University of Mostaganem-Algeria
VOL: 8 / N°: 1 / (2021), p. p. 119/135
International Journal of Social Communication
ISSN: 2437 – 1181
EISSN: 2710-8139

The role of artificial intelligence in eliminating economic cybercrime -judicial and ethical issues-

Fatima Zahra Drim[1] * Cherrara hayat [2]

fa_tomaz@yahoo.fr Laboratory of media studies Mostaganem
cherrarahayat@gmail.com Laboratory of media studies Mostaganem

Received: 25/05/2020 *Accepted: 27/10/2020* *Published: 28/7/ 2021*

Abstract: Abstract:

Artificial intelligence crimes are the crimes of the near future, if some of them have not started now. The technological development during the past years - which accelerated in the current period - helped in the emergence of many of these crimes, as advanced programming for some machines that work with artificial intelligence gave capabilities that reach their gravity To build a personal experience that enables her to make individual decisions in any situations she faces like a human being

Therefore, we aim from this study to legalize the conditions of artificial intelligence crimes to determine who is responsible for these crimes and to impose a penalty on it; the importance of the topic lies in the fact that our current age is not without a field in which artificial intelligence is available. For crimes committed by a method, and for whom will the responsibility lie, to determine the true perpetrator until the legal penalty is applied to him;

In the research methodology, the researcher will follow the original approach in order to return those facts to the laws that criminalize them. Then the analytical method is used to find out the criminal effects of this phenomenon; we have reached a set of results which are the rapid spread of artificial intelligence technologies and their penetration into various aspects of life, with no floating legislation protecting Society of those crimes, and that requires the enactment of legislation regulating the production and development of artificial intelligence techniques to reach a legal concept that allows criminal accountability.

Keywords: protection techniques; artificial intelligence; economic cybercrimes; information security, Judicial measures

Introduction:

---

* **Fatima Zahra Drim**

Security threats are one of the most pressing challenges facing global economies. The use of state-of-the-art complex protection technologies and the strengthening of information security infrastructure systems pose a major economic crisis for large sums. The investment in information security is a top priority for governments and companies around the world, So there must be many strategies to protect companies and their networks from real threats to information security.

in addition, electronic risks are constantly changing and cybercrime is international in nature, hence the need to build intelligent information security management systems based on artificial intelligence techniques and platforms to support control and control processes, accurate decision making by experts and knowledge owners, Information and detection of manipulations and espionage.

Without forgetting the legal and judicial aspect and its role in combating cyber crime through new laws within the virtual space and fighting criminals within the Internet using artificial intelligence tools.

Information security is a complex system that must be taken into consideration at all stages of work system development and how it is used by all workers. Therefore, facilities need an organized methodology that supports the stability of standards during all stages, based on safety forecasting and analysis and not only on addressing gaps or perceived weaknesses in the establishment’s work.

The integration of a number of artificial intelligence technologies such as data mining, smart neural networks, fuzzy logic, and expert systems, with traditional procedures and statistical methods may help in analyzing stored data to support information security management processes.

And the discovery of manipulation and espionage. These technologies improve the ability of information security management systems to link and analyze

Events resulting from various types of modern tools used in network management and control.

E-crime costs the global economy about $ 445 billion annually, and e-crime is the second most common economic crime at 37% after embezzlement of funds and assets in the Middle East, according to a survey on global economic crime 2014.

Problematic:

Therefore, the forms that we are going to address in this research paper are as follows:

Dade Economy, How can the use of artificial intelligence technologies and expert systems in the face of cybercrime that many countries and thus eating away the forces of the global economy?

Accordingly, we will try to answer the problem of the study by dividing the research paper into three main parts:

- Economic crimes in the virtual world.
- Legal and judicial measures and measures to combat economic crimes in the virtual world.
- The role of expert systems and artificial intelligence in strengthening information security.

so the problematic is:How artificial intelligence is aiding the fight against cybercrime?

Economic crimes in the virtual world

it is a crime of a material nature, which is represented in all unlawful behavior through the use of electronic devices, from which the criminal obtains material or moral benefits with the victim downloading a corresponding loss and often the goal of these crimes is piracy from In order to steal or destroy the information in the devices and then blackmail people using that information. Hence the need arises for a strong wall to protect companies from these risks, which is information security, which is an issue that examines theories and strategies for providing information protection from the risks that threaten This is from assault activities.(Anderson and Raine, 2018).

From a technical standpoint, they are the means and procedures required to ensure that information is protected from internal and external threats.

From a legal point of view, information security is the subject of studies and measures to protect confidentiality and integrity of the content of information and combat activities that attack it or exploit its systems to commit crime, which is the goal and purpose of information protection legislation against illegal and illegal activities targeting information and its computer and Internet crime systems.

Law experts define cybercrime as: anyone who is caught inside the automatic data processing system or a part of it, and this method results in one of the following: erasing data, modifying data, or disrupting the operation of the system, and defines information security as "providing the means and procedures that achieve protection from future events Unwanted, these are system particles.(Hamid Jahankhani, Ameer Al-Nemrat, Amin Hosseinian-Far, 2014).

Motives for committing electronic crimes: There are several motives for committing these crimes, including the following:

A. Political and military motivation: There is no doubt that the scientific and technical development has led to almost complete dependence on computer systems for most of the technical and information needs.

Since the end of the Cold War and the information conflict between the former Soviet Union and the United States of America, and with the emergence of new areas of conflict in the world and the changing informational nature of systems and countries, dependence on the computer and thus the penetration for political, military and economic information has become a more important issue;

B. Commercial motivation: It is known that the major commercial companies are also living with each other a war raging, and that a number of major commercial companies are being subjected to many attempts to penetrate their networks every day.

C. Individual motivation: The first individual penetration attempts among university students in the United States of America began as a kind of ostentation of success in penetrating the

personal devices of their friends and acquaintances, and soon that phenomenon turned into a challenge among them in penetrating the systems of companies and then the websites. The motivation is not limited to individuals only Rather, there are groups and unions that are similar to clubs and are not the same commercial targets.(Fatiha Rassaa, 2012).

D. Money crimes in the scope of electronic commerce:

It is one of the grave risks facing this government, and among the crimes that can take place in this scope are:

(1) Theft of information by hackers and spying on clients' accounts in banks;

Tampering with magnetic cards and using them to tamper with clients 'accounts or transfer amounts of their money to the accounts of the pirates themselves;

Destruction of networks or electronic devices, either in a physical way, such as pouring cold or hot liquids on the electronic supports on which data or information is stored, or by planting viruses (logical bombs, time bombs, trap door, electronic worm, Trojans) that work in total or partial disruption To create networks or to distort information provided by e-government to individuals.

(2) Credit card burglary crimes:

With the beginning of the use of credit cards through the internet and accompanied the emergence of many hackers to rob them relentlessly, credit cards are electronic money and seizing it is taking possession of the money of others. With the development of the concept of electronic commerce, many business companies have used the Internet and benefited from the benefits of trade.

Grabbing credit cards is not a difficult place, for credit card thieves, for example, can now steal hundreds of thousands of card numbers in one day through the internet and then sell this information to others. The matter exceeds the security risks that current credit cards can be exposed to. Now at the beginning of a monetary revolution called electronic money, which is expected to be

complementary to paper or plastic money, it is also expected that the dependence on this new and modern type of money will increase to gain the confidence that traditional money possesses.

(3) Online gambling:

In the past, gambling required that players be together at the same table in order to be able to play gambling. Now, with the spread of the Internet on the world level, gambling has become easier and tomorrow, players have wrapped around one page of the Internet pages worldwide and from separate places easier than before. . Many sites specialized in gambling games also competed to provide the pages of their sites with a lot of programs, given that players can play and each in his home, and money laundering often interferes in a way that is done on the internet and, for example, with the widespread gambling clubs, which made virtual casino sites The Internet is subject to suspicion and control by the American authorities, and despite the legality of gambling clubs in America, the legal problem facing owners of virtual gambling sites on the Internet is that they are not yet authorized in America, unlike in Las Vegas.

(4) Data fraud:

Data forgery crimes are among the most common crimes among all types of crimes committed, whether on the Internet or within computer crimes, given that it is not without a crime unless one of its details is a crime of data forgery in one way or another, and data forgery is by entering on a rule Existing data and modifying that data, whether by canceling data that already exist or by adding data that did not exist before.

The most common cyber threats in the region are applications, systems, and networks, in addition to the risks to mobile devices, storage devices, and mobile data in the third party, according to the PriceWater and Skopers study.

Among the recent examples that the Middle East region has witnessed in terms of electronic threats on a large scale what happened in 2012 when two major oil and gas companies were attacked.

An electronic technology has severely disrupted the work of tens of thousands of computers.

According to Allen Penel, Regional Vice President, Middle East, at Fortinet, the threats are becoming more sophisticated and financial services companies are becoming a showcase of many sophisticated attacks, pointing out that many IT security companies in the region are rethinking the information security strategy It has replaced traditional protection software to meet increasing data and information requirements while at the same time addressing the increasing number of complex threats. He added: “We at Fortinet advise customers to adopt technologies that have the least impact on the speed of network performance by allowing deep checks and accurate content analysis procedures and avoiding the use of products that operate at multiple points. We have products that have high performance, efficiency and moderate costs that are now used Wide range with the most prominent banks and financial institutions in the region. ”

"Recently, financial institutions in the Middle East and the world have had to deal with various threats with a devastating effect, which has necessitated a rethinking of network protection measures," said Joaquin Sandberg, designer of security solutions at FIVE. In parallel, F5 has developed a reference infrastructure to protect against various threats, which is a strategy for several levels that provide flexibility and risk management capability to mitigate the most impactful DDoS attacks. ”

It is noteworthy that the UAE has intentionally placed emphasis on the cyber security network and has become a leader in the region and the world. The UAE has attached great importance to cyber security as it ranked first at the level of the Gulf Cooperation Council states and the fourth globally in 2012 according to the report of the International Institute for Administrative Development, Switzerland, which showed that the UAE jumped in the ranking from 35th globally in 2011 to fourth place.

Legal and judicial measures and measures to combat economic crimes in the virtual world

States are seeking to establish new international measures to combat cybercrime by considering negotiating a new global legal instrument on cybercrime within the framework of the United Nations.

This instrument should be considered taking into account, inter alia, the concerns and interests of all Member States and the draft United Nations convention on cooperation in combating cyber crime.

Member States should promote international cooperation in combating cyber crime.

It is initiated by taking advantage of existing instruments and by concluding bilateral agreements based on the principle of providing support, in cooperation with the United Nations Office, to the process of networking and information exchange between the judicial and law enforcement authorities on a regular basis.

Countries should enact substantive legislation addressing new and emerging forms of cybercrime that formulate them in a technologically neutral language to ensure that they keep pace with future developments in the field of information and communications technology.

The use of artificial intelligence in storing electronic information and 'searching and reserving data stored in digital devices, which are the most important evidence to prove the charge of committing an electronic crime.

The role of expert systems and artificial intelligence in strengthening information security.(Daniel Küpper, 2018).

There are a set of administrative and technical procedures that can be used in this regard to achieve information security, as follows:

(1) Administrative measures for information security: The governments that adopt providing electronic services to citizens must perform several tasks towards information security, such as oversight and supervision of information security, and major tasks that they must perform will be reviewed, as follows:

(2) Providing hardware security: To secure the devices, the building must be secured as not allowing unauthorized persons to enter the computer room and storage media storage facility. It is preferable to use modern technology to enter systems such as: fingerprint, fingerprint, magnetic card ... etc.

(3) Providing data security: the administration must distribute powers and responsibilities according to the organizational structure in a manner that ensures raising the security level, reducing crimes, and setting up a mechanism to be implemented to carry out backup and secure external storage media to ensure its security and updating, and controls must be formulated to regulate the operations of operations, and for database programmers And its managers, for managing networks and communication lines, for input and output operations, and security controls for building and operating application programs.

(4) Providing individual security: When the administration wants to protect its information, it must follow administrative procedures in the field of individual security as follows:

Preventing temporary employment permanently, and taking into account procedures to end the employee's service by requesting the delivery of everything in his possession such as keys and magnetic cards, and changing the password before leaving it:

- Follow-up of employees and their forced transfer between the various departments in the department, noting those who do not request leave by forcing them to leave and monitoring the system afterwards to ensure that there are no defects that they avoided by their presence;
- Holding seminars, conferences and lectures periodically in the field of information security, and displaying internal bulletins and management instructions that include informing individuals of important information in the field of security, to compel workers to specific administrative systems;
- Paying workers to attend international exhibitions of hardware and software, and sending them to specialized information security courses, so that they have a strong background in order to achieve information security;

Grant incentives and link upgrading and courses to the extent of information security compliance.

(5)Providing an Information Security Department: The large organization appoints an Information Systems Security Director who is directly linked to senior management to the importance of the reports he prepares.

The Security Director heads a separate section of information security professionals who have technical and security expertise in data processing and programming according to operating systems, programming languages and databases used in the organization, and are trained in security coordination and have sufficient capacity to deal with information systems crime and emergency situations.

Technical measures for information security:

There are a set of technical measures that institutions must provide to protect their information, including:

Providing electronic protection: Electronic protection is subject to the settings of the computer and the attached devices, and it can be shown as follows:

- Delete unnecessary files even if the information they contain is insignificant and useless, and make sure not to keep them in the Recycle Bin.
- Detecting the computer after an absence by the explorer, and installing programs that prevent the erasure of information from such as the explorer's password protection system, or using programs that keep the operations performed, for a large number of passwords.
- Exploiting the file program to be protected. Compress the files and protect them with a password;
- Ensure that there are no Trojan spyware in the event of connection to networks in the computer;

- When using the Internet, the user's password should not be saved at the time of accessing the Internet, and the browser should be closed if it is away from the device in order to disable the reverse feature in the browser, and not to use the remember username and password feature:

When using e-mail attached files should only be opened after confirming them;

It is necessary to install anti-virus software on the machine and run it for the entire period of use of the device, and it is also necessary to update the virus explorer programs periodically.

Securing all network components: In the case of using networks, protection in this case depends on personal verification, to enter the network, and on network security means that must be fully examined and assess the possibility of penetration of the protection system and identify those risks related to design and management.

Use of encryption: Sending data over the network makes it easy to eavesdrop, and the only way to prevent this is known as encryption. Eavesdropping is to use encryption. It is the process of converting information into incomprehensible codes that seem meaningless to prevent unauthorized persons from seeing or understanding the information, and for this the encryption process involves converting regular texts into encrypted texts. The Internet is the largest medium for transmitting sensitive information, and in order to maintain its safety and security, it must from encrypting it. Three methods of encryption can be used as follows:

- Digital certificates: The digital certificates are issued by trusted donors who sign them and use these certificates to verify the reliability of the public keys that have been issued.
- Electronic fingerprint: It is a digital fingerprint that is derived according to certain algorithms called functions or camouflage coupling.
    - Digital signature: The digital signature uses the message that came from its source without being subjected to any change during the transfer process and the sender can use the private key to sign the document electronically. As for

the receiving end, the signature is verified by using the appropriate public key. And using the digital signature is secured The integrity and validity of the message, and a benefit of this signature is that it prevents the sender from denying the information he sent.

Use of passwords: The security of information systems requires the use of complex passwords to log into a network or computer, and strong passwords are important considering that password detection tools continue to improve and as the computers used to discover them become more effective than before , And it is now possible to easily crack network passwords.

The role of expert systems and artificial intelligence in activating corporate protection

The goal of using 10 AI-enhanced expert systems is to develop and improve cosplay-sized surveillance and decision-making processes beyond the capacity of information security experts. In addition to improving the process of creating a knowledge base regarding threats, policies, procedures, and risks related to information security. (Barman S, 2019). And the ability to adapt and support the model to handle and classify events and data that lead to the possibility of predicting attacks and determining appropriate treatment methods before they occur. And one of the most important components of the system's core, according to expert opinions, is the ability to develop a smart model that analyzes and connects events and data instantly (i.e. at the time of occurrence) in order to increase detection and prevention capabilities in security technologies: phishing detection systems, anti-virus programs, filtering advertising messages, and evaluation systems Weak points. for example:

Hazardous models should be used in risk management, which is considered one of the most important stages of information security management.

Artificial intelligence areas:

With the rapid advancement of computer technology and the fact that computers are originally designed to collect, store, process and use information, artificial intelligence technologies and applications are expected to become an important part of our lives.

Neural networks are divided into several parts, including: Expert systems The representation of sensory capabilities of a person can be divided into understanding natural languages, floating logic, robotics, especially computer vision, and these parts often intersect with each other ... the customer, the computer.(Jacques Bughin, 2017).

Smart systems consist of two main parts:

(1) The internal - mathematical part: which can be classified into four partial systems: sensory processing, sensors are used as an input tool in smart systems and as a tool for monitoring the outside world of the system and the system itself.

Modeling the world or the environment: It includes knowledge databases about the system world and a simulation unit, which builds a future state of the system world.

Behavior Creation: The decision-making unit, which selects objectives, plans and executes tasks.

Self-evaluation: evaluation of the perceived state of the system and the predicted state.

(2) Interactive outer part: the inputs and outputs to and from the smart system are either through sensors or actuators, which are the external parts of the system. (Actuators) way of sensors or actuators. Working method: Sensory processing processes the recorded data from the sensors to obtain the internal model of the system world and save it, then the behavior creation system selects the context of the actions to achieve the goals and controls the triggers to follow the behavioral goals within the context of the perceived global model. The data generated by the sensors is the basis for building knowledge bases, discovering attacks on the system and anticipating them before they happen, as well as making immediate time decisions. Examples of sensors data include measurements related to the performance, security, and condition of the following: (Bernard Marr, 2017)

Devices such as CPU performance: memory usage, disk space used, and number

Files used in active connections, number of failed system access attempts, number of operations (from queries, updates, and deletions), response time to requests, number of privileged users entering the system at the same time, number of changes in system settings, number of expected connections, and percentage of use System files, system clock monitoring, system clock synchronization protocols, and system log file size.

Network such as available communication capacity: delay, requests to enter the network, number of unavailable sources for part-time use, number of open ports, number of operations on the Internet, changes in network settings, number of dropped packets, number of emails and use of - interfaces such as statistics Use - the environment around the system such as temperature and alarms security guarantees: firewall, interference detection systems, antivirus software, virtual personal networks, and encryption) such as the number of rejected connections, the number of warnings, and maintenance times, number of software updates, number of keys used in the encryption and decryption process, and remote access, security Policies. (Casey Crane, 2019).

Emergency and recovery plans: Security and network managers activities (access, changes to settings, software installation and update, and number of notifications.

Characteristics of expert systems - advantages and disadvantages

Advantages:

The expert system is not forgotten while the human expert does not have this advantage:

Several copies of the expert system can be quickly copied, while training an expert before another is a long and stressful process. Building an expert system in itself may be costly, but the cost of development and maintenance can be distributed to several investors, and thus the overall cost is acceptable compared to the cost of the experienced person. An expert system treats similar issues in the same way, while an expert can be affected more by several factors, including:

- The latest information.
- The first information he obtained.
- The expert system can document its decisions permanently.

- The possibility of combining the experience of more than one person in one system.

Defects:

The experienced person is aware that the experienced person can respond to an unusual situation while the expert system cannot do this. The expert person adapts to changing circumstances while the expert system needs to update the conditions. Also, expert systems are limited to problems beyond their area of expertise.

As a result, it can be said that in some cases in the Bugs program, for example, anticipating the weather or searching for malfunctions - the expert system can be faster and / or more accurate than a person, but in other areas such as medicine, the expert system is an effective auxiliary - not a substitute - for The human expert. (Louis Columbus, 2018).

Conclusion:

Electronic crime is characterized by supernatural intelligence compared to traditional crime that is violent, and for this it is called the criminal of smart people, because it depends on advanced technological means to destroy or penetrate government websites or piracy of information about individuals and attack their privacy, and therefore, we can confirm that the success of information security depends a lot On the success of the protection system adopted by companies and economic establishments, which must be effective civil, criminal and information protection. Information protection is achieved by developing scientific research for security systems in order to secure their data and information from piracy and misuse, and discover cases of piracy if that happens.

Artificial intelligence is one of the main axes of contemporary scientific research, where the great and rapidly growing interest in it revolves around reaching smart systems that are able to behave similarly - as possible - to human behavior.

On the other hand, attention should be paid to the legal aspect in the process of combating cybercrime by creating methods and measures that are in line with the digital environment and commensurate with the nature of development, especially in terms of digital evidence, discovering criminals in the virtual space and using electronic devices to combat piracy.

And the use of experts in artificial intelligence to detect and eliminate viruses, and enlist new legislation related to cybercrime.

:rencesRefe

1. Janna Anderson and Lee Raine,(2018), the future of well-being in a tech-saturated world, april 17, accessible at: https://www.pewresearch.org/internet/2018/04/17/the-future-of-well-being-in-a-tech-saturated-world/
2. Hamid Jahankhani, Ameer Al-Nemrat, Amin Hosseinian-Far, (2014), Cyber Crime and Cyber Terrorism Investigator's Handbook, Chapter: 12, Publisher: Elsevier Science, Editors: Francesca Bosco, Andrew Staniforth, Babak Akhgar..
3. Fatiha Sarae, (2012), criminal protection of information on the internet,
4. Barman S, (2001), Writing Information Security Policies, New Riders Publishing, .Available at: http://Safari.informit.com November.
5. Daniel Küpper,(2018), Artificial Intelligence in the Factory of Future, (Boston: The Boston Consulting Group, April
6. Jacques Bughin,(2017), Artificial Intelligence: The Next Digital Frontier?, june, Access at : MGI-Artificial-Intelligence-Discussion-paper.pdf
7. Bernard Marr, (2017), The Biggest Challenges facing Artificial Intelligence)AI(in Business and Society, Forbes , July 13, ,accessible at: https://www.forbes.com/sites/bernardmarr/2017/07/13/the-biggest-challenges-facing-artificial-intelligence-ai-in-business-and-society/ 30/01/2019
8. Casey Crane, (2019), Artificial intelligence in cyber security: The savior or enemy of your business?, July 17, accessible at: https://www.thesslstore.com/blog/artificial-intelligence-in-cyber-security-the-savior-or-enemy-of-your-business/ 30/01/2019.

Louis Columbus, (2018), 10 Charts That Will Change Your Perspective On Artificial Intelligence's Growth, Forbes, January12, accessible at: https://www.forbes.com/sites/louiscolumbus/2018/01/12/10-charts-that-will-change-your-perspective-on-artificial-intelligences-growth/#16fe85b24758