Anti Crimes Committed Against Digital Data

مكافحة الجرائم المرتكبة ضد البيانات الرقمية

Imene Bouguessa [1]*
Faculty of Law and political sciences
University of Jijel
imene.bouguessa@univ-jijel.dz

Yahia Bedairia [2]
Faculty of Law
University of Tebessa
yahia.bedairia@univ-tebessa.dz

Date of send:07/09/2025 **Date of acceptance**:01/01/2026 **Date of publication** ;11/06/2026

Abstract:

Electronic societies have recently suffered from violations of electronic right of the spread of cybercrime or the crime of data infringement and of this type of technology and technology, and therefore the data crime has several characteristics, whether the computer as a device or persons who commit these crimes.

Accordingly, in this context, the crime of destruction falls within the scope of information technology by attacking the natural functions of the computer, by violating the programs and data stored and exchanged between the computer and its networks, internal or global, and this is done by tampering with data, Ciber security has become one of the most important priorities of political countries and regimes in the world as it is closely related to the security of information and data of the social, economic, cultural and political nature, whether it comes to state security or the security of individuals. we aim Through this study, to explain cybercrimes, their characteristics, and the legal and security mechanisms to confront them.

Keywords: Privacy Electronic; Cyber Crime; Infringement of data ; Ciber security ; data.

**** Corresponding author : Laboratory of Legal and Political Transformations***

Introduction

In light of the environment of automatically stored information, the grip of security, monitoring and control had to weaken, and the operations of espionage, piracy, sabotage and destruction of electronically processed information increased and multiplied, until it became a serious threat to all government organizations whose work depends on computers and

communication networks. On the one hand, it raises the risks of misuse of computers and tampering with programs and automatically stored information files with the intention of

obtaining undeserved money and services .

On the other hand, information, as the most important element in the world of automated data processing, raises several legal problems due to its use in committing a crime remotely on the one hand, or its being the subject of attack on the other hand, which raises the issue of assault and whether it constitutes a crime or not. Hence, we pose the following question: What are the crimes against digital data? What are their characteristics?

We will attempt to answer these questions through this study, using a descriptive approach to present these modern forms of crime, and an analytical approach by attempting to limit them to a set of legal forms, based on two elements.

This study will address the definition of digital data, then explain its characteristics, also the Characteristics of crimes affecting digital data, and The Legal and security mechanisms to counter threats and digital crimes.

Firstly: First main title: Section One: defining digital data:

Secondly :Second main title: Section Two Characteristics of crimes affecting digital data:

Thirdly: The third main title: Section Three: Legal and security mechanisms to counter threats and digital crimes:

Firstly: First main title: Section One: defining digital data:

The technical development taking place in the world of information technology and what it requires of the necessity of carrying out the tasks of providing, collecting, processing and exchanging information at the same time has led to the commission of crimes of the automated processing system, which in fact arose with the aim of describing the situation that emerged from the merger of information system technology and information technology.

telecommunications, It has been defined as a mechanism and organized procedures that allow the collection, classification, and sorting of data, processing it, and then converting it into information that a person extracts when needed to be able to accomplish work, make a decision, or perform any job through the knowledge he obtains from the information retrieved from The system that contains what is called data, and accordingly, we will discuss the definition of the data (the first section), then the definition of the data (the second section).

1. Definition of data:

Studying the legal nature of data is important and necessary, as the development and diversity of this data has completely changed the means of analyzing contemporary laws. It is not surprising that issues related to databases have become controversial, and the matter is due to two reasons :Technological development in communications and the process of including this data on electronic devices[1].

1.1.Its definition in jurisprudence and comparative law:

Jurists and legal scholars have worked hard to find a definition for data. Some have defined it as a collection of numbers, words, symbols, facts, or raw statistics that have no relationship to each other and have not yet been subject to change or preparation for use. As for information, it is the meaning that is extracted. From these data.

The French Agency has defined data as every intelligible event or instruction presented in an agreed-upon form that can be exchanged by humans, by computers, or produced by computers. It has adopted the Budapest Convention on Information Crime in defining data with the same definition adopted by the international standardization body ISO, where it stipulates: Its first article states that data is any representation of facts, information, or concepts in any form that is prepared for processing, including a program prepared of the same nature that makes the computer perform the task[2].

Based on this meaning, data is considered the raw materials from which information is extracted using automated processing in the extraction process. The data is collected and processed to obtain information, and then used to issue decisions that in turn lead to an additional set of data, which is collected and processed again. For additional information.

1.2.Its definition in Algerian law:

The Algerian legislator has taken what the rest of the legislation has taken. By referring to the Penal Code, Section 7 bis 01, entitled “Violation of automated data processing systems,” we find that the legislator did not know it, and he did well not to define the data. This is in view of the continuous technological development and the rapid and successive developments in technologies, which prevented this. Therefore, what we see today in terms of programs or data subject to protection may not be so tomorrow and vice versa. It is as if the term “data” means digital and non-digital data and data, as this term is considered more comprehensive and general[3].

While the term information data came in the law of special rules for the prevention of crimes related to information and communication technologies, it is a process of presenting facts or concepts in a form ready for processing within an information system, including appropriate programs that would make the information system perform its function[4].

With this conception, the data are digital or non-digital facts that are done in a systematic manner whose meaning can be understood directly without entering into

inductive deductive processes regarding their complex meanings through more than one statement[5], because that means that the shift from the matter being mere data to data and information must therefore be defined. Data and information as: individuals' lack of awareness of the true meaning of data and the extent of its danger and exploitation, which are problems in a continuous increasing.

2. Definition of information:

It is one of the terms that almost loses its semantic weight due to frequent use, as ...All definitions mentioned in the information largely express opinions and views Their owners, and these definitions may be accepted by some disciplines and rejected by others Others, so it is necessary to address their definition linguistically and then terminologically:

2.1. Its definition in language:

Information in terms of linguistic meaning is derived from the linguistic material "science" It is a subject rich in many meanings, such as knowledge, insight into matters, awareness, perception and certainty, guidance, information, fame, knowledge, education, know-how...to other meanings related to the functions of the mind, and in contrast,

A- Arabic definitions: The Egyptian legislator defined data as any distinct collection of data in which an element is present An innovation, arrangement, or any personal effort that deserves protection, in any language, symbol, or form, and may be stored Using a computer and it can also be retrieved using it[6].

B-Western definitions: -The American legislator defined data as: a collection, and a collection is defined as a work that collects or collects Collecting pre-existing data or materials, the appropriate ones have been tested, formatted, and arranged in such a way that the resulting work is functional An innovative work of authorship.

As for the Japanese legislator, he defined it as a group of information, such as articles and numbers, as its structure and classification allow To be searched by Computer. the English word is derived from the Latin word Information, which originally means the process of communication or what is communicated or received[7].

2.2. Defining it terminologically:

Information has been defined as a set of symbols, facts, concepts, or instructions that are suitable for exchange, communication, explanation, interpretation, processing, fragmentation, collection, or transfer by various means or forms[8].

Professor Calte defined information as a message expressed in a form that makes it transferable or reported to others. It is also defined as the abstract transfer of specific facts and then obtaining them from multiple sources.

Despite the diligence of legal scholars and their attempts to develop a comprehensive definition that would provide a specific definition for information, they have not yet been able to do so. Some legislation has attempted to define information, and it has varied, including Arabic and Western legislation[9].

Accordingly, information is the initial or mental result resulting from operating the data and interpreting it or extrapolating its meaning and deducing what can be

deduced from it alone or in combination with others or interpreting it in a way that impairs the knowledge of the decision users and helps them in making sound judgments about the phenomena and observations or contributes to the development of Theoretical or applied knowledge.

Information can be combined, as one piece of information is added to another piece of information to form new information that differs in value and importance, and thus the issue of the amount of protection necessary for it is raised, which is called the Integrative Information Theory[10].

Here the question arises: What is the difference between data and information?

Researchers and scholars often confuse data and information, and it is customary to use each in place of the other. However, there is a difference between the two terms, which lies in:

✓ Any information system begins with data and ends with information.

✓ Data are facts that have been recorded, or will be recorded in the future, regarding certain events. These facts may be independent, not related to each other, and of indefinite number. They are also known as inputs or raw material for information. In other words, they are a group of facts and observations that are collected. From a specific statistical community, it is entered into the computer to process it and produce results, such as name, age, profession...etc[11].

As for the information, it is the result of running the data, or the sum of the results obtained from the computer. In other words, it is the set of data that was collected and It was prepared in a way that made it usable, i.e. useful for its future, i.e. its user. It represents the outputs in the information system and has an impact on making various decisions[12].

Despite these points of difference, researchers believe that it is difficult to draw a dividing line between data and information “data”. What is considered information at some stages is considered data at the next stage, and that the information may not be in quantitative form, that is, expressed In numbers, but it may be known through a descriptive word[13].

Therefore, it can be said that data and information are complementary to each other. Without data, information and data would not have been formed.

Secondly :**Second main title**: **Section Two Characteristics of crimes affecting digital data:**

Crimes that affect data are considered cybercrimes, as they are linked to and based on them. The expansion of these crimes has led to harm to society, and the increase and prosperity of the volume of information technology in various sectors has led to giving cyber crimes a special legal color or character that distinguishes them from other crimes.

Crimes, whether traditional or new, include those related to the computer, some of them related to the Internet , and some of them related to the perpetrators of the crime. features related to the computer It can be limited to the following points :

1. A crime affecting computer data:

The computer is a tool for committing these crimes: Crimes affecting data or information are characterized by a unique characteristic that distinguishes them from traditional crimes.

1.1. If the computer or its accessories are attacked:

Here, the goal of committing these acts over the Internet is to attack computer data, such as information and data stored in memory, and this data is not of a tangible, transferable, material nature, so that we can confirm that it is subject to the provisions of the traditional penal code, and it is closer to the mental or moral entities that They are entered into the computer. Most often, the goal is to permanently store these devices or at least disable them for as long as possible, and most of these crimes are committed by using viruses[14].

1.2. Features related to the Internet:

At the beginning of the emergence of the Internet, there was no concern about crimes that could be committed on it or through it, not because it was safe in its design and construction, but rather because its users were limited, and because the Internet is a large network that connects individual networks located across various countries of the world to millions of computers that can Connecting to the same sites at the same moment and with high speed for a huge amount of information and services, so some resorted to it to achieve **Objectives:** The Internet has become a field for criminal attacks, in which most forms of money crimes are imagined. Therefore, it is a cross-border crime and a crime that is difficult to discover and prove. This is due to[15]:

2. The concealment of the crime:

Crimes related to data and data are characterized by invisibility, unlike traditional crimes, which are usually public. The victim does not notice them, even though they may occur while he is on the network, because the perpetrator has technical capabilities that enable him to commit the crime with high accuracy, such as sending destructive viruses, stealing money, and Private data or its destruction, spying, call theft and other crimes[16].

Data crime occurs outside the framework of tangible physical reality in an electronic environment in which information is transferred and circulated in an invisible manner, in addition to the difficulty of technically preserving its traces, if any.

2.1. Characteristics related to the perpetrators of the crime:

The perpetrator of the crime is a person with great experience in using a computer. To commit a crime on the Internet, the user of this computer must have great knowledge and experience in the field of its use, which enables him to carry out his crime and work to avoid detection. This person is intelligent, as he can overcome On many punishments She confronts him while he is committing the crime[17].

This criminal possesses the skills that qualify him to modify and develop security systems so that no one can pursue him and follow his criminal actions through networks or inside computers. The cyber criminal is a criminal who relies on intelligence. He is a person with high technical skills who specializes in cybercrime.

And he takes advantage of his awareness.His skills are in penetrating networks, breaking passwords or codes, and swimming in the world of networks to obtain all the valuable data and information contained in computers[18].

2.2. Sibian threats and crimes:

The Sibian threats mean those attacks and risks that hinder the use of software and digital networks in various transactions through computers, and necessarily lead to harm to devices, networks, data, information and users of these data, and deprives them of benefiting from various services in the digital image, as these threats differ from one country to another by looking at the dominance of that country on the digital side and the extent of their development In it[19], where cyber attacks have become one of the most dangerous threats of national security for countries, targeting biomus infrastructure, government regimes and military sectors, which threatens the stability and sovereignty of countries[20].

✓ **The sabotage of the system and destroying its ability to work:** The attack aims to stop programs and devices from work, including the inability to provide usual or supposed services, by providing the computer or the device with a huge amount of orders to carry a large group of services in one time, which generates a great pressure on the device and from it stops working[21], as it may be done by broadcasting viruses that work to suppress the device's ability to analyze information and data in the correct way, and from it the occurrence of a defect Treatment usually leads to the stop of the device and its inability to work[22].

✓ **Sibian espionage:** This crime is considered one of the most dangerous Sibian threats, as it aims to obtain military, political or economic information, with the aim of obstructing the progress of the work of the internal national bodies in a country[23], where it aims mostly to disrupt the work of networks, devices, systems and computers, with the intention of stealing information and confidential, political, economic financial economic financial, of importance and transporting them to another country, using advanced digital means and technologies, including devices Extracting, also piracy and penetration devices[24].

✓ **Sibian terrorism:** It is the use of information and computer networks for intimidation and spreading terror in certain groups to achieve political goals, where the terrorist group threatens electronic media, digital spaces, and global networks, by broadcasting content targeting a group of people on an ethnic, ethnic, national, or religious basis, so that a threat to their safety and security or deprives them of exercising their tasks normal[25] It is deprived of the use of digital means, or causes them material or moral damage by leaking information and data of a sensitive or secret nature. The goal of these organizations is mostly to obtain money, by threatening people, or having their financial accounts, and these terrorist groups may target countries[26].

✓ **heft of information and military data and the penetration of security rules and sites:** Electronic attacks in this case seek to penetrate the networks of military institutions with the aim of stealing, falsifying or destroying private data and information, with regard to armament systems, and military equipment designs and

equipment[27].

Consequently, it can be said that the Sibian threats affect national security in several aspects, including:

✓ Economically: Cyber attacks lead to losses that may exceed 6 trillion dollars annually by 2025[28].

✓ Military: By penetrating defense systems, weapons such as missiles or radar systems may be disabled.

✓ Politically**:** It leads to leaking sensitive information, which threatens international relations.

Thirdly: The third main title: Section Three: Legal and security mechanisms to counter threats and digital crimes

In light of the growing Sibian threats and its increasing effects on national security, Algeria was quick to adopt many efforts and mechanisms to confront various Simian threats and crimes[29].

1.The legal aspect

Algeria has introduced many legislations and laws to fight the Simian threats and crimes, with the aim of enhancing its Sindi security, including we find Law No. 09-04 related to the special rules for the prevention of crimes related to media and communication technology and their reward[30], and Law 05-10, which includes the electronic guide[31], Law 18-07 related to the protection of personal data[32], it also criminalized various forms of attack within the Penal Code and its complementary laws[33].

2.The security side

✓ Algeria has introduced many security services specialized in facing the Sibian threats in order to enhance and protect its national security. Examples of these security and judicial services. We mention the following:

✓ **Center for Prevention of Information Crime and Information Crime for the National Gendarmerie:**This center was established in 2008, its headquarters, its goals are to secure the information system for the service of public security, as it documents information and analyzes data and data related to electronic crimes, trying to identify the perpetrators, and ensuring that information systems of institutions, banks and companies, through work in coordination between various security services and other judicial authorities[34].

✓ **The National Institute for Criminal Evidence and Criminology of the National Gendarmerie:** in Algiers, which specializes in investigation and investigations related to misdemeanors and crimes, which depend on high -precision and level technical means, as it depends on scientific experience and accurate laboratory experiences for all the evidence obtained from the commission of a crime, where in 2017 more than 2500 electronic crimes relate to most of them violating personal freedoms, threats via the Internet, and publishing pictures Explanation and electronic piracy, and more than 1300 penetration attempts for the National Defense Foundation have been aborted by Hackers and viruses[35].

✓ **The Central Authority for Combating Information Crime of National Security**: which was established in 2011, which was also addressed by many crimes, especially those related to electronic crimes, and committed in social media, and after that it was attached to the Judicial Police Directorate in 2015, where more investigated in crimes that threaten national security such as the following cases: threats and crimes against public order and assaulting the private life of the citizen and terrorism Electronic crime and cases of inciting individuals to immorality and prostitution through the digital space, crimes against information systems and hackers, insulting a regular body, state symbols, fraud, fraud and sexual harassment against individuals in the electronic medium.

✓ **The National Authority for the Prevention of Crimes Related to Media and Communication Technology:** An independent administrative authority for the Minister of Justice, operating under the supervision and monitoring of a directorate committee headed by the Minister of Justice and mainly includes members of the government and two judges from the Supreme Court appointed by the Supreme Judicial Council, as this body was assigned to propose elements of the national strategy for the prevention of crimes committed by media and communication technologies and their rewards, stimulating and coordinating prevention operations, and assisting judicial authorities The interests of the judicial police in the field of combating these crimes, by collecting and providing information and providing them with judicial experiences, and ensuring preventive monitoring of electronic sites, a monkey monkey to reveal crimes related to terrorist and sabotage and prejudice the security of the state.

✓ **The National Criminal Pole to Combat Crime Connecting Technology and Communication:** A national criminal pole specialized in follow -up and investigation of crimes related to media and communication technologies and associated crimes in accordance with the text of Article 221 bis 22 of the order -21-11 amending the Criminal Procedure Law headed by the council's headquarters in Algiers, for this body of national jurisdiction, and has the state in follow -up, investigation and trial in continuous crimes With media and communication technologies and the most complicated crimes, which require special means, specialized technical experience or international judicial cooperation. and also created the National Pole To combat crimes related to media and communication technology[36].

Conclusion

As a conclusion, it can be said that digital data, which represents digital or non-digital facts, is done in a systematic manner, and its meaning can be understood directly without entering into inductive deductive processes regarding its complex meaning through more than one statement, and this digital data may be subject to attack.This crime has features that distinguish it from other crimes, the most prominent of which is that these crimes are committed using a computer, as it is the main method most used.in crime. Other computers are attacked, programs are accessed, stolen and destroyed, given that the Internet is a fertile field for attacks.

Also Electronic crimes are one of the biggest challenges facing modern societies, especially in Algeria. Through awareness and education, activating laws related to cybercrime, and enhancing safety measures at the individual and institutional level, these crimes can be significantly reduced. The strengthening of cooperation between the public and private sectors, and the development of judicial experiences in the field of Sindi security will have a decisive role in protecting digital financial transactions and ensuring the integrity of personal information and financial protection for citizens.

Results:

_ Algeria tried to set the regulatory legislation of digital security to establish laws that govern the security of electronic financial transactions, and to ensure that they are effectively applied.

_ That cooperation between the public and private sectors has been strengthened, by encouraging government institutions and the private sector to work together to meet the challenges that occur in the digital space.

_ It has been established bodies specialized in Sibian security, as bodies were established that supervise the application of digital security standards and provide technical and legal support to combat cyber crime.

_ One of the difficulties of reducing these activities is that it crosses the borders, as many electronic crimes are carried out via the Internet by individuals or groups that exist in different countries, which complicates the verification and prosecution process.

_ One of the difficulties of reducing these threats is that it also uses advanced technologies, such as VPN and encryption methods that complicate the process of tracking electronic crimes and identifying criminals.

Recommendations:

_ The necessity of training judges and lawyers: In order to keep pace with technological developments, training programs directed to the judiciary and law must be provided in how to deal with issues related to electronic crimes.

_ The necessity of increasing coordination between the concerned authorities: It is necessary for judicial bodies, security services, and technical companies together to effectively combat electronic crimes.

_ The necessity of strengthening international cooperation in various fields to confront these threats.

_ It must be taken into account the importance of investing in the technologies of Sibian security to confront this new type of crime.

_ The need to work to develop artificial intelligence systems to discover the locations of this type of attack.

_ It is necessary to train cadres specializing in Sibian security.

Margins:

[1] _ Hisham Muhammad Farid Rustom, Penal Code and Information Technology Records, Library of Modern Machines, 1992, p. 26.

[2] _ Muftah Muhammad Dabbab, Dictionary of Terms and Information and Communications Technologies, International Publishing House, Cairo 1995, p. 42.
[3] _ Intisar Oraib, Computer Security and Law, Al-Rateb University Publishing House, Beirut, 1996, p. 81.
[4] _ Article 02 of Law No. 09-04 of August 5, 2009 includes special rules for the prevention of Crimes related to information and communication technology and combating them, Issue 47.
[5] _ Rachida Boukar, Crimes of Assault on Automated Processing Systems in Algerian and Comparative Legislation, Al-Halabi Publications Jurisprudence, first edition, 2012, p. 67.
[6] _ As for the Lebanese legislator: he defines data and considers it a body of work, collections of information, whether in readable form Or mechanically or in any other form It must be created by the copyright owner.
[7] _ Naila Muhammad Farid Fawrah, Economic Computer Crimes, Al-Halabi Publications, Edition 01, year 2005, p. 97.
[8] _ Hatmat Qasim, Introduction to the Study of Library and Information Science, Dar Gharib, Cairo, 1990, p. 15.
[9] _ Khaled Mamdouh Ibrahim, Cybercrime Security, University House, Alexandria, 2008, p.
[10] _ Munir Muhammad Al-Janabihi, Mamdouh Al-Janabihi, Internet and computer crimes and means of combating them, Dar Al-Fikr University College, Alexandria, 2006, p. 25.
[11] _ Mahmoud Ahmed Ababneh, Computer Crimes and their International Dimensions, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 2009, p 36.
[12] _ Amir Faraj Youssef, Electronic and Information Crime and International and Local Efforts to Combat, 22nd Library Edition Al-Wafa Legal, Alexandria, 2011, p. 20.
[13] _ Muhammad Amin Al-Shawabkeh, Computer and Internet Crimes, Information Crime, Dar Al-Thaqafa for Publishing and Distribution, Amman, Year 2007, p. 129.
[14] _ Mahmoud Ahmed Abaniya, previous reference, p. 44.
[15] _ Muhammad Amin Al-Shawabkeh, previous reference, p. 135.
[16] _ Khaled Mamdouh Ibrahim, previous reference, p. 44.
[17] _ Ibid., p. 46.
[18] _ Amir Farag Youssef, information crimes on the Internet, University Press House, Alexandria, year 2008, p. 32.
[19] _ Ahmed Abis Nima Al -Fatlawi, Sibian attacks, Al -Muqihqa Magazine, College of Law University of Babylon, No. 04, 2016, p. 614.
[20] _ Bin Saber Belkacem, Sibian attacks and their confrontation in the light of contemporary international law, Journal of Human Rights and Public Liberties, Mostaganem University, Volume 02, No. 04, June 2017, p. 189.
[21] _ Biomatic infrastructure attacks: In the year (2022): The "cyber wind" attack was on energy systems in Ukraine, which caused the power outage from thousands of houses, and in the year (2021): the penetration of the "Colonio" pipeline in the United States, which led to the disruption of fuel supplies and the company to pay a ransom of $ 4.4 million.
[22] _ Nuran Shafiq, forms of electronic threats and their sources, European Center for Terrorism Studies and Control, Germany, was reviewed on 07/22/2025 at the hour: 20:30
Link: http://www.europarabct.com/%D8%A3%D8%B4%
[23] _ Amira Abdel -Azim, Sibian risks and ways to confront it in public international law, Journal of Sharia and Law, Volume 32, No. 35, Journal of Legal and Fiqh Research, Egyptian Patrols, 2020, p. 415.
[24] _ Sibian espionage: In the year (2019): The Israeli "Begasus" attack on political phones and journalists around the world, and also in the year (2020): accusing China of penetrating the "NASA" networks and the US Department of Defense.
[25] _ Amira Abdel -Azim, previous reference, p. 421.

[26] _ Wars of Information and Displacement: In the year (2022): Russia used social media robots to spread fake news during the war on Ukraine, and also the year (2016): Russian pirates enter the American elections by penetrating the democratic mail.
[27] _ Organized electronic crime: In the year (2023): The "Lockerit" group attack on Saudi and Emirati banks, theft of statements of millions of customers, and the year (2020): The penetration of the American company "Solar Windows", which affected several government ministries and major companies.
[28] _ According to the "Cybersecurity Ventures" report.
[29] _ Lami, a divorced woman, Sibian threats and crimes, Milestones Magazine for Legal and Political Studies, University Center Tindouf, Volume 04, No. 02, 2020, p. 56.
[30] _ Law No. 09-04, of May 09, 2009, related to the special rules for the prevention of crimes related to media and communication technology and their reward, Official Gazette, No. 47, issued on May 16, 2009.
[31] _ Law 05-10, dated June 20, 2005, which includes the electronic guide, Official Gazette, No. 44, issued on June 26, 2005.
[32] _ Law 18-07, of June 10, 2018, related to the protection of personal data, Official Gazette, No. 34, issued on June 10, 2018.
[33] _ Jamal Bawazida, the Algerian strategy in the face of the Spanish crimes, Journal of Legal and Political Sciences, Al -Wadi University, Volume 10, No. 01, April 2019, p. 1278.
[34] _ Youssef Bougara, Sibian security, African Studies Magazine and the Nile Basin, Arab Democratic Center, Volume 01, No. 03, Germany, September 2018, p. 111.
[35] _ Jamal Bawazida, previous reference, p. 1281.
[36] _ Ordinance No. 21-11, of May 25, 2021, which includes the amendment of the Criminal Procedure Law, the official newspaper, No. 65, issued on May 26, 2021.