3d Cir). The certificate was rejected. 429 US 871 (1971) (theft by photographing sufficient government records to support and 641 advocacy): United States v. MeAusland, 979 F.2d 970 (4th Cir. 1992) (theft of confidential bid information of the competitor violates & 641).

[17] Article 1 Definitions: "For the purposes of this Convention: devices connected to a computer system or related devices, a single device or intended for any internal device or group, according to a program, performs automatic data processing" Computer-related offences

other matters[18]. Perhaps the negative development that we see in the recommendations of the (Big Eight) conference in 1998 calls for further reflection in this regard, as the term high-tech or advanced crimes was reached as a kind of attempt to expand computer crimes to include all crimes in which the computer is a party. And this All of it makes us decide that there is an artificial paradox between computer crime and cybercrime, despite the almost natural adhesion between them.
This approach we follow is based on a jurisprudential rooting that seeks to establish its foundations on a basis that guarantees the interest of man before technology. According to this trend, cybercrime is defined as "any intentional act or omission resulting from the illegal use of information technology and aimed at attacking material and moral property." Although this analysis is correct for the definition of AI crimes as mentioned earlier, especially as it highlights the necessity of intentionality, this vision was groundbreaking. According to the views of the European Crime Convention Electronic dated 22-11-2001, this definition is criticized, as it requires abstention as a material activity in such crimes, which is difficult to imagine in the context of this issue.

**Third: What are artificial intelligence crimes?**
AI crimes can be defined if we take into account three main points, and in light of them, an integrated definition can be developed that is useful in identifying crimes arising from the Internet.

**The first point: the** subject of the virtual world, which is the visual world or the vital field of data and its information movement, which is the world that disappears in the technical machine[19]. Arabic jurisprudence calls cyberspace[20]. It is the world whose idea was invented by the famous science fiction writer in his famous novel, which he published in 1948, where he described in this book an electronic [21]fantasy It meets a hacker group of computer skilled people, as long as their activity is hacking and many manifestations that sometimes almost reach the logic of online crime as well as contemporary legislation.

If the law of the virtual world, the Internet, is not an obstacle in the framework of building its theory - if efforts can be intensified at least theoretically - this is not the case with regard to the application and implementation of this theory, especially in the judicial sphere. The composition of the law of the virtual world, the Internet, is in fact different from the composition of any other law, as it consists of a hypothetical nature with an international dimension[22]. This is in line with the concepts of globalization rather than those defined by international law, as it extends to other branches of law. This is because the term comparative jurisprudence rushes to Balqar has sought to develop serious ramifications of this term.

The process of harmonizing the existing legal system with the Internet had emerged at the beginning when the relative jurisprudence agreed on the possibility of legal dealing with the Internet in the manner of psychological regulation of the Internet, so that this regulation should not be the only tool, but rather accepts, in addition to the legal regulation with the legislative tool, the existence of regulatory tools

---

[18] Network Prof. Dr. med. Henrik W. K. Threats and Opportunities Criminal Perspective, p. 258. Five European criminal justice cases: corruption, women in the criminal justice system, criminal policy indicators, community crime prevention and cybercrime procedures of the Sixth European Symposium on Crime and Criminal Policy, Helsinki, 10-12 December 1998, European Institute for Crime Prevention and Control, United Nations Affiliated (HEUNI), P.O. Box 161, f. 00131 Helsinki Finland Publication Series No. 34 - Thumir
- Abuses in Cyberspace, op. cit., p. 10
[19] RCMP, op. cit.
[20] Jamil Abdel Baqi Al-Saghir, Substantive Provisions for Internet-Related Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 1999, p . 04.
[21] ) (Nicholson) Keith - International Computer Crime: A Global Village Under Siege - New England International and Comparative Law Annual 1996 - New England School of Law P. I. Available online September 2001 at: http://www.nest.edu/annual/vol2/computer.htm
[22] The transient nature of cyberspace, (cybercrime and the old law of global cyber punishment< information p. 2 Report by: McConnell International http://www.mcconnellinternational.com
of support provided http://www.witsa.com December 2000 available online in December 2000, at: http://www.mcconnellinternational.com/services/cybercrime.html

stemming from the nature of the Internet, i.e. information technology, and the reason for rejecting the self-regulation unit as a legal system for the Internet lies in the fact that self-regulation is not convincing enough.[23] This makes the virtual world secure enough to allow security and stability."[24]

It is not as simple as it seems, given the opposite trend that calls for the need for legal intervention to regulate the digital space, as it also faces challenges, the most important of which is determining the nature of the legal system that regulates the Internet. Are the basic systems of the state sufficient to address these challenges or did the virtual world arise suddenly and therefore have to have a foundation within the current legal systems? The problem is that the legal mind has not yet explored this basis. It just takes more Time, deep reflection and legal wisdom.

**The second point** is that this concerns the separation of computer-related crime from cybercrime, and the extent to which this is technically achievable. In fact, it is very difficult to separate computer crime from cybercrime because of the close technical connection between them. However, this difficulty may be significantly reduced if we realize that computer technology is much more extensive than Internet technology. Computer technology has spawned the Internet, but that doesn't mean the end in this area. Current indicators suggest that computer technologies New ones will appear soon. To illustrate this, countries like Canada where cybercrime is linked to telecommunications crimes that can be committed over the Internet (as well as over phone, radio, satellite, etc.).[25]

The expansion is likely to move towards a broader definition of AI crime, where autonomy is sought for its own in line with its non-computer connectivity and its effects. As we have already defined the Internet as a means of communication between networks, this is the prevailing trend of EU legislators in the Convention on Cybercrime of 11-11-2001, and it is also the orientation of US legislators when using the term digital crime. If we consider that the division of this network into three parts, as we mentioned earlier (information network Global – Email – Direct Contact) is the best, it is correct to criminalize aggression that takes place over the Internet using its sections, so cybercrimes are actually those committed using means of communication between networks.[26]

Based on this principle, the specific vision of the Internet is based not only on theoretical thought, but also on practical reality. This requires studying the extent to which society accepts it intellectually, as it is a vital area of society to which its mentality can be linked. In some countries that have experienced real life with the Internet, they have been able to create positive interaction associated with Internet law, such as in the Philippines, where a university student created a love virus. The state responded by intensifying its efforts to develop a law on This is especially after the international intervention as a result of the spread of harm across international borders and infected many computers around the world[27]. The actual world is an inseparable part of our world, so it is not far from the possibility of legal regulation of it. Rather, jurisprudence advocates a single mental being of the Internet , based on the principle of universality of thinking and regionalism of movement.[28]

**The second topic**: obstacles **associated with the legislative adjustment of artificial intelligence crimes**

The most important characteristic of AI crimes is the difficulty of detecting and proving them, in addition to the special subjectivity of evidence collection procedures in this field. [29]

---

[23] RCMP, op. cit.
[24] Cybercrime and Cyber Punishment Information, op. cit., p. 2
[25] FGSSC - Available online in February 2000 at: http://www.usdoj.gov/criminal/cybercrime/search docs/toc.htm
[26] Cybercrime and Computer Publishing Information - op. cit. - op. cit. - P.4
[27] Rcmp op-cita Computers and telecommunications explode in the next century Prosecutors and prosecutors face a new type explosion in the next century Prosecutors and prosecutors have begun to face a new kind of problem
[28] Thoumyre - Abuse in Cyberspace op. cit. P.9 Think globally and act locally
[29] Muhammad Zaki, Evidence in Criminal Matters, p. 16.

**First: Obstacles to Proof of Artificial Intelligence Crimes**

Crimes committed on computers and information networks are invisible in many cases.[30] Where the victim often does not notice or realize their occurrence. Concealing the behavior that constitutes them and obliterating or covering their results by invisible manipulation of the electronic pulses or vibrations through which the data is recorded is not impossible in many cases by virtue of the availability of knowledge and technical expertise in the field of computers by the perpetrator[31]. Embezzlement of money by manipulating computer programs and contents, often in Computer outputs cover it and cover it. Spying on the data file was an error that came from software, hardware, operating system, or the overall design of the information system. As a result of this difficulty, the possibility of concealing AI crime by manipulating data has become a term used in American criminological research (the non-primary nature of printed computer output).

**Second: Obstacles to Evidence of Artificial Intelligence Crime**

The most important obstacles associated with evidence of AI crimes are as follows:

**1- Lack of visual evidence**

It is noted that the evidence resulting from information systems about the crimes committed against them or through them are only invisible data that we do not disclose a specific personality, and these data are recorded electronically very heavily and in a coded form[32]. Often on props or media for storage, whether optical or magnetic, that cannot be read by humans, even if they are readable by the machine itself, and modification or manipulation does not leave any trace, which severs any link between the criminal and his crime and hinders or prevents the detection of his identity[33]. One of the main challenges faced by the authorities concerned with investigation and prosecution is the detection and collection of evidence to prove the crime and identify the perpetrators. This problem generally appears in all areas of automated data storage and processing, where The responsible cadres of these entities lack the ability to directly examine suspicious data. The magnitude of this problem is especially high in cases of manipulation of computer programs, because it requires thorough scrutiny of the program and the discovery of illegal instructions hidden within it, which consumes a lot of time and effort[34].

---

[30] This type of crime takes place in an environment where transactions do not depend originally on documents and written documents, but on invisible electronic pulses that can only be read by computer and data that can be used as evidence against the perpetrator can be tampered with in less than a second or completely erased, so coincidence and misfortune play a role in discovering them that exceeds the role of audit and control methods, and most of the perpetrators, who were caught, according to what one of the experts observed, either acted stupidly or they did not use information systems skillfully: see:
John Eaton and Jeremy Smithers, that's it. Amangagrs Guide to Information Technology, London, Philip Allan, 1982 p.263
Referred to Hisham Mohamed Farid Rostom, research presented to the Conference on Law, Computer and the Internet from 1 to 3 May 2000 at the United Arab Emirates University entitled Information Crimes).

[31]
Jay, J. Baker Computer Crimes Trial (1980), 2 Computer Law, Journal 441
Referred to by Dr. Hisham Mohamed Farid Rostom, previously referred to.

[32] Technical difficulties are related to the encryption methods used on the network.
Computer Criminamite Online, p. 58

[33] Ulrich, Sabre, ibid., p. 140

[34] Demonstrating the impact of the absence of visual evidence in obstructing the arrest procedures and prosecuting the perpetrators of crimes committed in the field of information technology, Professor Sieber refers to a real situation witnessed by the former Federal Republic of Germany in 1971, which is summarized in the discovery of a mail order firm that stole magnetic tapes belonging to it containing 300,000 addresses of its currencies and enabling it to obtain a court order. Known as business stoppage, injuction to recover all addresses from a competing company that had obtained these addresses from the perpetrators of the theft, and in implementation of this order, the competing company allowed to help the execution officer enter its headquarters and computer center, where he found himself in front of a huge amount of tapes and magnetic disks that he does not know anything about or knows their contents or has the ability to examine them and know their content, which forced him to leave the computer center of the competing company empty-handed and with the appropriate company On its own several days later, it delivered the address data to the victim's company, but it is certainly possible that the tapes in question had been reproduced prior to their delivery, which would have lost the court's order.

31. Lester, Martin. Duffy, John. Giddings, Seth. Grant, Ian. Kelly, Kieran. (January 29, 2009) New Media: A Critical Introduction, USA/UK Europe: Routledge. 2 edition.

2- **Easy erasure or destruction of evidence in a short period of time**

One of the challenges that may face the evidentiary process in AI-related crime cases is the ease with which the perpetrator deletes or destroys forensic evidence in a short period of time, in addition to the ability of a person to disavow his act by attributing it to a defect in the computer system or network. A practical example is a weapon smuggler making modifications to the standard commands of the operating system he uses to store his clients' addresses, which can lead to a command for the computer to be entered via the keyboard to copy , erase or destroy all data. Although the modification of the computer operating system was done specifically by the perpetrator with the aim of preventing the success of the follow-up devices in the procedures of searching and collecting evidence, he was unable to achieve this goal because the experts expected that something had been changed in the offender's computer operating system and they accordingly cloned the magnetic discs seized by their computer systems.[35]

**3- Difficulty accessing the directory**

Information stored electronically or transmitted over communication networks is surrounded by a wall of technical protection in order to prevent unauthorized access attempts to view or copy it[36]. A cyber offender can further complicate searches to obtain incriminating evidence by taking a variety of security measures such as using a password to access them, entering confidential instructions between them, or even encrypting them to prevent them from being seen or seized. Therefore, the use of encryption technologies for such purposes is one of the biggest obstacles facing the control of data stored or transmitted across international borders, as it reduces the ability of the competent authorities in investigation, investigation and prosecution to access it, making the protection of the privacy of personal data stored in data centers and networks or related to ordinary and electronic trade secrets or security and defense measures very complicated."[37]

The obstacle of accessing the information directory encounters a procedural problem related to the applicability of the restrictions on the seizure of the content of the automated data processing system, which is technically protected in the face of unauthorized access, as the Egyptian and UAE Code of Criminal Procedure, under articles 52-57, respectively, prohibits[38] the judicial officer from accessing sealed or sealed papers. [39]in the house of the accused during a search)[40]. The reason for this is to preserve the traces contained in the papers, and here the question arises whether the provision of these two articles must be followed with regard to the judicial officer's access to the content of the automated data processing system or not, in the event that it is surrounded by a wall of technical protection that hinders access to it. We take the initiative to affirm this question on two grounds:

**First,** the reason for placing this provision for sealed or sealed papers is the same as that applies to the contents of an automated data processing system that is technically protected from unauthorized access. The legislator prohibited the judicial officer from reviewing these papers in order to believe that the

---

[35] Hisham Mohamed Farid Rostom, previous reference, p. 34.

[36] The process of collecting challenges includes: Electronic evidence and its use face some key challenges Difficulty accessing files deleted, cached or protected by passwords within large systems linked through networks. Difficulty recovering data from some old media or media.

Difficulty finding pivotal files or records Among the vast areas of data, for example: email logs

Difficulty analyzing the health of files – and whether they have been modified or erased: see Linda volonino ph. D.ibid., p. 14

[37] Professor Sieber points out that many significant problems have resulted from the use of encryption or encryption techniques by perpetrators of some of the information crimes that occurred in the Federal Republic of Germany to impede the discovery or access to incriminating evidence, especially in the field of storage methods that are difficult to control. (See 141.Ulrich Sieber Ibid, p

[38] The first article of them stipulates that "if papers sealed or sealed in any way are found in the house of the accused, the judicial officer may not open them, and with almost the same wording the text of Article 58 A.J. UAE applies.

[39] If it appears that the packaging does not include but contains a solid body, the judicial officer may unwrap the cover to examine its contents Egyptian cassation 24 June 1958, collection of cassation rulings s 09 No. 180 p. 716.

[40] In Egypt, article 47 of the Egyptian Code of Criminal Procedure was ruled unconstitutional on 2 June 1984, and therefore the text of article 52 of this Code is no longer applicable in the case of flagrante delicto.

closure or packaging gives them more confidentiality and reveals the desire of the owner to maintain their confidentiality without his permission. This also applies to data stored or transmitted over the system or network, if technically protected. against any unauthorized access. Therefore, the content of the system is not actually exposed but rather obscured from others, as it can only be accessed with the knowledge of methods, keys and operating code.[41]

**Second:** Article 52 of the Egyptian Procedures 58 UAE procedures sets out a general rule to guarantee the secrets contained in other media and containers for the preservation, storage and transfer of information, whether traditional such as papers or novelties such as floppy disks, magnetic tapes, internal memories of computers and local, regional and international information networks.

It is important to note that both the Egyptian and Emirati procedural systems not only feature this provision, but share it with many other laws. For example, article 110 of the German Code of Criminal Procedure stipulates that the right to access the results of computers and other means of data is limited to the public prosecutor. Police officers are not entitled to access this data by running programs or accessing data files stored inside the computer without the permission of The person who has the right to dispose of it. What is legally permissible is to examine these means only by sight, without the use of technical assistance.[42]

**4- Lack of evidence traces**

Sometimes, data is entered directly into the computer system without the need for accompanying documentation (input documents), as in some direct operations systems that rely on replacing written permission to enter data with other procedures based on permission controls contained in the computer program. For example, a computer may perform some accounting operations without the need for entry, as is the case with calculating interest on bank deposits and automatically recording them on customer account balances based on agreed terms. preset and located in the computer program.

In both types of operations, crimes such as embezzlement of funds and forgery can easily occur by entering unauthorized data into the computer system or modifying its programs or data deposited in it, without leaving a trace indicating that such action or modification has occurred. The investigator must therefore take into account the difficulty of reaching the perpetrators of crimes in both types of operations and the absence of significant effects of changes in software or data as is the case with traditional forgery in official documents.[43]

To identify the circle of persons in charge or connected in the processes of entering and processing data seeks and other registration processes[44]. While taking advantage of the control controls that are initiated in the information system on the entry and processing, in addition to tracking the various funds, if any, as the outcome of the crime that the criminal eventually seizes."[45]

Third: Obstacles related to the human factor

There are many obstacles to this type as follows:

A- **Place where the crime was committed**

The crime of artificial intelligence is usually committed remotely, where the perpetrator is not present at the crime scene, and then the distances between the act (through the perpetrator's computer) and the result (the data in question) diverge, and these distances do not stop at the borders of the state, but may

---

[41] Hisham Muhammad Farid Rostom, previously referred to, p. 35.

[42] Manfred Motherin Schlager, Computer and Other Crimes against Information Technology in Bermani, rev, inter, D.P. leret 2e trimesters 1993, p. 351.

[43] Jack Bologona Faro Company Prevention and Detection Base, Butterworth Publishers 1984, p.75

[44] J.Tappolet , La fracuc infiromatieque, rev, int, crim poltech 1988, p.351

[45] Hisham Muhammad Farid Rostom, previously referred to, p. 21.

extend to the territorial scope of other countries, which doubles the difficulty of detecting or prosecuting them.[46]

- British authorities have announced that more than ten thousand AIDS education CDs have been admitted to hospitals in Britain, Sweden, Denmark and Norway. Data machines have discovered that they are infected with the Norjan virus, a virus that sabotages personal computers — and damages the software that runs on them in the meantime. Scotland Yard has launched a wide-ranging investigation into this case as a crime of sabotage and investigations have proven the following: that this cylinder reached people by mail from various sources with the aim of sabotaging the programs sent to them and that the names of those to whom the CDs were directed numbering about seven thousand people have been sold to a company called "Kitima", an institution belonging to a Kenyan businessman "named Kitima" It turns out that the list of names that were brought with him during his visit to Britain in The period from October 31 to November 30, 1989 but no address was inferred.
- A number of these cylinders appeared in California, Belgium and Zimbabwe.
- The messages were sent with messages labeled "AIDS Information" but were found to contain the Norjan virus, which attacks AB personal computers . m and compatible with it.
- The letter that came with the disc asks for a $189 or $378 ownership fee for the program on request, and asks to send a response to an address in Panama. But it turned out that most of these letters were sent from London. After searching, it turned out that there was no company with that name and no mailbox in Panama. It also transpires that the person who sent the letter used the name of one of the American companies operating in Panama, which confirmed that it was not responsible for what happened.
- The message warns that if the fees are not paid, the sender will use software to sabotage the information and automatically shut down the computer, but what drew attention to the issue happened during the loading of the cylinder, according to Gercerst, a British virus expert and application consultant.[47]

### B- **Lack of experience of the police and prosecutors and the judiciary**

To detect and prosecute AI crimes, special strategies are required to develop certain skills that help counter advanced computer technologies and methods of manipulation, as the techniques used to commit these crimes vary and complexity.[48].

Therefore, modern and innovative techniques and methods must be applied to determine the nature of the crime committed, the person responsible for it and the methods of its execution, in addition to relying on innovative means to apprehend the offender and collect evidence to convict him. Judicial officers are likely to have difficulty dealing with this type of crime using evidentiary means and traditional procedures[49]. This is made more difficult by the lack of computer systems and information networks in the early days of their use of control methods and auditing and auditing controls on processes and applications and the lack of technical means to detect and track the course of operations[50], in addition to the difficulties faced by these bodies in investigating cross-border computer crimes, especially after the widespread use of the World Wide Web Network.

---

[46] Osama Mohamed Mohieldin Awad, Computer Crimes and Other Crimes in the Field of Information Technology, Research presented to the Sixth Conference of the Egyptian Society of Criminal Law, Cairo, October 34, 1993

[47] Osama Muhammad Muhyiddin Awad, previous reference, p. 430

[48] Donn, B., Parkar, Weaknesses in the Electronic Remittance System for Intentionally Causing Losses to Computers and the Electronic Money Transfer System Banking, and Public Policy edited by Kent W. Colton and Kenneth L. Kramer, Full Translation Press 1980, p. 97

[49] According to European Council Recommendation No. (95) 13 of 11 September 1995 on the problems of criminal procedures related to information technology, it is necessary to form special units to combat computer crimes and to prepare special programs to qualify criminal justice workers to develop their knowledge in the field of information technology.

[50] Bernard B. Zajack Jr., Police Responses to Computer Crime in the United States, July – Uigh 1985 Computer Law and Security Report, pp. 16-17

Police agencies often fail to appreciate the importance of AI crime due to a lack of experience and training[51]. For the same reason, investigators often fail in computer crimes such as computer outputs and playlists, but the investigator is sometimes the case in some other crimes may destroy the evidence by erasing the hard disk from his error or negligence or by dealing with floppy disks or by dealing hasty or as wrong with evidence.[52]

C- **The role of experts in data testing**

The huge amount of information circulating through information systems is one of the obstacles to the investigation of artificial intelligence crimes. This is because printing all the data on the digital media of a medium-sized information center requires hundreds of thousands of pages, which may not reveal almost all of them. When an untrained investigator faces this difficulty, he or she chooses one of two options: Either seize electronic data beyond human ability to review it or overlook that data in the hope of obtaining a confession from the perpetrator[53]. In fact, this difficulty can be countered by one of two things:

- The use of technical expertise to identify the essential elements of research and investigation of IT-related crime cases is essential. This is due to the special technical nature of the methods of carrying out crimes, and the moral nature of the crime scene. The success of these bodies depends largely on the selection of the right expert, in addition to his competence in performing the task entrusted to him. Although the expert himself can determine the subject of his task, this may lead to the expert's role dominating the evidentiary process and absenting him from the role of investigator or judge.
- Use the methods of systematic or systematic auditing and examination provided by automated data processing systems, and testing and review systems and means .

**Fourth: Obstacles to international coordination in the field of evidence**

Collection There are many obstacles that stand as a stumbling block for international coordination in combating artificial intelligence crimes, the most prominent of which are the following:

- There is not yet a common public concept among countries about the models of computer-related crime.
- Lack of a unified legal definition of criminal activity related to this type of crime.
- Lack of coordination between the criminal procedure laws of different countries with regard to the investigation and investigation of information crime. With the complexity of legal and technical problems related to the inspection of information systems outside the borders of the state or the seizure of information stored in it or the order of its delivery.
- The absence of extradition treaties or bilateral or collective cooperation between states that allow international cooperation, or their inadequacy, if any, to meet the special requirements of information crimes and the speed of their investigations[54].

---

[51] I learned that a young man asked for a copy of a computer CD and photographed the card affixed to it and then put the CD on the glass surface of the camera, but the strategy that arose when the machine coined led to the erasure and tilt of all the information recorded on the cylinder and there is another case where the policemen put a whole bag containing the confiscated computer CDs in the trunk of the car near the radio transceiver, the result was that the strong electrical signals caused the destruction of them all. See In it: Burici sterling ibid, p. 208

The FBI said its expertise was unable to determine whether the event occurred due to a technical failure or a cunning attack. The National Brokerage Company's website, which is frequented by 200,000 customers, was blocked for more than an hour — during which the company's engineers tried to defend the system against what they saw as an attack. They noticed that the site was operating too slowly when the market opened, which led to a 50% drop in accessibility. See in It D. voloninalinu ibid, p. 6

[52] Richard Tutta and Antong Hardcastle, Computer Related Crime in Information Technology Law edited by Chris Edwards and Nigel Savage Macmillan Publisher 1986, p.201

[53] Hisham Muhammad Farid Rostom, previous reference, p. 36.

[54] In response to these problems, or some of them, the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Havana in 1990 , in its resolution on computer-related crime, appealed to Member States to intensify their efforts to combat more effectively computer abuse that warranted the application of criminal sanctions at the national level, including by considering whether States had been able to reduce such contact and exchange at times that were necessary to modernize criminal laws and procedures. Including measures from:

**Conclusion**

In this paper, we looked at AI-related crimes that are becoming increasingly common, resulting in serious harm to individuals, businesses and countries alike. A country's national security systems may be vulnerable to AI penetration. In addition, AI crimes appear in multiple forms and classifications, and it is clear that these crimes are not limited to certain countries. This is reflected in the reality imposed by technical and information progress, which has been confirmed by the continuous developments in the means of processing and transmitting information as it has become a strategic determinant of cultural construction and economic achievement. This shows that this modern crime is spreading across the world. In response to this widespread spread of this type of crime, countries have tended to include their laws to combat artificial intelligence crime, with the aim of applying the law to cybercriminals wherever they are and imposing punishment on them. Many countries are also seeking to activate the principle of international cooperation to combat artificial intelligence crimes.

Many legal experts stress the importance of establishing an electronic court to bridge the legal gap created by the tremendous technological development in the field of artificial intelligence. There are crimes committed and violations practiced, and rights taken through AI applications without any legal oversight. The reason is due to the lack of international law that prosecutes AI criminality. But this is not impossible and may be achieved in the near future. It is clear that AI-related crimes are not far from Arab countries, as they have affected all An almost corners of the world. Therefore, the information society in the field of criminal procedure law must establish modern legal rules that allow certain information to be placed at the disposal of the dominant party in the investigation of artificial intelligence crimes.

**References**

[1] Osama Mohamed Mohieldin Awad, Computer Crimes and Other Crimes in the Field of Information Technology, Research presented to the Sixth Conference of the Egyptian Society of Criminal Law, Cairo, October 34, 1993

[2] Jamil Al-Saghir - Crimes Arising from the Use of Computers, Cairo, Dar Al-Nahda Al-Arabiya, p. 23.

[3] Jamil Abdel Baqi Al-Saghir, Substantive Provisions for Internet-Related Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 1999.

[4] Abdel Razek Mukhtar Mahmoud, Applications of Artificial Intelligence, An Introduction to the Development of Education in Light of the Covid-19 Pandemic, International Journal of Research in Educational Sciences, Vol. 3, No. 4, 2020.*

[5] Dictionary of meanings available on the internet https://www.almaany.com/ar/dict/ar-a? Accessed November 20 , 2024.

---

- Ensure that existing sanctions and laws on investigative powers and the admissibility of evidence in judicial proceedings are appropriately applied and that appropriate changes are made to them if necessary.
- Provision for crimes and sanctions Investigation and evidentiary procedures where necessary to address this new and complex form of criminal activity in the absence of laws that are properly applied. The Conference further urged Member States to redouble their activities at the international level to combat computer-related crime, including, as appropriate, their accession, as appropriate, to treaties on extradition and mutual assistance in special matters relating to computer-related crime. Member States should ensure that their legislation on extradition and mutual assistance in criminal matters is sufficiently applicable to serious forms of criminality, such as computer-related crime, and that specific steps are taken. as appropriate in order to achieve this objective, in addition to other recommendations and may be appropriate as a step to enhance the path of effective cooperation and complement the decisions taken by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in this regard.
- International standards for automated data processing security.
- Appropriate measures to resolve jurisdictional problems raised by transnational or international information crimes (c) International conventions containing provisions regulating the procedures for direct cross-border inspection and seizure of interconnected information systems and other forms of mutual assistance, while ensuring the protection of their rights and freedoms and the sovereignty of States. See: Hisham Muhammad Farid Rustom, op. cit., p. 49.

[6] Jamil Abdel Baqi in his book - Crimes arising from the computer - a report submitted to the Sixth Conference of the Egyptian Society of Criminal Law - Dar Al-Nahda Al-Arabiya, Cairo, 1996.
[7] Hisham Mohamed Farid Rostom, research presented to the Conference on Law, Computer and the Internet from 1 to 3 May 2000 at the United Arab Emirates University entitled Information Crimes).
[8] Friedman. 445 F. 2d 1076, 1087 (9th Cir.) (The theft of grand jury minutes and the information contained therein was theft of government property.) The certificate was rejected. 404 U.S. 958 (1971) United States v. Morison, 604 F. Supp. 655, 663-65 (D. Md. 1985) ("theft" of confidential information supports a conviction for embezzlement); United States vs United States. DiGillo, 538 F. 2d 972 (3d Cir). The certificate was rejected. 429 US 871 (1971) (theft by photographing sufficient government records to support and 641 advocacy): United States v. MeAusland, 979 F.2d 970 (4th Cir. 1992) (theft of confidential bid information of the competitor violates & 641).
[9] (Nicholson) Keith – International Computer Crime: A Global Village Under Siege
[10] (SIEBER) D. Ulrich Computer and Other IT-Related Crimes, rev. inter.de droit penal, 1991, p. 1033
[11] 31. Lester, Martin. Duffy, John. Giddings, Seth. Grant, Ian. Kelly, Kieran. (January 29, 2009) New Media: A Critical Introduction, USA/UK Europe: Routledge. 2 edition.
[12] A Regona, Massimo & Yigitcanlar, Tan & Xia, Bo & Li, R.Y.M. (2022). Opportunities and Challenges of Adoption in the Construction Industry: A PRISMA Review. Journal of Open Innovation Technology Market and Complexities, 8(45). https://doi.org/10.3390/joitmc8010045
[13] Bernard B. Zajack Jr., Police Responses to Computer Crime in the United States, July – Uigh 1985 Computer Law and Security Report, pp. 16-17
[14] Cardona, Artificial Intelligence and the Future of Education, USA, (2) Miguel Office of Educational Technology, May 2023, p.13
[15] Cybercrime, Fall 1996, p. 1. "Accountability offence is any violation of the law involving knowledge of computer technology to be committed, investigated or prosecuted" available online in February 2000 at:
[16] Definitions: "For the purposes of this Agreement: devices connected to a computer system or related devices, one device or means any other device or group of devices, according to the program, automatically processes data" computer-related crimes
[17] Donn, B., Parkar, Weaknesses in the Electronic Remittance System for Intentionally Causing Losses to Computers and the Electronic Money Transfer System Banking, and Public Policy edited by Kent W. Colton and Kenneth L. Kramer, Full Translation Press 1980, p. 97
[18] FGSSC - Available online in February 2000 at: http://www.usdoj.gov/criminal/cybercrime/search docs/toc.htm
[19] Friedman, L., Blair Black, N., Walker, E., & Rochelle, J. (November 8, 2021) Al in Education Secure Needs You. Association of Computing Machines https://cacm.acm.org/blogs/blog-cacm/256657-safe-ai-in-education- Blog, Need You/ Full Text
[20] of support provided http://www.witsa.com December 2000 available online in December 2000, at: http://www.mcconnellinternational.com/services/cybercrime.html
[21] Gartner (n.d.) Gartner Glossary: Augmented Intelligence. Gartner: https://www. Intelligence
[22] gartner.com/en/informationtechnology/glossary/augmented-
[23] http://wings.buffallo.edu/complaw/complawpapers/scalion.html
[24] http://www.mcconnellinternational.com
[25] J.Tappolet , La fracuc infiromatieque, rev, int, crim poltech 1988, p.351
[26] Jack Bologona Faro Company Prevention and Detection Base, Butterworth Publishers 1984, p.75
[27] Jay, J. Baker Computer Crimes Trial (1980), 2 Computer Law, Journal 441
[28] John Eaton and Jeremy Smithers, that's it. Amangagrs Guide to Information Technology, London, Philip Allan, 1982 p.263
[29] Network Prof. Dr. med. Henrik W. K. Threats and Opportunities Criminal Perspective, p. 258. Five European criminal justice cases: corruption, women in the criminal justice system, criminal policy indicators, community crime prevention and cybercrime procedures of the Sixth European

Symposium on Crime and Criminal Policy, Helsinki, 10-12 December 1998, European Institute for Crime Prevention and Control, United Nations Affiliated (HEUNI), P.O. Box 161, f. 00131 Helsinki Finland Publication Series No. 34 - Thumir

[30] Technical difficulties are related to the encryption methods used on the network.

[31] Manfred Motherin Schlager, Computer and Other Crimes against Information Technology in Bermani, rev, inter, D.P. leret 2e trimesters 1993, p. 351.

[32] International and Comparative Law in New England Annual 1996

[33] New England College of Law P. I. Available online September 2001 at: http://www.nest.edu/annual/vol2/computer.htm

[34] Rcmp op-cita Computers and telecommunications explode in the next century Prosecutors and prosecutors face a new type explosion in the next century Prosecutors and prosecutors have begun to face a new kind of problem

[35] Richard Tutta and Antong Hardcastle, Computer Related Crime in Information Technology Law edited by Chris Edwards and Nigel Savage Macmillan Publisher 1986, p.201

[36] Russell, S. (2019). Compatible with human: artificial intelligence and the problem of control. Viking. ISBN978-0-525-55861-3 .

[37] Thoumyre - Abuse in Cyberspace op. cit. P.9 Think globally and act locally

[38] The transient nature of cyberspace, (cybercrime and the ancient law of global cyber punishment< Information p. 2 Report by McConnell International

[39] UNITED STATES V. SAMPSONM, 6 COMP, L. SERV. REP. 879 (N.D. Cal. 1978)

[40] Voir website: Temp (Royal Canadian Mounted Police) "Computer crime is any illegal act involving computer systems whether a computer is a crime, a tool used to commit a crime, or a response available on the Internet in the February 2000 crime." Guide related to http://www.rcmp.com (Mac D. Rush - Criminal Law and Internet - Internet and Society). © Copyright 1996 by Computer Law Society, in: Inc. P.6, Donn Parker of Sri,