Research Article

Received: 31 October 2022 / Accepted: 22 December 2022 / Published: 5 January 2023

Artificial Intelligence Crimes

Ibrahim Suleiman Al Qatawneh[1]

Ahmed Fekry Moussa[2]

Maher Haswa[3]

Zeyad Jaffal[4]

Jamal Barafi[5]

[1]*Professor, College of Law, Al Ain University, Al Ain, United Arab Emirates*
[2]*Assistant Professor, College of Law, Al Ain University, Abu Dhabi, United Arab Emirates*
[3]*Associate Professor, College of Law, Al Ain University, Abu Dhabi, United Arab Emirates*
[4]*Associate Professor, College of Law, Al Ain University, Al Ain, United Arab Emirates*
[5]*Associate Professor, College of Law, University of Sharjah, Sharjah, United Arab Emirates*

DOI: https://doi.org/10.36941/ajis-2023-0012

Abstract

The rapid evolution of information and communication technologies and the diversity of interconnection networks have been significant factors in broadening the application do-mains of such technologies. Consequently, so-called artificial intelligence crimes (AIC) have emerged involving a corresponding rise in criminality figures, affecting individuals' rights and freedoms. The emergence of AI-related crimes has triggered many challenges for the judiciary nationally and internationally. Thereby, jurisprudence and the judiciary must consider whether the existing provisions of law are sufficient to confront these crimes, or is there a need to strengthen international, regional, and national legislation to cover such cases. Such peculiarities characterizing AI crimes have complicated dealing with criminal activities, and they are usually dealt with using traditional criminal provisions, which may be compromised by the principle of criminal legality and the limited interpretation of a criminal provision. Accordingly, legislative steps must be taken to combat such crimes by enforcing legal provisions intended to criminalize the newly introduced criminal acts.

Keywords: *Artificial Intelligence, Cyber Crime, Information Technology, Crime, Jurisprudence*

1. Introduction

Crime has evolved throughout history, taking advantage of certain technologies and accompanying conditions. In the current period crime has advanced along with the proliferation of computers. Crimes committed online are known in contemporary criminal jurisprudence as advanced crimes. In accordance with the modern technological world evolution and the dominance of digital science in all aspects of human life, today's world has facilitated online crimes. Contemporary criminal behaviors have emerged relying on artificial and technological intelligence to steal victims' legal status and information, and obtain material of personal or national significance. In particular, cyber criminals hack into private systems, and adapt fraudulent methods to trap victims into either providing information, or allowing the criminal access to their system. It should be noted that AI crimes are carried out in many ways, many of which can be achieved by disrupting the automated data processing system. This can be done with destructive malware that can erase all or a part of the system's programs, files and stored data, thus damaging and disturbing it [1]. These malware include logic bombs[1], worm[2] and electronic viruses[3], and Trojans[4]. Regardless of how the criminals attack an automated data processing system, the malware wards the system off anyways.

To determine the theoretical and legal nature of AI crimes, this research will first examine their theoretical framework and peculiarities. It will then discuss the limited legal processing of AI crimes and the difficulties encountered.

The paper intends to examine certain significant matters such as: how sufficient is current legislation and efforts to counter and combat AI crime? This and other queries will be addressed by the authors, who will provide suitable answers within the concluding remarks. These queries include:

1. What legislation and efforts have been set up to combat AI crimes?
2. What are the most significant obstacles and difficulties to combating AI crimes?
3. What are the necessary means to combat AI crimes?

The study uses the Descriptive and Analytical Approach, which presents, analyzes, and evaluates texts and opinions related to the subject of the study in a way that accomplishes the purpose and answers the problem of this study.

2. Theoretical Nature of Artificial Intelligence Crimes

2.1 Peculiarity of AI Crimes

Arguably, AI Crimes comprise every form of illegal or harmful act to a digital structure committed using a computer or digital device. Noting that a computer system plays the key role in committing such a criminal act, it makes no difference whether the computer is a means or a sphere for doing so. Artificial intelligence crime is a criminal act designed primarily to harm the interests of others through various electronic means. The means and objectives differ in each case, making them no

---

[1] *Logic or time bombs in a program, prepared by the software designer, which is installed within the information system in order to be operated after a specified period to use it for destroying, disrupting, or erasing the data contained therein.*

[2] *Information worms are programs that exploit any gaps in the operating systems to move from one computer to another, covering the entire network.*

[3] *They may transfer due to interconnections. During such a transition, they multiply like bacteria by producing copies. An electronic virus is a program that includes destructive goals for information systems and is characterized by its ability to reproduce itself in the program it infects, thereby controlling and modifying it, its ability to distinguish between infected and non-infected programs, and protect itself against the virus.*

[4] *The Trojan Horse: analogous to the well-known story of the "Trojan Horse", a deceptive program that conceals hidden functions known only to the hacker. The hidden components allow him to circumvent the existing security and surveillance systems.*

different from traditional crimes in their criminal consequence, which is attributable to the element of harm. Artificial intelligence crimes are just like any other crime; a set of formative elements must be fulfilled to ascertain the crime as prescribed by law.

Artificial intelligence crimes may be either crimes against national security[5], against persons[6], or against funds. The association between artificial intelligence crimes and classical physical criminal thought has given AICs a special legal scope distinguishing them from conventional crimes [2]. As a result of the evolving nature of such criminal acts, they acquire extraordinary privacy when compared to conventional crimes, which can be summarized as:

1. Crime occurring in the automated data processing and transaction environment;
2. Cooperation and complicity in damages for artificial intelligence crimes;
3. Difficulty detecting artificial intelligence crimes;
4. Crimes based on computerized data;
5. Difficulty in detecting and proving them;
6. Transnational Artificial intelligence crimes [3].

Based on the foregoing, we can analyze the subject of AI crimes, which differ in terms of how they are perceived. On one hand, an AI system maybe be considered the subject of a crime, in which case the crime is assault on the computer's [7]physical components and hardwware.

On the other hand, AIC may involve an assault on the moral or logical components of the information system (software)[8]: Such a case occurs when the intangible components of the information system are targeted by the criminal. In this case, the cybercriminal may assault electronic data and software stored in the computer's memory by deleting, altering, or counterfeiting the software, or other legally prohibited acts.

In other cases, AI crimes may be considered a tool to commit a conventional crime [4] when the criminal exploits AI to engage in more traditional law-breaking. Thus, the nature of the crime varies according to the right or interest protected under each subject matter, such as forgery and theft.

This shows that AI crimes differ from others regarding how they are committed. These crimes are less disturbing in nature because they are not based on violence, but rather on the criminal's ability to handle a computer with the technical skills needed to commit the crime in question [5]. Unlike artificial intelligence crimes, the conventional ones require muscular exertion of diverse forms.

It is worth noting that committing this type of crime requires extreme intelligence; one of the main characteristics of the cybercriminal [6] is demonstrating the mental ability to achieve his objectives. In addition to the criminal's technical knowledge, his intelligence enables him to become a computer specialist and gain extraordinary experience.

Some jurisprudence suggests that this type of crime has given rise to factors used in perpetrators' minds. Many commit such crimes for fun or a desire to show their superiority over software dedicated to information systems security. Otherwise, they may simply want to brag about their intelligence and show their victims the weakness of their systems since the cybercriminal is a mere social human being [7] yet engages in antisocial activity. In addition to having a criminal tendency[9], the criminal gained advanced technological skills; he mastered these skills specifically to

---

[5] *They are crimes intended to harm and negatively affect States' security, and are as diverse as cyber terrorism.*

[6] *Such crimes vary, including threats committed through electronic media, impersonation and deception, as well as slander.*

[7] *Hardware includes tangible pieces of machinery that can be touched and controlled manually, such as a keyboard and mouse*

[8] *Software: a computer's programming, such as Android, windows, operating systems, software and games,, etc https://io.hsoub.com/programming*

[9] *This criminal tendency consists of being impacted by psychological and internal factors influenced by person's upbringing, coupled with another element that helps stimulate the criminal situation and increases the external pressures of criminality factors.*

commit crimes [7].

It is worth pointing out that due to the nature of AI crimes, in many cases the perpetrators remain free from criminal accountability and are provided with anonymity. This provides them with a sense of superiority and high self-esteem.

2.2 Regional and International Agreements Attitude on Artificial Intelligence Crimes

The European Council has endeavored to confront the illegal use of computers and information networks by implementing numerous legislation. The Council's has paid attention to these crimes and their accompanying problems since the early 1970s. At the outset, attention was directed at protecting personal data so that increases in computer efficiency would not threaten individuals' right to privacy. A Convention relating to the Protection of Individuals against the Misuse of Electronically Processed Data was signed in 1981.

Said Convention contained several principles, including minimum precautions to be included in States' domestic legislation of the Treaty. These include legislation to protect individuals from the misuse of electronically processed data, along with the necessity of obtaining personal data from legitimate sources. It further stipulated that this data shall be updated and consistent with the purpose it was developed for; or the legislation should take into consideration the formal rules required to prevent misusing personal data.

The aforementioned Convention is not the European Council's first attempt at legislating AIC. Rather, the Budapest Convention against Cybercrime, known as the "European Convention", is the most important statement issued by this Council, to which the reality of AI crime can be adapted.

The standards set by the international community regarding the procedural rules required to combat crime in general focused on the following: supporting international judicial cooperation, and considering the cybercrime convention (Budapest Convention) a basis for extradition; Considering inter-State cooperation in criminal proceedings (Controlled delivery, letter rogatory); exchanging information adequately and quickly; Providing mutual aid (data revealing- entering the computer data – reservation to data- objection to data content…). Additionally a focal point for each country will be established to encourage criminal procedures, facilitating cooperation thereon, and collecting evidence.

The prevalence of information in all Arabic countries has resulted in the emergence of several criminal practices through artificial intelligence. This has lead Arabic countries to try to find effective legislative and judiciary means to counter these contemporary crimes. Among the efforts made, the resolution of the Seventh Arab Council of Ministers of Justice on crimes against individuals contained a chapter relating to the violation of people's rights, resulting from information in Articles 461-464. The Articles stipulate that individuals' privacy and secrets must be protected from automated processing. They further refer to collecting and accessing nominal information, as well as the applicable punishments for these crimes.

3. Limited Legal Handling of Artificial Intelligence Crimes

3.1 Methods of Legally Rooting Artificial Intelligence Crimes

3.1.1 Perilous Nature of Artificial Intelligence Crimes

Notwithstanding weak protections against crimes of artificial intelligence internationally and nationally, attacks are increasing due to the evolution of information technology. This provides criminals with opportunities to improve their computer skills and use them illegally, and thus poses another difficulty in legally proving and preventing such attacks.

Perhaps the most significant form of artificial intelligence crimes is that after the software is programmed, the computer will automatically carry out piracy, theft, data destruction, and other

crimes. This costs the State billions of dollars in losses.

3.1.2 Proving Artificial Intelligence Crimes

To locate and ensure evidence, the information expert and the research and investigation bodies must follow steps that include inspecting devices and information systems, from the computer components to the internet connection system, as follows:

a) Computer components check: computers consist of hardware and software (non-physical or intangible software) and they share the informatics element "informatique". Hardware can be checked partially or in whole, being highly important in assisting research and investigation bodies and computer science experts in obtaining digital evidence. It is noteworthy that partially checking the disk leads to the identification of dual-digit data, the handling of which leads to the disclosure of data and inputs stored within, whether such data is written, images, sounds... etc. When presenting digital evidence before the judiciary, computer safety is a main condition, therefore digital evidence must be taken from an undamaged computer [8]. When checking the hardware, the computer science expert will disclose documents, photos, and internet page caches used by the perpetrator. Through these documents, the inspector can investigate the suspect's identity through archived files, Internet addresses and emails, as well as the specialized software they used, such as "Word", "Photoshop" and other files stored inside the hardware [7]. Therefore, it is necessary to inspect the software[10], information system[11] [8], storage memory system[12], and printer[13] as well as the computer system software security[14] [8].
b) Internet Connection System Check: A computer science expert shall examine the Internet connection system to determine the crime location and the computer used; thereby helping identify the perpetrator by their e-mail search system via the web in case of a crime-related file. This system is checked through the Internet route Network[15] [9], Security System Check[16] [8], Server Check "Le serveur"[17], in addition to the IP System Check[18] [10].

3.2 Failure of Legal Regulation to Provide Adequate Protection from Artificial Intelligence Crimes

3.2.1 Inadequacy of Existing Criminal Legislation

Despite the fact that the technological harbingers of the telecommunication revolution have spawned a number of emerging crimes of a special nature, such as those of artificial intelligence, most methods of combating these crimes are still carried out within the framework of the familiar punitive provisions designed for conventional crimes. Consequently, many challenges have arisen regarding the prosecution of such crimes, which may multiply within the same State, or extend to many States

[10] *Through which the technology inspector checks the software.*
[11] *It aims to control the information contained in the computer through which it can be retrieved.*
[12] *Checking this system is one of the important places that the computer science expert can examine. It provides a record of internet browsing.*
[13] *Modern printers can store a set of pages that have been extracted from the computer, even in cases where files are removed from the computer.*
[14] *Such a system makes the offline computer safe from crimes.*
[15] *It is the transcriptional movement of activity on the Internet.*
[16] *Obtaining the electronic guide is faster when the computer is not connected to any type of network because it is not exposed to hacking.*
[17] *The server's task enables access to site and page traffic.*
[18] *Anyone can identify the holder of this protocol by searching the registrar's database, and multiple web-based software can be used to monitor the Internet Protocol.*

via the Internet. As such, it is impossible to gather evidence to prosecute them, since there may be issues of jurisdiction [11]. To take a different issue, the failure of laws to evolve as rapidly as media, technology and the skills of human mental dexterity in harnessing the innovations of technology, has rendered conventional laws powerless to confront numerous new crimes associated with the emergence and proliferation of electronic means and devices. Laws are particularly useless if we are aware that the positive laws prevailing in most of the world are governed by the principle of criminal legality, which states, "no crime nor punishment shall be imposed except by law". In addition, the scope of analogously criminalization under this principle is very limited since certain criminal acts- associated with using computers- cannot be criminalized under traditional penal laws. This is in spite of threats to public interests and serious dangers to public order. An example of such acts, punishable under the Criminal Code when being linked to a special case, is the abuse of personal information. Yet infiltrating and accessing an individual's secrets and personal or professional data stored in computer information systems is not criminal, according to general rules [12].

Moreover, hacking someone else's computer system and stealing information is not a crime according to customary laws. According to the law, theft is only related to movable money. In such a case, the criminal quality has not yet been proven for information being non-fungible. Likewise, the classical concept of theft or embezzlement means the dispossession of other people's money, whereas the embezzlement of information is to take a copy while the original is at the owner's disposal. Therefore, information is not protected by the criminalization established for financial crimes. The same goes for the non-occurrence of damage crimes on intangible electronic means such as data and software. Similarly, the forgery of information programmed in the computer or in any hardware did not occur since the legal instrument description was not applicable. In such cases, many difficulties arise in the application of traditional criminalization codes, as they were developed mainly to protect physical objects in the face of familiar and traditional methods of assault. Based on the foregoing, it is impracticable or impossible to punish a non-physical attack on the elements and components of AI systems. Additionally, the application of such criminal codes may sometimes be inconsistent with the nature of the means used to carry out crimes, which are data or information with all kinds of visual, comic, or written forms [13]. The failure of the law to keep pace with the rapid and continuous developments of artificial intelligence crimes has prompted most countries, especially those that have not enacted laws to criminalize various types of recently developed crimes, to broaden the interpretation of traditional criminal codes to extend their application to these crimes. They do so by granting their judicial authorities the flexibility to interpret these provisions to allow placing these exploits under penalty of criminalization and follow-up, in order to bring the perpetrators to justice.

However, it is obvious that these laws do not cover all the illegitimate acts ensuing from artificial intelligence, as the law does not evolve as efficiently as crime. Most of the world's countries have not implemented laws criminalizing such illegal acts and have merely applied existing laws despite proven limitations. Perhaps the underlying reason for such limitations is a lack of expertise, specialization, and adequate knowledge of the high and complex artificial intelligence environment.

4. Variation of Procedural Legal Systems

The different procedural laws among countries constitute another obstacle to the international confrontation of AI crimes. AI crimes are international and transnational in nature, making verification, evidentiary and prosecution procedures that demonstrate their usefulness and effectiveness in one country, ineffective and useless in another. For example, the procedures allowing electronic surveillance, interception of correspondence, tapping, recording of calls, telephone conversations and other veiled operations [14] differ from country to country. If an evidence-gathering or investigation procedure is considered legitimate and accepted by the law of a particular country's perspective, the same may be illegitimate under the law of another. Therefore one country may be disappointed by the inability of another's law enforcement authorities to use what it regards as an effective instrument of proving a crime. In addition, the second country's judicial authorities

may not permit the use of any evidence obtained in ways it considers illegitimate. An example would be the existing legislative divergence between Latino and Anglo-Saxon laws on the extent to which the digital guide is derived from the computer in criminal evidence. Under Latino laws based on the free criminal evidence system, such as French, Moroccan, Syrian and Lebanese law, a criminal judge has absolute freedom to assess and take from the evidence presented to the court, digital or electronic, that is deemed appropriate to form a conviction. Anglo-Saxon systems, such as British and American, do not recognize digital evidence as criminal evidence unless one of the forms predetermined by the legislator is taken in the means of proof and its value is persuasive, and obtained under predetermined conditions [15].

5. Conclusion

To summarize, criminal legislation needs legal empowerment and development to address the AIC, through the adoption of protocols, the establishment of specialized bodies for this purpose, and community and institutional education to protect citizens from such criminal behavior.

It is worth pursuing a clear policy that will effectively and efficiently handle artificial intelligence crimes. Implementing such a policy will require extensive discussion, comprehensive planning, capable and active executive bodies, and specialized and effective legislative and judicial tools. All these measures should lead to comprehensive, integrated and evolvable policy solutions that will keep pace with the developments of this era.

6. Findings

In view of the foregoing, this research finds:

1. Artificial intelligence crimes are characterized by a set of emerging peculiarities that touched the general foundations of recognized crime theory;
2. An absence of adaptive crime prevention solutions within an international framework despite the efforts made;
3. The fragmentation and complexity of AI crimes made prosecution a challenge not only at the judicial level, but at the international level as well;
4. An absence of institutions and centers for tracking and monitoring the movement of crime, not to mention the absence of a national crime observatory dedicated to researching ways to combat criminal elements.
5. A lack of educational and formative institutions for rehabilitating legal and judicial frameworks, and an absence of an artificial intelligence department in law faculties, various police institutions and schools, institutions and specialized centers.

7. Recommendations

- A unified legal framework and a comprehensive definition of AI crimes should be created in order to identify them;
- States that have not yet implemented substantive and procedural penal laws for AI crimes shall expedite the amendment and rationalization of their laws to appropriately address such crimes, in order to avoid legislative deficiencies and overcome legal gaps in this regard;
- It is not enough to rely on existing legislation to overcome procedural difficulties arising from the process of searching and investigating cybercrime. There is a need for new special provisions that include appropriate investigative procedures for such a new form of criminal behavior. There is also a need to keep up with changes and developments in the techniques and methods of such investigations. Those provisions should ensure their consistency with all constitutional guarantees, the rules of legality, and the right to privacy.
- Arabic nations should consider the recommendations of the Council of Arab Ministers of

Justice relating to artificial intelligence crimes, including the establishment of an Arabic police organization dedicated to coordinating the fight against cybercrime in general, and artificial intelligence in particular, as well as encouraging the Arabic federations to address such crimes. The role of Arabic organizations, departments and governments in the face of these crimes should also be defined and planned.

- It is necessary to establish security units and judicial bodies specialized in combating AI crimes. These bodies must have adequate knowledge of the specialized and technical aspects of the follow-up, detection, and investigation of such crimes and their perpetrators. Such specialized knowledge will require periodic special training programs. Said programs help personnel improve and update their knowledge and expertise and familiarize themselves with the latest developments in the field of cyber information.
- A clear and effective policy should be adopted regarding security cooperation and judicial and technical assistance among States to combat AI crime. This will require adopting prompt and appropriate investigative and follow-up procedures. It is also crucial to create bilateral or multilateral channels of communication that allow investigating authorities to easily communicate and coordinate with their foreign counterparts.

References

Abbad, A. "Information Crime." National Journal of Legal and Judicial Sciences.

Abdel-Muttalib, M. Digital Forensic Research and Investigation in Computer and Internet Crimes. Dar El-Kutub El-Qanoneiyah, 2006.

Al-Maini, S. "Investigation of Information Technology Crimes." Police Thought Journal, vol. 20, 2011.

Al-Qahwaji, A. Criminal Protection of Electronically Processed Data. 3rd ed., vol. 2, United Arab Emirates University, 2004.

Bakri, B. Inspection of Information in Modern Technology. Alexandria, Dar Al-Fikr Al-Jamii, 2011.

Benhamou, M. Crime Committed via the Internet. 2016.

Fuentes-Camacho, Teresa. Les Dimensions Internationales Du Droit Du Cyberespace. Paris, Éditions Unesco, 2000.

Ghommam, G. The Inadequacy of Traditional Rules in the Penal Code to Combat Computer Crimes.

Hegazy, A. Combating Computer and Internet Crimes in the Arab Model Law. Alexandria, Dar Al-Fikr Al-Jamii, 2006.

Ibrahim, K. Cyber Crimes. 1st ed., Alexandria, Dar Al-Fikr Al-Jamii, 2009.

Mousa, M. Criminal Investigation in Electronic Crimes. 1st ed., Cairo, Police Press, 2009.

Noman, D. Cyber Fraud, Phenomenon and Applications, a Critical Analytical Study in the Light of the Position of Moroccan Legislation Jurisprudence and Comparative Judiciary. 1st ed., Marrakech, National Press and Paper, 2011.

Pradel, Jean. "Les Infractions Relatives à L'informatique." Revue Internationale de Droit Comparé, vol. 42, no. 2, 1990, pp. 815–828, 10.3406/ridc.1990.1994. Accessed 20 Dec. 2022.

Qlaish, A. Criminology and Punishment. 2nd ed., Fadha' Adam Library for Publishing and Distribution, 2017.

Zulaiji, M. "Authority of Evidence for Computers in the Criminal Domain." Journal of the Basic Private Law Laboratory, 2010.