Received date: 20.05.2024
Accepted date: 16.11.2024
Publication date: 17.12.2024

Science, Education and Innovations in the Context of Modern Problems
International Academic Journal
ISSN: 2790-0169; E-ISSN 2790-0177; OCLC Number 1322801874

Tampering with Automated Data Processing Systems

Sabrina Maiza[1]

Abstract:
Crimes targeting automated data processing systems represent a distinct type of criminal phenomenon that differs from traditional crimes. These offenses raise numerous challenges, particularly in terms of detection and proof, due to the ease with which traces can be erased. This is especially problematic given that cybercriminals often possess high levels of intelligence and technical skills. Therefore, more flexible and adaptive solutions are essential to effectively address and combat such crimes.

Keywords: Cybercrime, automated data processing systems, digital evidence, cybercriminals, detection, proof, adaptive legal solutions.

| DOI: 10.56334/sei/7.4.16

Introduction:
Since the mid-twentieth century, the world has witnessed a new revolution known as the information revolution. This revolution has affected all areas of human life, and its cornerstone is the invention of the computer and the Internet. As a result, humans have come to rely on this technology and automated information systems as the main means of storing and processing data. However, this bright side does not negate the existence of negative repercussions represented by the assault on these systems, leading to the emergence of a new type of crime that differs from traditional crimes—namely, cybercrimes. These crimes take two forms: in the first, information or

1 PHD in Private Law, University of Taref Algeria, E mail: sabrina.maiza@gmail.com

automated processing systems serve as a means to commit the crime, while in the second, the system itself, including its physical components, is the object of the crime. The latter is the focus of this study.

These crimes are of recent origin, as they are linked to automated data processing systems and electronic computers. They target information and data and are committed by highly intelligent offenders—Internet hackers—whose attacks affect both stored computer data and information transmitted through information systems and networks. The latter are represented by invisible electronic signals flowing automatically through parts of automated processing systems and global communication networks.

As mentioned earlier, crimes of assault or tampering with automated data processing systems are modern topics that have imposed themselves on both national and international levels, prompting legislators in various countries to intervene with specific provisions to put an end to such practices.

Given the special nature of criminal law—which is based on the principle of legality, the prohibition of analogy, and strict interpretation—it became clear that traditional rules were inadequate to address this phenomenon. Consequently, the Algerian legislator, like others, enacted laws consistent with the nature of the crime of tampering with automated data processing systems. This was done by introducing a new section—Section 7 bis—under the title "Crimes of Tampering with Automated Data Processing Systems," through the amendment of the Penal Code by Law No. 04-15 of 10/11/2004, supplementing Ordinance No. 66-156 containing the Penal Code, under Articles 394 bis to 394 bis 7, which are the crimes under study.

This raises the following problem: **To what extent is the protection established by the Algerian legislator effective in limiting these assaults, considering them as modern crimes of a special nature?**

To answer this problem, we must first address the concept of the automated data processing system, then the legal framework of crimes against these systems, and finally the protection established by the legislator against such crimes.

I. The Concept of Automated Data Processing System

The automated data processing system is the essential condition for determining whether an assault on such a system exists or not. In its absence, there is no crime to investigate; therefore, it is necessary to define this concept.

1. Definition of Automated Data Processing System:

a. **Definition of "system":** It is a composite entity formed from several distinct units connected to each other through a number of relationships established to achieve communication and interconnection among its different components and units.[2]

b. **Definition of "data":** Data are words, numbers, symbols, facts, and raw statistics that have no relationship among them but are suitable for forming an idea or knowledge through human interpretation or by tools and devices. Data are often used synonymously with "information," but infor-

[2] Rachida Bouker, *Crimes of Assault on Automated Processing Systems in Algerian and Comparative Legislation*, 1st ed., Al-Halabi Legal Publications, 2012, p. 50.

mation refers to data that have been processed appropriately to provide complete meaning to a specific user.[3]

Accordingly, data are the raw material of information systems that are processed to obtain information.

The term "automated data processing system," according to the definition proposed by the French Senate, is:

"Any combination consisting of one or several processing units that include memory, programs, data, input and output devices, and connection devices linked together by a set of relationships through which a specific result—data processing—is achieved, provided that this combination is subject to a technical protection system."[4]

The Algerian legislator defined it in Article 2 of Law No. 09-04 concerning specific rules for the prevention and combating of crimes related to information and communication technologies as: "Any separate system or group of interconnected or interrelated systems, one or more of which performs automated data processing according to a specific program."

Thus, a data processing system includes two elements: the first relates to the components that make up the system, and the second relates to the relationships linking these elements together for the purpose of automated data processing.

The French Senate points out that the system must be protected by a security device, and only protected systems enjoy criminal protection. However, jurists have disagreed on this idea, and the prevailing opinion is that computer systems and their data must enjoy protection regardless of whether they contain security mechanisms or not.[5]

2. Components of the Automated Data Processing System:

It consists of **hardware**, which refers to the tangible physical components necessary for its operation and performance, without which [6]a cybercriminal cannot commit the crime. These include input units, the central processing unit, and output units.[7]

It also includes **software**, which represents the logical aspect of the computer. It consists of a set of instructions aimed at carrying out operations through the data processing system. It is defined as a collection of programs, methods, and rules, and, where appropriate, documents related to the data processing unit[8]. Types of software include operating system programs and application programs.

Additionally, there are **network connections**, meaning the interconnection of two or more computer devices through wired or wireless connections. The most common types of networks are the Internet and Intranet.

---

[3] Boukthir Hayat, *Crimes of Assault on the Automated Data Processing System*, Dissertation submitted for the Master's Degree in Law, Faculty of Law and Political Science, Mohamed Lamine Debaghine University, Setif, 2014/2015, p. 9.
[4] Khetir Massoud, *Criminal Protection of Computer Programs: Methods and Gaps*, Houma Publishing House, Algeria, 2010 ed., p. 109.
[5] See Khetir Massoud, *previous reference*, pp. 111–113.
[6] Abdel Fattah Bayoumi Hegazy, *Evidence in Computer and Internet Crimes*, Al-Shatat Publishing and Software House, Egypt, 2007, p. 100.
[7] See Ali Jabar Al-Hussainawi, *Computer and Internet Crimes*, Al-Yazouri Scientific Publishing and Distribution House, Jordan, 2009 ed., pp. 24–25, and Rachida Bouker, *previous reference*, pp. 58–59.
[8] Ali Jabar Al-Hussainawi, *previous reference*, p. 25

II. The Specific Nature of Crimes Involving Automated Data Processing Systems

It is first necessary to define cybercrime in general. It is any unlawful act committed with criminal intent for which the law prescribes a penalty or preventive measure. Crimes arising from the unlawful use of the Internet rely primarily on information, which led to the term "cybercrime"[9] being used to describe this type of offense. The Algerian legislator defined it in Article 2 of Law No. 09-04.

1. Definition of Crimes Involving Automated Data Processing Systems:

They are any unlawful conduct directed at automated processing systems through attacks on the confidentiality of their non-material components, or their availability, integrity, or completeness.[10]

This crime is characterized by its special nature, both in terms of the object of the attack and the particular profile of the cybercriminal, who is marked by intelligence and technical expertise. The motives for committing these crimes vary depending on the psychology, mentality, and nature of the offender—ranging from fascination with technology, desire for wealth, revenge, or mere amusement.

Cybercriminals are classified into several categories, though not every offender fits strictly into one group. These include:

- **Hackers** (both amateur and professional),
- **Intruders**,
- **Malicious individuals**, and
- **Minors**.[11]

Unlike traditional crimes, cybercrimes are characterized by their use of "soft destruction techniques" and the absence of physical violence.[12]

III. The Legal Framework for Crimes Against Automated Processing Systems

As mentioned earlier, criminal law is based on the principle of legality. Accordingly, the Algerian legislator criminalized assaults on automated data processing systems and also criminalized conspiracy and attempts related to such crimes.

The legislator listed several criminalized acts under Articles 394 bis to 394 bis 07, including the following:

1. The Crime of Unauthorized Access or Unauthorized Remaining in an Automated Data Processing System:

The legislator addressed this crime in Article 394 bis, which requires the presence of both the material and moral elements.

[9] Saghir Youssef, *The Crime Committed via the Internet*, Dissertation for the Master's Degree in Law, specialization in International Business Law, Faculty of Law, Mouloud Mammeri University, Tizi Ouzou, 2012/2013, p. 7.
[10] Rachida Bouker, *previous reference*, p. 48.
[11] Boukthir Hayat, *previous reference*, pp. 35–38.
[12] Mohamed Ali Al-Aryan, *Information Crimes*, New University Publishing House, Alexandria, 2011, pp. 77–78.

a. **Material Element:**

According to the article, there are two forms of the material element of this crime: the **simple form** and the **aggravated form** related to unauthorized access or remaining in the system.

a/1. The Simple Form of the Crime of Accessing or Remaining in the System:

A-1-1 The act of entry: It refers to any form that involves breaching the computer system and accessing its contents, without the consent of the person responsible for that system, or to the misuse of the computer and its system by a person not authorized to use it and entering it to reach information.[13]

Referring to the Algerian Penal Code and according to Article 394 bis, the legislator did not require any particular status for the person who performs this entry; therefore the crime can be committed by any person regardless of his status, whether he works in the field of systems or has no relation to that field — it is sufficient that he is not among those entitled to access these systems. Likewise, entry need not be carried out in a specific manner.

Unauthorized entry is also established whenever it is contrary to the will of the system owner or the person who has control over it; it is also established when the offender entered the entire system or part of it. In addition, the act of entry is established when the offender was permitted to enter a specific part of the program but exceeded that permission by entering a part for which he was not authorized.[14]

Accordingly, the crime is constituted by the act of entering the system regardless of any other result — that is, the crime exists even if the perpetrator did not have the technical ability to carry out operations on the system.

A-1-2 The act of remaining: It is the presence of the offender inside the automated processing system, roaming among files, folders, data, and information, and moving from one part of the system to another continuously.[15]

There is no doubt that remaining inside a computer system after having entered it by mistake does not differ from unauthorized entry in terms of the need for criminalization; the criminal outcome in both cases is the same, namely access to a system not authorized for entry. The interest protected by the law in both cases is the protection of the computer system.

Unauthorized entry and unauthorized remaining may coincide. So when does the crime of entry end and when does the crime of remaining begin? One opinion in jurisprudence holds that the crime of entry is fulfilled from the moment of actual entry into the program and the offender remains for a short period inside it; after that moment the crime of remaining begins and ends when the state of remaining terminates. Another opinion defines that moment from the time when the offender knows that remaining inside the system is unlawful. The prevailing doctrinal opinion states that the crime of remaining inside the system begins from the moment the offender starts to roam within the system: if he entered and remained stationary, the act remains the crime of entry into the system; but if he begins to roam, the crime of remaining commences from that moment.[16]

2/ The mental element:

[13] Boukthir Hayat, *same reference*, p. 47.
[14] Khetir Massoud, *previous reference*, pp. 115–116.
[15] Rachida Bouker, *previous reference*, p. 213.
[16] Khetir Massoud, *previous reference*, p. 117.

The crime of entry is an intentional crime and general intent suffices. It is sufficient for this crime that the offender knows he is entering a system to which he has no right of access and intentionally remains in it despite the expiration of any right he may have had to remain there, even if the entry was lawful. If his knowledge is absent, the crime is not established. If the criminal intent is present in its two components — knowledge and will — the motive does not affect it; the criminal intent remains even if the motive for entry or remaining was mere curiosity.[17]

A/2 Aggravated form of the crime of entry into the system or remaining:

A reading of Article 394 bis shows two aggravating circumstances that increase the penalty for entry or remaining within the system: the case where the unauthorized entry or remaining results in erasure or alteration of the data contained in the system or in the system's inability to perform its function. It is sufficient for these aggravating circumstances to exist that there be a causal relationship between the unauthorized entry or remaining and the result that occurred, namely the erasure of the system data, the system's inability to perform its function, or the alteration of data.[18]

2/ The crime of intentional assault on system data

The Algerian legislator provided for it in Article 394 bis 1. This crime takes three forms — insertion, erasure and alteration — which together represent the material element, in addition to the mental element.

1- The material element:

The criminal activity of this offense consists in the unlawful acts of inserting, erasing, or altering, and the occurrence of any one of them is sufficient for the crime; their concurrence is not required for the criminal activity to exist. The common feature of these acts is that they involve manipulation of the data organized by the processing system: inserting new, incorrect information, erasing, or altering, and this is done by information technology[19]. Data that are processed externally and have not been entered into the processing system fall outside the scope of this crime.

Referring to Article 394 bis 1, the material element of the crime of intentional assault on data is a criminal conduct carried out by the offender that may take the form of insertion, alteration, or erasure.

1- Insertion:

It is feeding the system with the data to be processed, or with instructions necessary for the processing operation[20]. It also means entering data into the processing system that were not previously present. These data may be entered with the intention of confusing the correctness of existing data. Fabrication of data is perhaps the easiest to execute, especially in establishments with financial resources; the person responsible in the IT department is in the best position to commit this type of illicit manipulation.[21]

2- The act of erasure or removal:

[17] Khetir Massoud, *same reference*, p. 118.
[18] Khetir Massoud, *same reference*, p. 119.
[19] Ali Jaafar, *Crimes of Modern Information Technology Against Individuals and Government – A Comparative Study*, 1st ed., Zein Legal Publications, no place of publication, 2013, p. 534.
[20] Rachida Bouker, *previous reference*, p. 215
[21] Khetir Massoud, *previous reference*, p. 124.

There is no uniform term used among legislations to denote this act. The Algerian legislator used the term "removal," meaning removing part of the data recorded in the computer and present within the system, or destroying that support, or transferring and storing part of the data to another memory area, or setting new attributes that obliterate the old ones[22]. It is noted that the Algerian legislator intended by "removal" the destruction or complete erasure of data; the text did not exclude partial removal but rather adopted both partial and complete removal.

3- The act of alteration:

This term means changing the data present within the system and replacing them with other data. This act is carried out by foreign programs that tamper with the data either by erasing them wholly or partially or by altering them, using informational bombs, viruses[23]. Finally, we note that these acts are listed by way of example.

2- The mental element:

The crime of assaulting data is an intentional crime that is based on general criminal intent with its two elements — knowledge and will. The offender's will is directed to the act of insertion, erasure, or alteration with his knowledge of their illegality. Does it require specific criminal intent?
A/ General criminal intent: For general criminal intent to be established, the two elements — knowledge and will — must be present as previously explained. These acts performed by the offender intentionally and with knowledge are likely to change the state of the information, and it is not required that the criminal intent be direct in the sense that the offender's will be exclusively directed to cause the resulting effect; it is sufficient for intent to take an acceptable form, and it is not required that intent be specific — there is no distinction in Algerian legislation between some information and others.

Criminal intent is absent when knowledge is lacking, for example if the offender believed that the data subject to manipulation belonged to him.

B/ The necessity of specific criminal intent: The term "fraud" used in the text of Article 394 bis 1 does not indicate specific intent; rather it indicates that the crime is intentional only. The legislator did not use phrasing that would require specific intent or a special motive, which implies that this crime is established upon the mere presence of general intent.

3/ The crime of unlawful dealing in data:

The Algerian legislator criminalized it under Article 394 bis 2 and punished dealing in such data as well as dealing in data obtained from a crime. If the purpose of criminalizing dealing in data ab initio is to prevent the commission of the crime, then once the latter occurs the aim is, as far as possible, to eliminate it and limit its effects.

A- The crime of unlawful dealing in data fit for committing a crime:

The subject matter of the crime of dealing in data according to Article 394 bis 2 is the data stored, processed, or transmitted through an information system.

A/1 The material element:

[22] Boukthir Hayat, *previous reference*, p. 62.
[23] Khetir, Massoud. *The same reference*, p. 124.

Article 394 bis 2 criminalizes a set of acts that precede the use of these data to commit a crime, beginning with their design and research, passing through their collection, and reaching their provision, publication, or trade.

1- **Design:** It means preparing and creating programs or information suitable for committing a crime, usually done by specialists in this field, such as programmers. This includes designing programs to access and control an automated processing system — for example, hacking programs like viruses.[24]

2- Research: The Algerian legislator did not specify what is meant by the term "research," but we see that it refers to researching how to design and prepare this information, not merely searching for the information itself. That is why the word "research" follows the word "design" immediately, even though its wording is general.

2- **Collection:** It is the gathering of information that can be used to commit one of the offenses against automated processing systems, and it is assumed that such information poses a great danger and can be used to commit these crimes.
3- **Provision**: The legislator also criminalized this act under Article 394 bis 2 — placing devices online to be used by others and creating and assembling links between branching lines in order to access these devices.[25]
4- **Publication:** It is broadcasting the information that is the object of the crime and enabling others to view it by various means that can be used for publication. Publication extends to include any activity that transfers data to others, and publication is one of the most dangerous acts that can be committed regarding illicit information because it can transfer the criminal information to the greatest number of people and thereby enable its use.
5- **Trade:** It is offering the information to others for consideration; the consideration need not be monetary but may be in kind, such as services or otherwise. Trade includes all kinds of dealings involving information suitable for committing a crime against automated processing systems.[26]

A/2 The mental element:

The crime of unlawful dealing in data is an intentional crime, as indicated by the phrase "whoever intentionally and by fraud," and it is noted that the legislator employed two terms in the same article, whereas in previous articles he confined himself to indicating intent by the phrase "by fraud"; here not only general criminal intent suffices but also specific criminal intent is required. What is meant is that the offender's intent in dealing with this information is to prepare and pave the way for its use in committing a crime against automated processing systems.

B/ The crime of unlawful dealing in data obtained from a crime:

This is the second form provided by the legislator and consists of possessing information obtained from a crime, creating it, publishing it, or using it — and the occurrence of any one of these acts suffices for the establishment of the crime.

1- **The material element:**

It is sufficient that one of the acts occur, namely possession. Possession is realized by the holder's absolute control over the data such that he can erase, alter, or use them. The material element of

[24] See Bouker, Rachida. *The same reference*, p. 259.
[25] Bouktir, Hayat. *The previous reference*, p. 72.
[26] Bouktir, Hayat. *The previous reference*, p. 74.

this crime is established once the offender stores and possesses the data without permission or authorization.

The Algerian legislator also criminalized disclosure; this presumes the transfer of these data from the possession of one person to others, as is the case with publication — that is, presenting these data unlawfully to people other than the possessor. The legislator intended to prevent disclosure and publication in order to limit their spread. Publication, as previously explained, was not limited by the legislator to any specific means.[27]

Likewise, use is one of the most dangerous acts, and through the text of Article 394 bis 2 the scope of criminalization was widened to include the use of the data and its purpose, whatever its type. The article did not specify the number of times necessary for the crime to occur as a result of unlawful use; thus a single use suffices for the crime to be established.

2- The mental element:

What is noticeable in the second paragraph of Article 394 bis 2 is that it punishes possession, disclosure, publication, or use for any purpose of all data obtained from one of the crimes; therefore, if the legislator had required specific intent, he would not have decided that the crime is established "for any purpose whatsoever," i.e., regardless of the offender's intent. Accordingly, the legislator intended general intent.

Fourth: Penalties for crimes of assault on automated data processing systems

The legislator prescribed a set of penalties for these crimes that affect the system, consisting of primary (principal) and additional penalties. He also provided for penalties for legal persons in addition to natural persons, as well as penalties for accomplices and partners, and the legislator considered attempt to be governed by the rules applicable to the completed crime according to the general rules.

1- Principal penalties:

Penalties prescribed for the natural person

A penalty is the sanction determined by the legislator and imposed by the judge on whoever is found responsible for committing his crime.[28]

a/ Penalty for entry or remaining within the system:

For the simple form of the crime the legislator fixed the penalty as imprisonment from three months to one year and a fine from 50,000 DZD to 100,000 DZD, according to Article 394 bis. As for the aggravated form of the crime, Article 394 bis provides for doubling the penalty if this entry or remaining resulted in deletion or alteration of the system's data; while if this entry or remaining caused destruction of the system's functioning, the penalty shall be imprisonment from six months to two years and a fine from 50,000 DZD to 150,000 DZD.

b/ Penalty for intentional assault on data:

[27] Bouktir, Hayat. *The same reference*, p. 75.
[28] Khalifa, Mohamed. *The Criminal Protection of Computer Data in Algerian and Comparative Law*, Dar Al-Nahda Al-Arabiya, Cairo, 1988, p. 208.

The legislator fixed the penalty under Article 394 bis 1 as imprisonment from six months to three years and a fine from 500,000 DZD to 2,000,000 DZD.

c/ Penalty for unlawful dealing in data:

According to the text of Article 394 bis 2, the penalty is imprisonment from two months to three years and a fine from 1,000,000 DZD to 5,000,000 DZD.

Penalties prescribed for the legal person

The Algerian legislator approved the principle of criminal liability of the legal person in the Penal Code by the text of Article 51 bis and set three conditions for the possibility of criminally prosecuting the legal person, which he specified as follows: that one of the crimes provided for by law be committed, that it be committed by one of the members or representatives of the legal person, and that the crime be committed for the account of the legal person[29]. He specified the penalties in Article 18 bis of the Penal Code.

It should be noted that the liability of the legal person does not preclude the prosecution of natural persons as perpetrators or accomplices.

2- Penalty for participation and attempt in the crime

a/ Penalty for participation: According to Article 394 bis 5, it does not depart from the general rules regarding the penalty for an accomplice and prescribes for him the same penalty as for the completed crime, and likewise in the case of an agreement among a group of natural or legal persons, it is punishable by the same penalty as the crime for which the preparation was made. As for the penalty for attempt, the legislator provided for it in Article 394 bis 7 and stipulated punishment for attempt to commit the offenses provided for in this section by the penalties prescribed for the offense itself. Referring to the text of Article 394 bis 5, we find that it is included in this text, meaning the Algerian legislator adopted the notion of attempt in criminal agreement.

3- Additional penalties:

Article 394 bis 6 stipulated a set of additional penalties, which are as follows: Confiscation — meaning confiscation of the devices, programs and means used to commit offenses against the system, by selling them or seizing them while taking into account the rights of third parties in good faith; closing sites — by this the legislator means Internet sites or electronic sites in general that were a means of committing these crimes or contributed to their commission; closing the establishment (the cybercafé) in the case of participation by the owner of the premises as a participant in the crime.[30]

Conclusion:
Crimes of assault on automated data processing systems are among the most dangerous crimes known to the modern world. These crimes have particular characteristics and the criminals possess a high degree of expertise, knowledge and intelligence; they commit their crimes in complete calm.

From this study we conclude that the object of these crimes is the automated processing system with its components, and that traditional provisions are insufficient.

[29] Bouskiaa, Ahsan. *A Brief in General Criminal Law*, 9th ed., Dar Houma for Printing and Publishing, Algiers, 2009, p. 243
[30] Khetir, Massoud. *The same reference*, pp. 130-131..

The Algerian legislator's establishment of legal protection for informational assets and thereby his implicit recognition of the economic value of information.

The legislator did not condition protection on the presence of technical protection for the information system.

Therefore, the Algerian legislator must continuously develop the existing legislation to achieve its flexibility and keep pace with the rapid developments in information technology. Create a new social culture that regards crimes of assault on automated processing systems as unlawful acts like other crimes.

It is necessary to develop international cooperation by strengthening training, research activities and exchange of expertise and experiences in order to continuously reduce the areas of imbalance and vulnerabilities that can be exploited by criminal networks specializing in cybercrime.

References

1. Rachida Bouker, *Crimes of Assault on Automated Processing Systems in Algerian and Comparative Legislation*, 1st ed., Al-Halabi Legal Publications, 2012, p. 50.
2. [1] Boukthir Hayat, *Crimes of Assault on the Automated Data Processing System*, Dissertation submitted for the Master's Degree in Law, Faculty of Law and Political Science, Mohamed Lamine Debaghine University, Setif, 2014/2015, p. 9.
3. [1] Khetir Massoud, *Criminal Protection of Computer Programs: Methods and Gaps*, Houma Publishing House, Algeria, 2010 ed., p. 109.
4. [1] See Khetir Massoud, *previous reference*, pp. 111–113.
5. [1] Abdel Fattah Bayoumi Hegazy, *Evidence in Computer and Internet Crimes*, Al-Shatat Publishing and Software House, Egypt, 2007, p. 100.
6. [1] See Ali Jabar Al-Hussainawi, *Computer and Internet Crimes*, Al-Yazouri Scientific Publishing and Distribution House, Jordan, 2009 ed., pp. 24–25, and Rachida Bouker, *previous reference*, pp. 58–59.
7. [1] Ali Jabar Al-Hussainawi, *previous reference*, p. 25
8. [1] Saghir Youssef, *The Crime Committed via the Internet*, Dissertation for the Master's Degree in Law, specialization in International Business Law, Faculty of Law, Mouloud Mammeri University, Tizi Ouzou, 2012/2013, p. 7.
9. [1] Rachida Bouker, *previous reference*, p. 48.
10. [1] Boukthir Hayat, *previous reference*, pp. 35–38.
11. [1] Mohamed Ali Al-Aryan, *Information Crimes*, New University Publishing House, Alexandria, 2011, pp. 77–78.
12. [1] Boukthir Hayat, *same reference*, p. 47.
13. [1] Khetir Massoud, *previous reference*, pp. 115–116.
14. [1] Rachida Bouker, *previous reference*, p. 213.
15. [1] Khetir Massoud, *previous reference*, p. 117.
16. [1] Khetir Massoud, *same reference*, p. 118.
17. [1] Khetir Massoud, *same reference*, p. 119.
18. [1] Ali Jaafar, *Crimes of Modern Information Technology Against Individuals and Government – A Comparative Study*, 1st ed., Zein Legal Publications, no place of publication, 2013, p. 534.
19. [1] Rachida Bouker, *previous reference*, p. 215
20. [1] Khetir Massoud, *previous reference*, p. 124.
21. [1] Boukthir Hayat, *previous reference*, p. 62.
22. [1] Khetir, Massoud. *The same reference*, p. 124.
23. [1] See Bouker, Rachida. *The same reference*, p. 259.

24. [1] Bouktir, Hayat. *The previous reference*, p. 72.
25. [1] Bouktir, Hayat. *The previous reference*, p. 74.
26. [1] Bouktir, Hayat. *The same reference*, p. 75.
27. [1] Khalifa, Mohamed. *The Criminal Protection of Computer Data in Algerian and Comparative Law*, Dar Al-Nahda Al-Arabiya, Cairo, 1988, p. 208.
28. [1] Bouskiaa, Ahsan. *A Brief in General Criminal Law*, 9th ed., Dar Houma for Printing and Publishing, Algiers, 2009, p. 243
29. [1]Khetir, Massoud. *The same reference*, pp. 130–131..