CYBERCRIME FOLLOW-UP PROCEDURES – A COMPARATIVE STUDY OF ALGERIAN AND QATARI LEGISLATION.

Zerrouki Assia[1], Hamel Mohamed[2]
[1]University of Ghardaia, Faculty of Law and Political Science (Algeria).
[2]University of Laghouat, Faculty of Law and Political Science (Algeria).
The Author's E-mail: zerrouki.assia@univ-ghardaia.dz[1], m.hamel@lagh-univ.dz[2]
Received: 10/2023 Published: 04/2024

Abstract:

This research paper aims to examine the issue of cybercrimes as a newly emerging legal issue, coinciding with the widespread adoption of the technological revolution. This revolution has had a significant impact on various aspects of economic, social and administrative life. In this article, we try to highlight the interest of the Algerian and Qatari legislatures in regulating and combating cybercrimes, considering them as newly emerging crimes resulting from the misuse of information technology.

Keywords: *cybercrime, computer crime, cyber offences, Algerian legislation, Qatari legislation.*

INTRODUCTION:

The world is witnessing an unprecedented and remarkable development, and if the law is a product of social thought, it evolves as society evolves. It is no secret that the phenomenon of crime is also growing and evolving, taking on dangerous and complex dimensions that were not previously anticipated. Crime is no longer confined to its traditional concepts and forms, but has diversified into an organised system that emerges from the fabric of planning and management, ultimately embodying a structured construction governed by rules and behaviours that are difficult to contain and control[1].

From here, the world speaks of a global communication network that goes beyond the transmission and reception of materials, but rather facilitates the transfer of human beings, with all their senses, without leaving their place, from one end of the earth to the other, in order to connect and interact with their counterparts from that distant end[2].

The rapid and astonishing development of the means of communication in recent decades has provided significant services to people in various aspects of their lives. Telecommunications technology and information systems have facilitated the conduct of many daily, commercial, industrial and cultural transactions and interactions. However, this progress and advancement has not been without some negative aspects that have accompanied its spread. Crime has found new horizons that were not available in the past, as these vast spaces have stimulated the imagination of many to invent forms and means that were unknown in previous societies.

This development has given rise to a new type of crime, some of which is new and some of which is innovative. There is even disagreement about what to call them. Some call it cybercrime, while others use terms such as computer crime, information system crime, or crimes committed in the virtual world. What is known is that both ordinary crime and cybercrime have a perpetrator and a victim. The perpetrator in this crime has a computer.

Cybercrime affects money and people in the same way as conventional crime. However, the difference can be justified from two perspectives.First, the tools used in cybercrime are highly sophisticated and efficient. Secondly, the perpetrators of these crimes are usually highly intelligent, as they know how to use these tools and devise new methods and means to facilitate their crimes[3].

Based on what you have said, it can be said that cybercrime is the most common type of crime today because it has many advantages for criminals that drive them to commit it. These crimes can be defined as crimes that do not recognise geographical boundaries ("crimes trans border") and are committed through the use of a computer tool via the Internet by individuals who have advanced knowledge of both[4].

Based on the above statement, this study will focus on the monitoring procedures in electronic crimes through a comparative study of Algerian and Qatari legislation. Therefore, the research problem of this study revolves around the following question What are the monitoring procedures identified by Algerian legislation and Qatari legislation to combat electronic crimes?

In order to answer the research problem, the study is divided into two main axes:

Axis 1: The concept of cybercrime:

E-crime is considered to be an emerging crime that has become widespread in recent years because it is a new crime that arises from the unauthorised use of information technology to attack financial assets and intellectual property. Various concepts have been used to define these crimes, as they are a new phenomenon that has kept pace with technological and information developments. It is impossible to provide a definitive definition of cybercrime due to the constant evolution of technology and information systems.The terms used to describe this type of crime have also varied, such as computer crime, Internet-related crime, information technology crime, misuse of information technology, as well as the widespread use of the term "economic crime" for hackers and crimes in the virtual world, such as "cybercrime" or "cyberspace crime". As a result, numerous definitions have emerged, each defined by researchers based on their perspective of electronic crime, such as unauthorised actions, copying, deleting, entering falsified data, etc[5].

Firstly, the definition of electronic crime and its characteristics:

The issue of defining electronic crime has been the subject of the efforts of jurists who have proposed different definitions. This will be clarified through the terminological definition of cybercrime and an examination of the linguistic and legal definitions in Algerian and Qatari legislation.

A. Linguistic definition:

Before delving into the legal definition of the term "cybercrime", it is necessary to begin with the linguistic definition, as the meanings attributed to words in language often influence commonly accepted terminology and meanings. The term "electronic crime" is composed of two words: "electronic" and "crime". The word "crime" has its roots in the concept of wrongdoing, violation and guilt. It is said to be a Persian word that was Arabised. "Crime" is derived from the root word "jarim", which means to commit an offence or transgression against oneself or others. It can also refer to what a governor takes as tribute or what a person acquires unlawfully. In addition, "jarimah" refers to the sound that is made loudly, and "jarimah" can mean what a sinner gives to a ruler or what a person unlawfully acquires. Therefore, "jarimah" can mean a crime, offence or transgression[6].

B. Legal definition:

Jurists and scholars have provided numerous definitions of cybercrime, which vary depending on the background of the scholar and the criteria used for the definition. We have attempted to summarise most of the definitions proposed in this area.

Some definitions are based on the nature of the crime or the types of behaviour that are criminalised. For example, Professor Rosenbalt defined electronic crime as "an unlawful activity aimed at copying, altering, deleting or accessing information stored in or transmitted by a computer". Similarly, the lawyer Solares defined it as "a pattern of known crimes under criminal law, as long as they are related to information technology".

Other definitions focus on the means used to commit the crime, asserting that electronic crime is committed using a computer as the primary tool. Examples of such definitions include Professor John Forrester's definition of cybercrime as "a criminal act that uses the computer as its principal instrument" and Tadman's definition of cybercrime as "all forms of unauthorised behaviour facilitated by a computer"[7].

In addition, some definitions provided by legal and relevant institutions emphasise the personal characteristics of the perpetrator. The United States Department of Justice, in a study conducted in collaboration with the Stanford Research Institute and adopted in its 1979 guide, defined cybercrime as any crime committed by a person with technical knowledge of computers. Professor David Thompson defined it as "a crime that requires the perpetrator to have knowledge of computer technology"[8].

It is worth noting that some criminal laws do not provide a specific definition of electronic crimes, including Jordan's Electronic Crimes Law No. 27 of 2015 and Sudan's Information Crimes Law of 2007. We support the approach taken by these legislations, as there is no comprehensive definition that can encompass all types of electronic crimes, given their diverse methods and rapid evolution.

1- Definition of electronic crime by the Algerian legislator:

The Algerian legislator has defined the concept of crimes related to information and communication technology in Law 09/04, which contains specific provisions to prevent, combat and punish crimes related to technology. Similarly, Law 21/11 of 16 Muharram 1443, corresponding to 25 August 2021, amended Law 66/155 of 18 Safar 1386, corresponding to 8 June 1966, which includes the Algerian Code of Criminal Procedure[9].

On the basis of the above legal texts, it is worth noting the terminology used by the Algerian legislator in relation to this type of offence. Contrary to the terminology used in jurisprudence and some comparative legislation, such as "cybercrime", "electronic crime", "information crime", "Internet crime" and others, the Algerian legislator has adopted the term "crime related to information and communication technology" in an attempt to extend the scope of criminalisation as much as possible. This is intended to draw attention to criminal behaviour that goes beyond interference with or manipulation of computerised data and includes the use of technological means to commit traditional forms of crime.

This approach aims to achieve the principle of legality and to ensure the application of criminal provisions specific to crimes related to information and communication technologies to all behaviours recognised as such crimes. The Algerian legislator intervened by providing a legal definition of crimes related to information and communication technologies through Law 09/04. Law 21/11 also makes an important addition in this respect.

In article 2, paragraph A, of law 09/04, the legislator defines these crimes as "crimes against automated data processing systems as defined in the penal code, as well as any other crime committed or facilitated by means of an information system or electronic communication system"[10]. And through this text, it appears that the Algerian legislator has effectively established the definition that combines the behaviours affecting automated data processing systems, which are specified in the Penal Code as information crimes, and the range of acts committed through or against information systems.

The first category includes the behaviours that affect the automated data processing system, while the second category includes the traditional crimes that are committed or facilitated through an information system, which are different from those specified by the legislator in the Penal Code and those addressed in specific texts.

With regard to Law 21/11, we note that the legislator has maintained the same definition of information and communication crimes in Article 211, repeated 23. However, there are two new aspects:

1. The specification of the categories of crimes that fall exclusively under the jurisdiction of the judicial pole, as well as the use of the term "crimes related to information and communication technology", which includes all crimes related to information and communication technology, in an attempt to extend criminalisation to everything that is done or connected to information systems.

2. The adoption of a more complex concept of crimes related to information and communication technology, which is defined as "...a crime which, due to the multiplicity of actors, partners or victims, the wide geographical scope of its commission, the magnitude of its effects, the resulting damage, its organised nature, its transnational character or its impact on public order and security, requires the use of specialised investigation methods, expertise or recourse to international judicial cooperation"[11].

D. The definition of electronic crimes in Qatari legislation:

The Qatari legislator defines electronic crimes as "any act that involves the use of information technology means, an information system or a computer network in an illegal manner that violates the provisions of the law"[12]. This definition is similar to the definition adopted by the Kuwaiti

legislator, which defines electronic crimes as "any act involving the use of a computer, information network or other information technology means that violates the provisions of this law"[13].

However, there is a difference between the two legislations in the terminology used to describe these crimes. The Qatari legislator refers to them as "electronic crimes", while the Kuwaiti legislator refers to them as "information crimes".

Thus, the Qatari legislator identifies the occurrence of electronic crimes based on the presence of three elements: the use of technological means, an information system or a computer network. The intended meaning of these three elements is explained as follows:

1. Information technology means: It refers to any physical or non-physical medium or set of interconnected or non-interconnected means used to store, organise, retrieve, process, develop and exchange information according to stored commands and instructions. It includes all wired inputs and outputs associated with it within an information system or computer network.

2. Information system: A collection of programs and devices used to create, extract, transmit, receive, display, process and store information.

3. Computer network: It refers to the interconnection of various information technology means for accessing and exchanging information, including private networks, public networks and the global network (the Internet)[14].

Second - The forms of electronic crime in Algerian and Qatari legislation:

Traditional crimes are classified according to their severity into felonies, which are the most serious crimes, misdemeanours, which are of medium severity, and violations, which are less serious. They are also classified according to their nature as common crimes, political crimes, military crimes and terrorist crimes. In contrast to these crimes, cybercrime has seen variations in its classification and forms due to differences in terminology. Each approach is based on a specific criterion. Some classify them on the basis of the method used to commit the crime, others on the basis of the motive for committing the crime, and others on the basis of the multiple locations of the attack and the multiple rights violated[15].

As far as the Algerian legislator is concerned, electronic crimes are divided into crimes committed using information systems that are not specified by the legislator, thus including all crimes committed using information and communication technology. The second type of crimes are those committed against information systems, which are defined by the legislator in the Penal Code.

1. Forms of electronic crime in the Algerian Penal Code: The Algerian legislator has defined the forms of electronic crimes in the Penal Code as follows:

A. Electronic crimes committed through information systems: This category includes major crimes related to information technology. The computer is considered a means of facilitating and amplifying the criminal result, and these crimes include crimes against individuals, crimes against other information systems and crimes against secrecy[16].

B. Electronic crimes against natural persons: These crimes are further divided into crimes against intellectual property and crimes against privacy.

C. Electronic crimes against intellectual property rights: The information system is used as a means to infringe intellectual property rights. Examples include unauthorised access to databases and unauthorised storage and use of information.Unauthorised use of certain information without the owner's permission is considered a violation of moral rights and a violation of its financial value, since information has literary value and falls within the scope of intellectual property rights, including copyright and patent rights, as defined in Algerian legislation on copyright and related rights in Order 05/03 of 2003 and Order 03/07 on patent rights[17].

D- Electronic crimes against privacy:

The Algerian Constitution emphasises its commitment to protecting the personal privacy of citizens and to preventing violations of that privacy. As computers serve as repositories of vital information about individuals, they have facilitated unauthorised access to this information by third parties for various purposes.

E. Computer crime against other information systems: This crime is committed by a person physically accessing the data processing centre or by using specific electronic tools to intercept and spy on information within information systems. It also includes credit card fraud[18].

F. Electronic Secrecy Crime: This category includes two types of offence. The first relates to crimes against state secrets, as the Internet has enabled many countries to engage in espionage and to access military and economic secrets of other nations, particularly those involved in conflicts. The second type is crimes against professional secrets. The aim of these crimes is to steal information with the intention of defaming a particular person or group. The Algerian legislator has taken measures to protect these secrets by repeating articles 61 to 96 of the first chapter of the Penal Code, which deals with crimes against public interests[19].

B. Electronic crimes against information systems: The Algerian legislator filled the gaps in Algerian legislation in this area by adopting Law No. 04/15 of 10 November 2004, which contains provisions criminalising various attacks on data processing systems.The text of the law addresses these offences in the repeated seventh section of the Penal Code, entitled "Interference with data processing systems", specifically in Articles 394 to 394/7. The forms of attack include unauthorised access to and presence in an information system, manipulation of an information system and other forms of fraud[20].

First point: Unauthorised entry and stay in a system:

Article 394 bis of the Algerian Penal Code provides for the punishment of anyone who enters or remains, or attempts to enter or remain, in any part of the data processing system by fraudulent means, and if this entry or presence results in damage to the information system, the penalty is doubled. The simple form of the offence consists in the mere entry or presence, while the aggravated form occurs when this unauthorised entry or presence results in the deletion or modification of the data present in the system[21].

1- Unauthorised entry: By this we do not mean physical entry, i.e. entering a specific place such as a house, but it is considered as a mental phenomenon, similar to when we talk about entering an idea or possession of a thought in human thinking. It refers to entering the mental processes carried out by the data processing system, and it is not necessary for the person to capture or obtain the information within the system or any part of it. The offence is committed even if the perpetrator does not have the technical ability to perform operations on the system. Unauthorised entry includes all categories of fraudulent entry into a protected or unprotected system, including the use of a key by a subsequent person to access the system.

2- Unauthorised stay: Article 394 bis of the Algerian Penal Code deals with the offence of unlawful entry and presence in a system. It states that anyone who enters or remains, or attempts to enter or remain, any part of a computer system by means of deception shall be punished. If this entry or remaining results in damage to the information system, the penalty is doubled. The simple form of the offence consists of the mere act of entering or remaining, while the aggravated form occurs when this unlawful entry or remaining results in the deletion or alteration of data present in the system[22].

The second provision: The offence of interfering with an information system:

Article 394 bis 1 of the Criminal Code No. 04/15 criminalises anyone who enters data into an automated processing system or modifies such data by means of deception. This criminal behaviour takes three forms: input, deletion and modification. The Algerian legislator does not require a combination of these forms; it is sufficient for the perpetrator to commit one of them in order to fulfil the material element. The acts of inputting, deleting and modifying involve the manipulation of data contained in the automated data processing system, including the addition of false data, the deletion of existing data or their modification. This behaviour includes acts of sabotage and manipulation of data within the automated processing system, such as the introduction of computer viruses to destroy programs.

The third provision: Other offences: Article 394 bis 2 of the Penal Code criminalises the following acts: designing, researching, compiling, providing, publishing or trading in data stored, processed or transmitted by means of an information system capable of committing one of the aforementioned

computer fraud offences[23]. In addition, Algerian legislation criminalises the possession, disclosure, publication or use, for any purpose, of data obtained through computer fraud[24].

An examination of the various forms of cybercrime in Algerian legislation reveals that these crimes have a distinct and unique nature. They are considered non-violent crimes because they are not characterised by physical violence in their consequences. Just pressing a key or a combination of keys on a keyboard can lead to the commission of serious crimes in a matter of seconds, without any direct contact between the perpetrator and the victim.This difficulty in combating electronic crime is a major challenge.

The Algerian legislature has been criticised for focusing its provisions on specific electronic crimes and neglecting the electronic offender. The legislator has not addressed the electronic offender in any legal text, including defining his characteristics or providing relevant provisions.

2. Forms of Electronic Crimes in Qatari Legislation:

Pursuant to Law No. 14 of 2014 on Combating Electronic Crimes in Qatar, the Qatari legislature has categorised electronic crimes into different forms in the second chapter of the law. These forms include crimes related to intrusion into electronic systems, content crimes, forgery and fraud crimes, electronic card crimes, and crimes against intellectual property rights[25].

A. Crimes of intrusion into information systems, programmes, networks and websites:

The Qatari legislature has divided crimes related to unauthorised access to information systems, network programmes and websites into three types, each of which carries a specific penalty. The law has also increased the penalties for certain cases that are specifically mentioned. The types of crimes and their corresponding penalties are as follows:

Type 1: Crime of unauthorised access to a website or information system belonging to the state or one of its institutions, bodies or affiliated companies:

The penalty for this crime has been increased because it involves accessing, deleting or damaging data. The offence includes:

- Obtaining electronic data or information.
- Obtaining data or information that affects the internal or external security of the State or the national economy.
- Obtaining classified government data or data on the basis of instructions given.
- Obtaining undeserved money, services or benefits.
- Causing damage to beneficiaries or users.
- Deleting, damaging, destroying or spreading electronic data or information.

Type 2: Crime of intentional unauthorised access, by any means, to a website, information system or computer network, or to an information technology tool or part thereof, or exceeding authorised access and remaining present after being aware of it[26].

The Qatari legislator has provided for more severe penalties if such unauthorised access results in:

- Deleting, altering, adding, disclosing, damaging, altering, transferring, capturing, copying or republishing stored electronic data or information.
- Causing harm to users.
- Destroy, suspend or disable a website, information system or computer network.
- Altering a website, disabling it, altering its content, design, or usage, or impersonating its owner or administrator.

Type 3: Crime of intentionally intercepting, disrupting or eavesdropping on data transmitted through a computer network, information technology tool or traffic data.

B- The types of offences related to terrorist organisations in Qatari legislation are as follows:

C- Creating or managing a website for a terrorist group or organisation on the computer network or any information technology means, facilitating contact with the leadership or members of these groups, promoting their ideas, financing them, or publishing instructions on how to make incendiary or explosive devices or any tools used in terrorist activities.

D- The crime of creating or managing a website through the computer network or any technological means, with the aim of disseminating and promoting false news that affects the internal or external security of the State or its general system, with the intention of causing harm.

E- The offence of producing, importing, selling, offering for sale, using, circulating, transferring, distributing, transmitting, publishing, making available or broadcasting pornographic material involving a child under the age of 18, without taking into account the child's consent to this offence.
F- Crimes committed through the computer network or any information technology means, including:
- Offences against moral principles and values.
- Crime of invasion of privacy.
- Crime of defamation or libel of others.
- Crime of threatening or blackmailing a person to compel them to do or refrain from doing an act.
- Crime of counterfeiting and electronic fraud.
- Crime of falsifying an official or unofficial electronic document with knowledge of the fact. The legislator has increased the penalty for forgery by doubling it, as it relates to trust in the public system.
- Crime of using the computer network or any information technology means to impersonate a natural or legal person, obtaining movable property for oneself or others by fraud, obtaining a document or signing it by fraudulent means, using a false name or impersonating a false capacity through the computer network or any information technology means.
- Crimes related to electronic transaction cards: the crime of using an electronic transaction card, obtaining its numbers or information, or facilitating its unauthorised acquisition through the computer network or any information technology means[27].

Third, the elements of electronic crime:

In general, electronic crime is based on three basic elements, whether it is a traditional crime, a cybercrime or an electronic crime:

1. The material element of electronic crime:

The material element of electronic crime refers to the tangible aspects of the crime that are visible to the outside world. One of the operational challenges of electronic crime is the nature of its material element. The concept of crime focuses on an electronic system that has been unlawfully penetrated, resulting in either physical damage to information leading to the possibility of destruction of property, theft, or suspected forgery through the manipulation of computer data[28].

In traditional crime, criminal behaviour such as theft or forgery is visually observed and confirmed. However, the material element of electronic crime, and in particular the difficulty in physically apprehending it, arises from the fact that the crime is committed using information flowing through computer systems that cannot be physically apprehended. It requires a digital environment, a computer device and an Internet connection. It is essential to understand the inception, initiation and outcome of this activity. For example, the offender may prepare the computer to facilitate the crime by downloading or creating hacking software. They may need to configure pages with offensive content and download them to the host computer. In addition, the commission of offences such as the creation of virus programs in preparation for distribution may not always require preparatory acts. In the field of information technology, however, the situation is somewhat different. The acquisition of hacking programmes and decryption equipment or the possession of child pornography images is an offence in itself[29].

For the material element to be present in electronic crime, the criminal result must be causally linked to the criminal behaviour.

B- The moral dimension of cybercrime:

The moral dimension refers to the perpetrator's intention to achieve criminal results. It includes the elements of knowledge and intent. The Qatari legislator explicitly mentions the moral dimension in Article 32 of the Qatari Penal Code. According to this article, the moral dimension of a crime consists of intent or negligence. Negligence refers to the perpetrator's intention to commit or refrain from committing an act that, due to the perpetrator's mistake, results in a punishable outcome. The perpetrator can be held accountable for the offence whether it was committed intentionally or by mistake, unless the law explicitly requires intent.

Cybercrime, by its very nature, is usually committed intentionally. The perpetrators have the ability to use computers and the electronic environment, and often these crimes are committed by

individuals with high skills in using the Internet. Thus, there is full knowledge and intent to achieve the criminal result[30].

3- The legal dimension (legality) of cybercrime:

The principle of "no crime or punishment except by law" governs the legal dimension of cybercrime.This principle is fundamental to modern criminal law.

It limits the sources of criminalisation and punishment to written laws. The Qatari Permanent Constitution of 2004 explicitly enshrines this principle in Article 40, which states that there can be no crime or punishment except by law.

This principle implies that every criminal act must have a written legal provision specifying the applicable punishment.The legislator has the authority to define and specify the acts that are punishable and to impose penalties on their perpetrators. Qatar's Cybercrime Law No. 14 of 2014 defines various cybercrimes and the corresponding penalties in its provisions.These include crimes related to the violation of information systems, programmes, networks, websites, content crimes, electronic forgery and fraud, crimes related to electronic transaction cards, and crimes related to the violation of intellectual property rights.

The legal provisions define the powers of the criminal judge, who may not impose a penalty for an act that is not expressly punishable by law or impose a penalty that is not provided for by law, within the limits set by the law[31].

The second axis: Confronting cybercrime in Algerian and Qatari legislation:

Looking at the legal texts of the Algerian and Qatari legislators, we find a number of legal provisions established by each legislator to confront this type of cybercrime. Various measures and procedures have been put in place to combat this new form of criminal activity, and a procedural policy has been adopted to combat cybercrime.

First: The Algerian legislator's fight against cybercrime:

The Algerian legislator has addressed the phenomenon of cybercrime and the significant damage it causes to individuals and state institutions. In an attempt to fill the legislative gap in this area, the Algerian legislator has made numerous amendments to national legislation, including criminal legislation, in particular the Algerian Penal Code, in order to bring it into line with developments in criminal law. Specific laws have also been introduced to ensure the criminal protection of electronic transactions.

1. The Algerian legislator's fight against cybercrime through general legislation:

The Algerian legislator has sought to enact general and specific laws, structures and bodies to combat cybercrime. The Algerian legislator has made significant efforts to combat and prosecute cybercriminals, influenced by many Arab countries that have enacted laws to combat cybercrime. One of the areas to which the Algerian legislator has attached the greatest importance is national security and the maintenance of public order.

A. Combating cybercrime under the Algerian Constitution

The Algerian Constitution of 1996[32], as well as the constitutional amendment of 2016, guarantees the protection of fundamental rights and individual freedoms and ensures that human dignity is not violated. These constitutional principles have been translated into practice through the legal texts of the Algerian Penal Code, the Code of Criminal Procedure and other specific laws, which prohibit any violation of these rights. One of the most important general constitutional principles is set out in Article 38, which guarantees "fundamental freedoms and the rights of human beings and citizens". Article 44 also states that "the freedom of intellectual, artistic and scientific innovation shall be guaranteed to citizens, and the rights of authors shall be protected by law". Printed matter, recordings and other means of communication and media may not be confiscated except by a court order. Academic freedom and freedom of scientific research shall be guaranteed and exercised within the framework of the law.

The State shall work to promote scientific research and to value it in the service of sustainable national development. The privacy of individuals, their honour and the secrecy of their correspondence and communications in any form shall be protected by law. The law protects the

rights of authors, and no printed matter, recording or other means of communication and media may be confiscated except by judicial order[33].

B. Cybercrime in the Algerian Penal Code:

The emergence of new forms of crime resulting from the information revolution has prompted the Algerian legislature to address the criminalisation of acts affecting computer systems. This led the Algerian legislator to amend the Penal Code by Decree 04/015 of 10 November 2004, which supplements Decree 22/15 containing the Penal Code. This amendment deals specifically with offences related to computer systems. This section contains eight articles, from article 394 bis to article 394 octies[34], which aim to fill the legal gap. The Algerian legislator, through Law 04/15, has introduced a series of provisions prohibiting acts related to data processing systems and establishing the corresponding penalties for each act. The legislator has established objective legal rules to determine all acts related to data processing systems and the corresponding sanctions and penalties[35].

In addition, the Algerian legislator, through amendments to the Code of Criminal Procedure, has adopted procedural rules for investigations that are adapted to the specific nature of cybercrime.

Article 394 bis states: "Anyone who, by fraud, enters or remains in all or part of a data processing system, or attempts to do so, shall be punished by a term of imprisonment of between three months and one year and a fine of between 50,000 and 100,000 Algerian dinars. The penalty shall be doubled if it results in the deletion or alteration of data in the system, and if the aforementioned acts result in the disruption of the operation of the system, the penalty shall be imprisonment for a period ranging from six months to two years and a fine ranging from 50,000 to 150,000 Algerian dinars.This applies regardless of the domain or nature of the information system and may include violations affecting certain aspects of private life".

Article 394 bis 2 states:"Anyone who intentionally and fraudulently commits the following acts shall be punished

- Designing, researching, collecting, providing, publishing or trading in stored or processed data through an information system that can be used to commit the offences referred to in this section".

Possession, disclosure, dissemination or use for any purpose of any data obtained from any of the offences referred to in this section. Article 394 bis 6 also provides that, in addition to the primary penalties of imprisonment and fines, and while respecting the rights of others in bad faith, supplementary penalties shall be imposed, namely the confiscation of devices, programmes and means used, and the closure of websites that serve as a venue for any of the offences punishable under this section. In addition, the closure of the premises or places of exploitation shall be ordered if the offence has been committed with the knowledge of its owner[36].

C- Tackling cybercrime through criminal procedure:

With regard to criminal proceedings for cybercrime, they are conducted using the same procedures as for traditional crimes, such as search and examination, interrogation of the accused, arrest, seizure, testimony and expertise.With reference to the Algerian Code of Criminal Procedure, article 37 extends the local jurisdiction of the public prosecutor to electronic crimes, while article 45, paragraph 7, allows for search measures in such cases[37]. The search of the information system differs from the traditional search in the general procedural rules in terms of formal and substantive conditions. The legislator has established strict rules for searches as part of the investigation of electronic crimes. Thus, the provisions of Article 44 of the Algerian Code of Criminal Procedure do not apply to electronic crimes. Article 51, paragraph 6, allows detention for the purpose of investigating offences involving data processing systems. Similarly, the interception of correspondence, the recording of voices and the recording of images are permitted under Article 65 bis 5.

The interception of correspondence refers to the interception, recording or copying of correspondence in the form of producible and distributable data, sabotage, reception or display, carried out through wired or wireless communication channels, within the framework of the investigation and collection of evidence of the crime.

The Algerian legislator has specified the conditions and procedures for resorting to this measure in Article 65 bis 5 of the Algerian Code of Criminal Procedure as follows "If the needs of the investigation of a crime caught in the act or the preliminary investigation of crimes involving data processing systems require it, the competent public prosecutor may authorise it:

- Intercepting communications using wired or wireless means of communication.
- Making technical arrangements, without the consent of the person concerned, for the collection, recording, transmission and recording of the spoken words, in particular or in confidence, of one or more persons in private or public places, or for the collection of images of one or more persons present in a private place"[38].

By virtue of this article, the Algerian legislator has authorised the investigation and evidence authorities, in the event of the need to investigate a crime caught in the act or an electronic crime, to have recourse to the interception of wired and wireless communications, the recording of conversations and voices, the capture of images and the use of all the technical means necessary to detect and prove the electronic crime, without resorting to the traditional methods of search and seizure.

It is noteworthy that the Algerian legislator has not granted the right to resort to this measure without surrounding it with all the legal guarantees that prevent arbitrary action by the authorities of investigation and evidence, while protecting the public and private freedoms of individuals[39].

2. Combating cybercrime through specific laws and structures:

Given the seriousness of cybercrime, which requires it to be dealt with by specific provisions in addition to the general rules, and considering that intellectual and literary property is a fertile ground for these crimes, the Algerian legislator has provided it with criminal protection. In order to step up its efforts to combat cybercrime, it promptly adopted a law specifically aimed at preventing and combating offences related to information and communication technologies.

A. Criminal Protection of Computer Data in the Law on Intellectual and Literary Property

The legislator's interest in enacting laws on intellectual property is to protect the human right to creativity and innovation as essential factors in the progress of societies. Therefore, it was necessary for the legislator to provide these components with the protection prescribed in the Law on Intellectual and Literary Property.

Recognition of the description of computer data: This description has been expressly recognised by Decree 03/05 of 19 July 2003 on Copyright and Related Rights in the Protected Description of Computer Media. Any infringement of the financial or moral rights of the author of the program and data, through the acts of imitation referred to in Article 151 of Decree 03/05, is considered a criminal offence, with the penalties set out in Articles 153, 156, 157 and 158.

The offences related to the author's moral rights include:

- Unauthorised communication of literary or artistic works, such as the unauthorised communication of programmes at a time or in a manner that the author considers inappropriate.
- Tampering with the integrity of literary or artistic works, such as modifying, altering, deleting, adding to or transforming computer programs or data without the author's permission.

Copyright related offences include:

- Unauthorised reproduction of the work, as provided for in Article 151, paragraph 1, of Decree 03/05. For example, the reproduction of computer programs or data in any form without the author's authorisation.
- Unauthorised communication of the work, as defined in Article 152 of Decree 03/05. This includes the public communication, directly or indirectly, of computer programs and data without the author's knowledge and authorisation.

The offences related to the copied work are as follows:[40]

- Importing or exporting counterfeit copies of the work, selling counterfeit copies of the work, delaying the publication of the copied work, or deliberately refusing to pay the author the remuneration due under the established rights.

The penalties for offences relating to the counterfeiting of computer data are defined in Article 153 of Decree 03/05 and range from six months to three years' imprisonment, in addition to fines of between 500,000 and 1,000,000 Algerian dinars.

In addition, the judge may impose one or more supplementary penalties for offences related to counterfeiting.

These additional penalties include the confiscation of sums corresponding to the proceeds obtained from the unauthorised use of the work, in accordance with Article 157 of the previous law, as well as the confiscation and destruction of all equipment specifically used for the unauthorised activities and of all counterfeit copies, in accordance with Article 157, paragraph 2.

In addition, at the request of the party concerned, the court may order the suspension and publication of the provisions of the conviction at the expense of the convicted party[41].

It should be noted that the Algerian legislator has empowered the criminal court to increase and intensify the initial penalties in the event of recidivism and to order the closure of the establishment used by the counterfeiter or its control for a period not exceeding six months or, if necessary, to issue a permanent closure order[42].

B. Confronting cybercrime under the Law on the Prevention and Combating of Crimes Related to Information and Communication Technology (ICT):

The Algerian legislator has strengthened protection in the field of cybercrime, in addition to the general provisions that address these crimes, by enacting Law 09/04 on the prevention and combating of crimes related to ICT. This law contains various preventive measures, some of which are preventive and others of a procedural nature.

1. Preventive measures:

These preventive measures are set out in Article 4 of Law 09/04, which specifies the situations in which the security authorities may monitor electronic communications. These situations include

- Prevention of acts constituting terrorism, sabotage or crimes against national security.
- When there is information indicating a possible attack on an information system that threatens state institutions, national defence or public order.
- Within the framework of requests for mutual legal assistance[43].

In addition, the Algerian legislator has introduced new measures to support those provided for in Law 09/04 under the Code of Criminal Procedure, particularly those relating to the fight against cybercrime. These measures include

- Authorisation for remote inspection of an information system or part of it by the competent judicial authorities and judicial police officers.
- The possibility of extending inspection periods with the authorisation of the competent authority.
- The possibility of requesting assistance from foreign authorities to obtain data stored in an information system located outside national territory, in accordance with international agreements and the principle of reciprocity[44].
- Allow Algerian authorities to cooperate with foreign authorities in the field of investigation and evidence gathering in order to detect cross-border ICT-related crimes and their perpetrators, by exchanging information and taking precautionary measures within the framework of international agreements and the principle of reciprocity.

Under Law 09/04, the amended law on the prevention of crimes related to information technology and communication, the Algerian legislator created the National Authority for the Prevention of Crimes Related to Information Technology and Communication. This authority focuses on activating judicial, security and international cooperation and coordinating preventive measures. It also provides technical assistance to judicial and security bodies. The authority can be tasked with providing judicial expertise in cases of attacks on the information system that threaten the security of state institutions, national defence or the strategic interests of the national economy[45].

Second, the treatment of electronic crime in Qatari legislation:

Electronic crime has a special nature that is different from traditional crimes, as it exists in a virtual digital world that spans the globe without geographical or political boundaries. It is linked to the Internet, which allows it to spread across different countries with a single click. The cybercriminal

does not have to physically go to the scene of the crime, as it can be committed behind the screen of his electronic device while he is at home[46].

The Qatari legislation, similar to its Algerian counterpart, addresses the phenomenon of electronic crime. The Qatari Constitution emphasises the fight against cybercrime and demonstrates the State's commitment to international cooperation in general. Relevant provisions include the following:

- Article 6 of the Qatari Constitution states that "Qatar respects international conventions and treaties and works to implement all agreements and international treaties to which it is a party".
- Article 7 of the Qatari Constitution outlines the principles of Qatar's foreign policy, including cooperation with peace-loving nations.

In addition, the Penal Code, enacted by Law No. 11 of 2004, includes computer crimes and classifies them as crimes against property. It consists of 18 articles, beginning with Article 370 and ending with Article 387. The Penal Code includes provisions relating to data processing systems, computer viruses and magnetic stripe cards. Qatar is one of the first Arab countries to include provisions on computer-related crimes in its Penal Code"[47].

Regarding the application of Qatari law to transnational crimes, it should be noted that the Qatari legislator has adopted the principle of universality and has specified the crimes subject to this principle, without explicitly mentioning electronic crimes. Article 17 of the Penal Code states that "the provisions of this law shall apply to any person found in the country as a perpetrator or accomplice after committing crimes abroad, including drug trafficking, human trafficking, piracy or international terrorism"[48].

In this regard, Dr Bashir Saad believes that it is necessary to include cybercrime among the crimes subject to the principle of universality, as it contributes to activating international cooperation in combating this type of crime.

The Qatari legislator also emphasises international judicial cooperation in the field of cybercrime, as reflected in the provisions of the Qatari Criminal Procedure Code. Article 407 states that "without prejudice to the provisions of international agreements, including those of Qatar, and subject to reciprocity, the Qatari judicial authorities shall cooperate with foreign and international judicial authorities and provide them with mutual legal assistance in criminal matters in accordance with the provisions of the law"[49].

It is clear from the above article that the Qatari legislator attaches great importance to international cooperation in the fight against crime by facilitating cooperation between Qatari and foreign judicial authorities through the provision of mutual legal assistance, provided that it does not conflict with the agreements to which Qatar is a party and subject to reciprocity.

With the enactment of the Cybercrime Law, ten years after the enactment of the Penal Code under Law No. 11 of 2004, the Qatari legislature realised that it was not sufficient to rely solely on the provisions of the Penal Code with regard to the principle of legitimacy of crimes and punishments. It was necessary to intervene and enact specific criminal legislation to deal with attacks on the information system and to keep pace with the modern means used in this type of crime. Thus, the Cybercrime Law was enacted under Law No. 14 of 2014.

The Qatari legislature dedicated the third section of Law No. 14 of 2014 to combating cybercrime. This section is divided into three chapters. The first chapter, from Article 14 to Article 20, deals with evidence and investigation procedures. The second chapter, in article 22, imposes obligations on state bodies.

1. Evidence and investigation procedures: Articles 20 to 14 of Law No. 14 state that the Public Prosecutor's Office or the authorised judicial control officers are competent to conduct inspections, collect evidence and issue search warrants for persons, places and information systems related to the crime. The Public Prosecutor or the authorised judicial control officers have the power to order the inspection of persons, places and information systems relevant to the offence, as well as the collection of electronic data, information, traffic data or content information necessary for the investigation and their immediate registration. They also have the power to order the surrender, seizure or preservation of equipment, tools, data and electronic information, and to adopt measures and procedures for their preservation pending a decision by the judicial authorities.

2. Obligations of service providers: Article 21 stipulates that the service provider must undertake to provide the investigating authorities with the data and information necessary in the case and to take various precautionary measures prescribed by law, such as blocking network connections and retaining subscriber information for a period of one year. They must also temporarily and urgently retain technical information data, traffic data or content information for a renewable period of ninety days.

3. Obligations of public authorities: Article 22 states that state entities must take preventive security measures and immediately notify the competent authority of any crimes detected, while retaining the data for a period of 120 days[50].

4. Specialised units for investigating electronic crimes in Qatar:

a. The Public Prosecution: The Attorney General issued Decision No. 72 of 2018 on the establishment of the Electronic Crimes Prosecution and the definition of its jurisdiction. Accordingly, the Electronic Crimes Prosecution was established on 21 June 2018[51]. It is responsible for the investigation and prosecution of the following crimes

- Crimes that violate the provisions of Law No. 8 of 1979 on publications and publishing, with the exception of those that fall under the jurisdiction of state security and counter-terrorism.
- Crimes specified in articles 203, 293, 331, 332, 333 and the fifth chapter on computer crimes of the Criminal Code No. 11 of 2004.
- Crimes that violate the provisions of Law No. 34 of 2006, as amended by Law No. 17 of 2017, on telecommunications.
- Crimes that violate the provisions of Law No. 14 of 2014, the Cybercrime Law, with the exception of those that fall under the jurisdiction of the State Security Prosecutor's Office and the fight against terrorism[52].
- Crimes that violate the provisions of Law No. 16 of 2010, the Law on Electronic Transactions and Commerce, with the exception of those that fall under the jurisdiction of the Commercial and Consumer Affairs Prosecution Service.
- Crimes that violate the provisions of Law No. 13 of 2016 on the protection of personal data.
- Dealing with the victim in accordance with Article 213 of the Qatari Criminal Procedure Law.
- Any other task assigned to it within its jurisdiction. The jurisdiction of the Electronic Crimes Prosecution covers all regions of the world.

4- The Administration for Combating Economic and Electronic Crime:

It is one of the administrative units within the Ministry of the Interior. It specialises in investigating economic and electronic crimes, submitting them to the Public Prosecution, conducting research and investigations on suspicious websites, and handling reports submitted by victims[53].

C- The National Committee for Information Security was established by Emiri Decree No. 19 of 2016. It is chaired by the Prime Minister and Minister of Transport and Communications, with a deputy from the same ministry. The committee includes representatives from various entities, including the Ministry of Interior, the Ministry of Defence, the Ministry of Economy and Industry, the Ministry of Finance, the Ministry of Justice, the Ministry of Transport and Communications, the Public Prosecution, the State Security Bureau and the Qatar Central Bank. Article 3 of the Decree states that the Committee aims to enhance information security in the country, in line with comprehensive development plans in all fields, by strategically guiding the necessary national efforts to achieve the objectives set out in the National Information Security Strategy. The decree also grants the Committee all the necessary powers and authorities to achieve its objectives.

C- The National Agency for Cyber Security: It is established by Article 3 of the Emiri Decree No. 1 of 2021. The purpose of establishing the agency is to maintain and regulate national cybersecurity, promote vital state interests, protect the country and combat cyber threats. The agency's responsibilities include developing the national cybersecurity strategy, establishing and updating policies to enhance cybersecurity, creating frameworks to manage cyber risks, raising awareness about cybersecurity, and authorising the agency to enter into contracts and memoranda of understanding with local and international entities involved in cybersecurity. The agency also prepares reports on the status of cybersecurity at the local, regional and international levels[54].

CONCLUSION:

Through our study of electronic crime, it has become clear that this type of crime is one of the most dangerous crimes that the modern world is experiencing. It is a phenomenon generated by the technological and information revolution, and no country in the world, developed or developing, is immune to it, because it is different from traditional crimes. From the above, we have derived a number of findings that can be summarised as follows:

First, the results:

1. There is no single term for electronic crime. Some call it information fraud or information misappropriation, while others call it information or cybercrime. The reason for these differences is the fear of confining this crime to a narrow field, while all these terms convey essentially the same meaning.
2. It should be noted that the Algerian legislator, like its Qatari counterpart, has not chosen a single term. In Algerian Law No. 04/15, electronic crime is defined as the violation of automated data processing systems, while in Law No. 09/04 it is defined as crimes related to information and communication technology. Despite this difference, both designations serve the same purpose, which is to combat electronic crime.
3. Cybercrime is a transnational crime that can only be fought through international cooperation.
4. It is noteworthy that both the Algerian and the Qatari legislators have addressed the perceived legal vacuum in the field of cybercrime. They have adopted a solution that provides dual protection against cybercrime, through legal provisions on the one hand, and through institutions aimed at achieving the desired objective of prevention and suppression as a mechanism for combating cybercrime on the other.
5. Qatar has signed several international agreements with various countries to combat electronic crime.
6. There is no specific global agreement to combat electronic crime.

Secondly, the recommendations are as follows

1. The need to enact dissuasive legislation against perpetrators of electronic crimes by filling the legislative gap in the field of combating electronic crimes, including detailed objective and procedural rules and defining the nature of crimes committed on communication networks, social media and e-mail.
2. The need to recruit cybercriminals as assistants to members of the judiciary in order to benefit from their expertise and insight.
3. The establishment of specialised centres to study this type of emerging transnational crime.
4. Activate the role of civil society and institutions in raising awareness and preventing individuals from falling into the abyss of vice and criminal practices.
5. Encourage the establishment of international committees to monitor the compliance of States with their obligations under international conventions to combat cybercrime.
6. The need to include in Algerian and Qatari schools and universities, as well as in law faculties and judicial institutions, subjects related to information systems and the crimes resulting from them, and to teach them in a simplified manner.

In conclusion, cybercrime is characterised by differences in definition, development and legislation. Different legal systems have addressed this phenomenon by clarifying its nature, scope and characteristics. Efforts have been made to fill the legislative gap in the area of cybercrime by criminalising attacks on computer systems, but a law specifically criminalising electronic forgery is still lacking.

List of footnotes:

[1]- Zibida Zidan, "Cybercrime in Algerian and International Legislation", 1st edition, Dar Al-Huda, Algeria, 2011, p. 05.

[2]- Mohamed Mohamed Al-Alfi, "Criminal Liability for Ethical Crimes on the Internet", 1st edition, Al-Maktab Al-Masri Al-Hadith, 2005, p. 68.

[3]- Munir Mohamed Al-Junihi, Mamdouh Al-Junihi, "Internet Crimes and Computer and the Means to Combat Them", 1st edition, Dar Al-Fikr Al-Jami'i, Egypt, 2006, p. 13.
[4]- Nawal Thabet, "Cybercrime in Algerian Legislation: Nature, Subject, Characteristics, Manifestations and Challenges", Cesiologia Journal, Vol. 06, Issue 02, University of El-Hadj Lakhdar, Batna, Algeria, 2022, p. 63.
[5]- Samia Aziz, Mazia Issawi, "Crime from a Sociological Perspective: Causes, Effects", Studies in Deviance Psychology Journal, Vol. 6, Issue 1, 2021, p. 128.
[6]- Huda Qashoush, "Computer Crimes in Comparative Legislation", 1st edition, Dar Al-Nahda Al-Arabiya, Egypt, 1992, p. 180.
[7]- Hisham Mohamed Farid Rostom, "Penalties and Risks of Information Crimes", 1st edition, Dar Al-Nahda Al-Arabiya, Egypt, 2000, p. 20.
[8]- Law 09/04, "Law on Special Provisions for Preventing and Combating Crimes Related to Information and Communication Technology", Official Gazette No. 47, 16 August 2009.
[9]- Law 21/11, dated 16 Muharram 1443, corresponding to 25 August 2021, supplements Decree 66/155, dated 18 Safar 1386, corresponding to 8 June 1966, which incorporates the Algerian Code of Criminal Procedure.
[10]- See Article 2 of Law 09/04.
[11]- Amina Ben Amiz, Ilham Bouhalas, "The National Judicial Pole for Combating Crimes Related to Information and Communication Technology", research paper presented at the International Conference on Criminal Law for Business, Towards a New Approach to Criminalisation, held on 21 October 2002, Volume 7, Issue 1, pp. 71.
[12]- Cf. Article 01 of Kuwait Law No. 63 of 2016 on Combating Information Technology Crimes.
[13]- Hamda Mohamed Al-Shuraim, "Electronic Crimes and the Position of Islamic Sharia Law on Them: The Qatari Legal Case", Journal of Islamic Studies and Thought for Specialized Research, Volume 5, Issue 1, 2019, p. 106.
[14]- Ahsan Bousgaia, "Concise General Criminal Law", 1st edition, National Office of Touristic Works, 2002, p. 24.
[15]- Rasa' Fatiha, "Criminal Protection of Information on the Internet", Master's Thesis in Legal Sciences, Tlemcen, 2011, 2012, p. 69.
[16]- Souber Sufian, "Information Crimes", Master's thesis in Criminal Sciences and Criminology, Tlemcen, 2010, 2011, p. 33.
[17]- See Decree 05/03 of 19 Jumada al-Awwal 1424, corresponding to 19 July 2003, on Copyright and Related Rights, Official Gazette No. 44.
[18]- Souber Sufian, ibid, p. 37.
[19]- See Article 61 and subsequent articles of the Algerian Penal Code.
[20]- See Article 394 bis and subsequent articles of the Algerian Penal Code.
[21]- Brahami Jamel, "Fighting Cybercrime in Algerian Legislation", Critique Journal of Law and Political Science at the Faculty of Law and Political Science, University of Mouloud Mammeri, Tizi Ouzou, issue 2, published on 15 November 2016, p. 125.
[22]- Hamza Ben Aqoun, "Criminal Behaviour of the Cybercriminal", Master's Thesis in Legal Sciences, University of El-Hadj Lakhdar, Batna, 2011, 2012, p. 54.
[23]- See Article 394 bis 2 of the Algerian Penal Code.
[24]- Dardour Nassim, "Information Crimes in Light of Algerian and Comparative Law", Master's thesis, University of Constantine, 2012, 2013, p. 45.
[25]- See Articles 12 and 13 of Qatar Law No. 14 of 2014 on Combating Electronic Crimes.
[26]- Souber Sufian, ibid, p. 41.
[27]- Rasa' Fatiha, ibid, p. 73.
[28]- Maashi Samira, "The Nature of Information Crime", Al-Muntada Al-Qanuni Journal, Issue 7, University of Khider, Biskra, Algeria, 2018, p. 280.
[29]- Hajazi Abdel Fattah, "Computer and Internet Crimes", 1st edition, Dar Al-Kotob Al-Qanuniya, Egypt, 2004, p. 113.
[30]- Amal Kara, "Criminal Protection of Information Technology in Algerian Legislation", 2nd edition, Dar Homa for Printing, Publishing and Distribution, Algeria, 2007, p. 33.
[31]- Mokhlal Ibrahim Zghibi, "The Effectiveness of Arab Laws and Legislation in Combating Cybercrimes: A Comparative Study", Arab Journal of Scientific Publishing, No. 37, 2021, p. 282.
[32]- Amal Kara, ibid, p. 54.
[33]- Fadila Aqil, "Cybercrime and Its Confrontation through Algerian Legislation," Fourteenth International Conference on Cybercrimes, 24-25 March 2017, p. 127.
[34]- Hussein Nuwara, "Mechanisms for Regulating the Algerian Legislative Crime of Assault on Privacy Electronically," National Meeting, Strategies for Combating Crimes in Algerian Legislation, Algeria, 29 March 2017, pp. 121-122.
[35]- Law No. 06/22 of 20 December 2006 amending and supplementing Decree No. 66/155 containing the Algerian Code of Criminal Procedure, Official Gazette No. 84 of 24 December 2006, as amended and supplemented.
[36]- See Article 394 bis of the Algerian Penal Code.

[37]- See Article 37 of the Algerian Code of Criminal Procedure.
[38]- See Article 65 bis 6 of the Algerian Code of Criminal Procedure.
[39]- Mokhtaria Bouzidi, "The Nature of Cybercrime", National Meeting, Mechanisms for Combating Electronic Crimes in Algerian Legislation, Algiers, 29 March 2011, p. 9.
[40]- See Article 151, paragraphs 3 and 4, and Article 155 of Decree 03/05.
[41]- See Article 158 of Law 03/05.
[42]- Mokhtaria Bouzidi, ibid, p. 14.
[43]- See Article 4 of Law 09/04.
[44]- See Article 5 of Law 09/04.
[45]- Najia Sheikh, "On Combating Cybercrime in Algerian Legislation", Journal of Legal and Political Sciences, Vol. 09, No. 02, June 2018, p. 697.
[46]- Hamida Mohammed Al-Sharim, ibid, p. 114.
[47]- Ashraf Tawfiq Shams al-Din, "Explanation of the Qatari Penal Code", Qatar University, 2010, p. 184.
[48]- Ashraf Tawfiq Shams al-Din, ibid, p. 184.
[49]- See Article 407 of Law No. 23 of 2004 on the Code of Criminal Procedure.
[50]- Hamad Mohammed Al-Sharim, ibid, p. 15.
[51]- See Decision No. 72 of 2018, Public Prosecution website www.fh.gov.qa: http
[52]- Abdul Rahman Abdullah, Lectures within the Cybercrime Course, Introduction to Master's Students, General Law, Qatar University, 2019, p. 24.
[53]- See Article 03 of Emiri Decree No. 19 of 2016.
[54]- See Article 03 Article 18 of Emiri Decree No. 01 of 2021