ISSN: 2352-975X مجلـة البـاحث للـدراسات الأكـاديـمـيـة EISSN: 2588-2368
ELBAHITH for Academic Studies
Volume: 09 /N°: 02 /Year: 2022 /pp: 767 - 782

The Crimes Of Attacks On Electronic Banks

Received date: 02/02/2022 **Accepted date: 03/06/2022**

Hadda Boukhalfa [*]
Oum El Bouaghi University
hadda.boukhalfa@univ-oeb.dz

Abstract:

There are many forms of violations and attacks targeting electronic bank security and the means through which these attacks are carried out are renewed and varied. Behind this is the special nature of the Internet, as it is an electronic network characterized by development, which helped the abusers to easily navigate through various websites, and the ease of sending and receiving data, which threatens the security of electronic banking transactions, in addition to the financial nature of banking transactions that are coveted by abusers to assault her. This study aims to focus on the images of abuse that pose a threat to the security of the electronic bank, and they are crimes against the data of these banks' websites and the systems and software they operate.

Keywords: *electronic bank; internet; banking services; e-client; electronic security.*

[*]**- Corresponding author**.

Introduction:

As the circle widens use of the Internet, and the data and information it contains, covering all aspects of economic life, its risks have broadened, and the methods and forms of the crime of penetrating bank account data and credit cards have developed, which is one of the most dangerous electronic crimes at all, and targets the majority of countries in the world, being a tempting target for hackers and fraudsters electronics.

In the light of evolving of the abuser method of these crimes, banking transactions have been of great importance to legal systems and jurisprudence studies, so it is not permissible to view them, or disclose them directly or indirectly, to any party, and the law punishes whoever deliberately discloses the confidentiality of banking and credit information seizure to, or by attacking the systems and software that he works with.

Achieving the bank’s electronic security is by securing the bank’s internal network and website, and securing all banking services it provides, against all forms of security threats.

The topic of this study aims to detail the most important forms of abuse that the electronic bank may be exposed to, and that negatively affect the financial services it provides and its relationship with clients.

Accordingly, the problem of this study becomes clear to us in: **What is the legal description of crimes committed against electronic banks?**

To answer this problem, we chose the following plan:

- Crimes against the bank's website data
- Crimes against the electronic banking system.

1. Crimes against the bank's website data

In order for electronic banks to be a safe environment to deal with and benefit from their services, the data that passes through their sites links must be secured, by addressing all crimes that threaten banking transactions, which is the crime of imitation of the bank's website and the crime of stealing personal data of clients.

1-1. The crime of imitation the website of the bank

The bank's website is the main base that the bank uses to contact its clients and provide its services through it, and the crime of imitation of this website poses a threat to the continuation of its work on the Internet, for that we will discuss this crime in detail.

1-1-1. Introducing imitation of the bank's website

This image is represented by the abuser's attempt to imitate the bank's website on the Internet, with the same design, by carrying the same logos and number of pages, and by creating the same links with it, in a way that the imitated website turn up as if it were the real website of the electronic bank. It is not required that the counterfeit site appear similar and identical to the real one. Rather, it is enough for the counterfeit site to cause confusion or ambiguity among clients in a way that prompts them to deal with it as the real site of the bank, as if the abuser imitated the basic distinguishing elements of the bank's site as its trademark, or his brand name(1) .

As for the Algerian legislator, it decided the implicit protection of computer programs, databases, multimedia work, and websites, in accordance with the text of Article 4 of Ordinance 05-03 related to copyright and related rights, and considered them as literary works written, whether in the source language or in the language of the machine(2).

We also note to the Algerian legislator that he did not defined the delict of imitation digital works, but rather explained its images in Articles 151 and 155 of the same order, in the following form:

- Illegal disclosure of the website: It means the disclosure process that takes place without the permission of the right holder, and it is considered a moral right, and it is not considered a misdemeanour of imitation.

- Compromising the integrity of the website: Electronic Bankmay pay any attack that affects the integrity of his work, and this prevents any distortion or modification of his work without his permission, and this is confirmed by the Algerian legislator, and compromising the integrity of digital works appears by the holders of the sites publishing copyright-protected works on their sites without the holder's permission(3).

- Reproduction of the website in the form of counterfeit copies: It means re-copying the website for several counterfeit copies in various ways to communicate it to the public, and the imitation takes place using several means, which are the reproduction of the entire website or part of it in an automated media system.

The abuser also works in exploiting the data exchanged between the bank and the client, which it obtains from the website, as the latter, after being deceived in this fake website, enters it and deals with it as he deals with the real website of the bank, so he enters his data as the user name and password The password, credit card numbers, and any other data related to dealing with the bank's website, then the abuser uses this data to deal with the accounts of these clients in a way that achieves the interest of the abuser and harms the client(4).

2-1-2. Crimes related to copying the bank's website

There are some indirect crimes attached to the crime of imitation the website of the bank, which were identified by the Algerian legislator in the text of Article 151, paragraphs 3, 4 and 5 of Ordinance 05-03 related to copyright and related rights(5), and they are:

• The crime of dealing in a counterfeit website:

The material element of the crime of dealing on a counterfeit website is the behavior that is based on dealing on the website of the electronic bank, whoever of where it is copied, whether it is counterfeit in the homeland or outside its borders. since the counterfeit

programs lie in their similarity to the original programs that are protected by law, the latter is based on simulation, in which the similarity is made between the original and the imitation, and the lesson in it is the similarities and not the differences(6).

Among the forms of abuse of these works lies according to the method and mode of their exploitation, and it occurs during sale, where the work cannot be exploited except for that. The act is focused on the same website or on an exact copy of it, and this extends the scope of protection as it includes the website and all its copies(7).

. Selling or renting counterfeit copies of software and offering them for circulation:

Article 149 of Ordinance 03-05 related to copyright and related rights confirm that "whoever sells, rents or offers for circulation a counterfeit copy of the work after committing a misdemeanour of imitation", the program shall be counterfeited if it is similar to the original program that is protected by law as stipulated use licenses attached to software have limits. Such dealings prevent the sale, rental, or lending of legitimate copies of the programs obtained by themselves, so that the right to exploit the programs granted for the purpose of the programs is limited to him, and cannot be transferred to others,also with regard to the rental in which the lessee uses the software for a certain period of time in return for a specific fee. Renting counterfeit copies of the software makes the lessee commit the crime of imitation(8).

• Import and export of counterfeit website:

This process consists in inserting real, non-imitation programs published abroad without the author's permission. The entry can be done in any behavior that would cross the programs published abroad, regardless of the nationality of the person who entered them and also whatever way they entered and it is required to provide the material corner in this crime, it is that these programs are published abroad, as it is required that their entry be without the permission of electronic bank or whoever replaces him(9),then this crime, as soon as the entry act,which appears completely,bypasses the perpetrator with the work on the customs or border area without being discovered by the border guards or those concerned. That and also, the illegal entry of these works, and the location, amount or size of the work or the behavior of the perpetrator towards it is not considered after that. The crime is

ISSN: 2352-975X _____EISSN: 2588-2368

related to the entry act, the subject of which is computer programs that are published abroad(10).

2-1.The crime of stealing electronic bank client's personal data

The protection of the personal data of the electronic client is a priority of the bank, as the credibility of the banking services provided by this bank is based on the trust between the bank and its clients, but the personal data of the bank client can be attacked through theft, and this is what we will discuss.

2-2-1. Definition of personal data theft of an electronic bank client

We will first go to the definition of the data under protection, then we'll figure out the crime of theft threatening this data.

• Identification of the data subject to protection:

It is the data of a personal nature as being the data through which the identity of a person can be inferred, whether such data declares the identity of that person, such as his name, or contains data in the aggregate that can be processed through the identification of this person. Personal data means also, any information, sound or image related to a person, identifiable or identifiable, either directly or indirectly, especially by referring to distinct elements of his physical, genetic, economic, cultural or social identity(11).

The data of electronic bank clients is characterized by the fact that it is not linked to the identity of its holder, unlike biometric data such as a fingerprint, which allows the use of this data by its holder, or others who work with it.

• Defining the crime of stealing the private data of the electronic client

Some jurisprudence defines data theft of dealers on the Internet as a misuse of another person's personal data, such as name, date of birth and e-mail address, without his knowledge or consent.

It was also known as penetration of computers connected to the Internet with the intention of stealing their data and the data stored in them, such as penetrating the networks of financial banks and banks to make illegal bank transfers(12).

What is noted on these definitions is that they do not view the theft of data related to clients via the Internet as merely seizing this data, but also require the use of this data badly, through the thief's dealing with this data as its holder, in a way that harms its true holder, Which

ISSN: 2352-975X _____EISSN: 2588-2368

makes the activity of this crime a complex activity that includes the appropriation of data and then using it in an illegal manner.

There are recent trends that tend to describe money on data of economic value for its holder, which finds its fertile field in banking transactions, where the bank's client data acquires the importance of the transactions that are used in it, and accordingly it seems to us the definition of theft of this data as a form of violations that It targets the electronic bank security since it is a person who seizes the data of the bank's client, which he uses in dealing with the bank over the Internet.

2-2-2. Elements of the crime of stealing the personal data of the client in the electronic bank

The crime of stealing the personal data of the electronic client of the bank has several elements, which we mention as follows*:*

• Methods of stealing personal data of electronic bank clients

The process of stealing the personal data of the electronic client is carried out in one of the following ways(13):

a- The abuser sends fake e-mail messages to the electronic bank client, portraying them as coming from the bank, where they ask in these messages to send the client's password, or his account numbers, and justify this, for example, by wanting to delete this data from the database Bank's due to a malfunction.

b- The abuser installs devices that monitor the client's behavior and dealings with all the tools that he can use to communicate with the bank, such as his personal computer or cash withdrawal machines.

c- The abuser resorted to fraudulent means, such as creating a website, displaying fake products or services through this website, and asking the client to enter the details of his name, email address, and bank account numbers to obtain the item or the advertised service, and then exploits this data in dealing with the electronic bank.

d- The abuser searches the papers, documents or invoices of the electronic bank client, for details of his personal data, which can be exploited in dealing with the electronic bank.

• Methods of exploiting the data of the e-client

The process of stealing personal data does not stop when it is seized, but rather goes beyond its disposal and exploitation, and this is as follows:

A- Controlling the client's electronic account

The abuser, after seizing all the data of the client's account, uses it

ISSN: 2352-975X _____EISSN: 2588-2368

to access this account through the bank's website, and to deal with this account as its holder by making electronic transfers for himself or for others, and he can also open a new account with the money in this account in his name, the abuser can also, after entering the account, change the password for accessing it in order to deprive the real account holder from entering or dealing with it.

B- Submitting fake requests

The abuser exploits the data he seized, and treats it as if it were its holder. For example, he fills out forms for obtaining goods and services using this data.

As for the Algerian legislation, in the absence of a provision to protect personal data in the face of automated processing, indirect protection of information privacy can be provided through Articles 394 bis to 394 bis 7 of Penal Code No. 04-15(14),under a new chapter entitled: "Infringement of automated data processing systems." In which the legislator abuserizes activities or actions that are considered an attack on automated data processing systems.with the aim of protecting automated processing systems or systems. It seems clear not to refer to personal data or data from near or far, because the goal of the text is to protect the processing systems in themselves.

We need legislation that protects data or personal data for themselves as they constitute an important aspect of an individual's privacy and private life. There is no law related to this issue in particular, with reference to Article 27 of the law No. 04-19 related to the recruitment of workers and the monitoring of employment(15),which provides for the protection of personal data, as it states: "Disclosure of personal information that affects the private life of an employment applicant is subject to a fine of 50,000 to 100,000 DA".

It is also noteworthy Law No. 09-04 of August 15, 2009 setting the rules for the prevention and control of crimes related to information and communication technologies(16) ;which did not bring anything new regarding the protection of personal data. On the other hand, it obligated service providers to collect traffic data, which are data related to communications operations and their preservation. For a period of one year, he organized the inspection of the information system; Without regard to the issue of the protection of the personal data that it may contain.

Addition to it, Law No. 15-04 related to electronic signature and certification(17); in which the legislator set out the general rules related to electronic signature and certification, which require the collection and processing of some personal data, as Article 05 of it stipulates that the collected databases must be located within the national territory, Article 71 punishes with imprisonment from 6 months to 3 years, and a fine of 200,000 to 1,000,000 dinars, and with one of these two penalties, the certification services performer who collects personal data of the electronic signature without his express consent or uses it for other purposes.

And in Article 72, he is punished by imprisonment from 3 months to two years, and a fine of 200,000 to 1,000,000 dinars, or one of these two penalties for the certification services performer who breached his obligation to maintain the confidentiality of data, which makes it provide penal protection for personal data by preventing its collection without the consent of its holder or its exploitation outside The specific purpose of its collection, even if the protection remains limited to personal data related to the electronic signature.

2- Crimes against electronic banking systems

Shows the gravity of these crimes appears in the bank's internal network linking to the Internet that is open to the whole world, as it represents a weak point that abusers can exploit to penetrate and infringe the electronic bank systems, and we will address the forms of this infringement in the following form.

2-1. Illegal presence in electronic banking systems

The abusers are working to gain access to the electronic bank systems and carry out illegal entry hacks to the electronic bank devices, and this form of attacks may be in various forms, which can be addressed as follows.

2-1-1. Illegal access to electronic banking systems

Entry to the information system is based on a permit from the electronic bank, which is the holder institution, or the person who owns this system. Otherwise, this is considered a breakthrough, and this phenomenon has grown due to the development of the Internet and technology.

And what is meant by illegal access, is the process of accessing information systems without the permission of the holder, and it is also defined as entering the information system without the

permission of the holder of the computer or information[18], or "It is the misuse of a computer and its system by a person who is not authorized to use and access it, to gain access to the information and data stored inside it, to view it or just for fun, or to satisfy the feeling of success in penetrating the computer"[19] ,"Unauthorized access to the computer system derives its illegality from being unauthorized or in violation of the provisions of the law"[20].

The Algerian legislator included the crime of entering information systems in Article 394 bis of the Penal Code[21],according to the amendment, " …Anyone who enters or stays by fraud in all or part of the automated data processing system or attempts to do so".

The meaning of the term fraud is that it is carried out in a fraudulent way, so that he does not have the right to access or password or any legal electronic procedure used by the electronic bank ,the holders of this system, and accordingly, every person who entered an information system in part or all of it is considered in violation of the law and is punished for the crime of entry, Therefore, some legal legislations and jurists use the term hack to denote the illegality of access to the information system[22].

And "French jurisprudence considers that entry has a moral meaning, as entering a data processing system, information system, or electronic system is similar to entering a human's memory, and it also has a physical meaning, which is that the person has tried to enter or has already entered the information system for electronic trade"[23].

That is, the illegal entry is not always by entering the information system, as information may be intercepted to access the information that it transmits without the need to enter into a local network, as in the case of capturing signals bounded by an electronic device, without the need to enter directly within the network that carry the message[24]."That is because the act of entry, which constitutes the physical pillar, is not to go to the place where the computer and its system are located. Rather, It means access, using technical means, to the information system, or physical or electronic access."[25]

And "some people differentiate between two types of illegal entry, the first is defined in terms of location, which is infiltration into the information system, and the second is defined in terms of time, which is to exceed the limits of the permit or license within the system and granted for a limited period of time, by exceeding this limited period

of time"[26].

And "abuserizing access may focus on accessing information that is processed automatically, for every information is recorded on any medium for storing information, such as magnetic tapes, for example, which form part of the computer, and can only be accessed through automated information processing systems"[27],Which is the subject of an act of unauthorized entry.

Access may be to one of the parts of the automated information processing system, most of the legislation that abuserizes unauthorized access to computer systems tends to abuserize access to one of the parts that make up the system[28]. In France, the computer system means all its parts, from the processing unit to the memory unit, to the parts that connect the different elements of the system[29].

The Algerian legislator did not specify the character of the abuser who carried out the illegal entry process, so Article 394 bis of the Penal Code[30]expressed this by saying: "Anyone who enters or stays...", whether the abuser is an amateur or a professional using computers who constitute a category Internet users or visitors, or if he is one of the workers in the information system, and the abuser may be affiliated with one of the employees of the electronic bank that owns the system that was hacked.

We also note that the entry procedure may be similar to other behaviors via the information network, including the operations carried out by technicians via the Internet. The Internet who carry out their tasks of entering the information systems and transferring the data, if these operations that they carry out within an authorized legal framework, it is not considered a crime of entry punishable by law.

2-1-2. Stay fraudulent

Stay fraudulent is an operation that follows the process of entering the system, whether this entry is legitimate or illegal, and therefore it is the entry and stay of any person in the information systems in a fraudulent manner and in bad faith. It is defined as "being inside the automated processing system against the will of those who have the right to control this system"[31]. "The crime of illegal stay within the information system in general is considered one of the crimes that is difficult to prove, as the accused claims, in the event of his arrest, that he was about to separate from the infringed system"[32].

And the illegal stay within the information system is continuous,

meaning for a certain period, but this does not mean that staying for a short period does not constitute a crime. That this is illegal, and thus it is a crime that requires the continuation of the act of survival, and here the question arises for the abuser who enters by mistake and leaves quickly, is he considered a perpetrator of the crime of survival or not.

Article 394 bis of the Algerian Penal Code(33) explicitly states that the crime of illegal presence in information systems must be an intentional crime, and this is evident from its saying: "Anyone who enters or stays through fraud ...". On this, Article 323-01 of the French Penal Code stipulates that it says: "Frauduleusement, and this expression means that the perpetrator commits his act or refrains from it knowing that he is not authorized to do so, and if the crime is in violation of the legislator's orders and prohibitions, the will to investigate This violation constitutes the utmost degree of sin, given that the abuser has thus expressed his will to disobey and comply with the law."(34) .

3-2. Disable the electronic banking system

The process of penetrating the electronic bank systems leads to another type of attack, which is the attack on the information, data and sites occupied by this system, which we will discuss in detail in the following form.

3-2-1. The crime of information attack on electronic bank systems

The crime of informational attack on electronic bank systems is considered a deliberate crime in which the abuser's will is directed to carry out an illegal act, which is the introduction, modification or deletion of the data of the bank's information system, whether it is data or information programs, and this is what the Algerian legislator stipulates in The Penal Code in Article 394 bis 1(35).

• Introduction:

"The act of inserting is intended to add new data to its props, whether they are empty, or there were data on them before, and this act is achieved in the purpose for which the legitimate holder of magnetic debit cards uses the latter to withdraw money from ATMs, when he uses his private and secret number to enter in order to withdraw an amount of money more than the amount in his account"(36).

And the Introduction here works to change the data and information

in the information system and it can also change the way the programs in which this electronic bank system works, which leads to a change in the entire system. The abuser may enter fake data or information that enables him to seize the data Personal often related to the elements of financial disclosure in order to make money for himself.

.Deletion: "The act of erasure means removing a part of the data within the electronic bank system, or transferring and storing it in another part of this system to the memory area. This process here works to change the content of the information system."(37) And the Algerian legislator did not specify the way in which the act of removal is carried out, and whether it is done with a special program or by means of a key or icon of erasing only, nor did it indicate the type of data or programs that are being erased, and thus it can be said that the Algerian legislator stipulated the act of erasure on all The data and systems contained in the electronic bank's information system.

However, this erasure sometimes may be by distinguishing some programs or information that the information system contains or works with.

•**Modification:** The act of modification means changing the existing data within the electronic bank system, either by replacing it or adding other data different from it, or the modification is also by changing the program in which the data is processed with another program similar or different from it, as it can be an act .

Modification is by changing the channel through which the data is sent or the way it is sent. The abuser is by violating the ports and accessing the database, modifying it or adding false information to it with the aim of illegally taking advantage of that data.

"Where the abuser intent here on the information system is to make a change in it, whether by adding data, programs,viruses, operating systems, deleting them, or transferring them from the information system to another place. As for the physical element, it is done as soon as there is a change in the system, the abuser behavior is assault The information system may have a negative impact on it by modifying its electronic content in any way"(38).

3-2-2. The crime of hamper the work of the electronic banking system

The Algerian legislator did not provide a text for the intentional attack on the functioning of the electronic banking system. It was

satisfied with the text on the intentional attack on the data inside the system. This may be explained by the fact that the attack on the data may affect the validity of the system to carry out its functions, and jurisprudence has set a criterion for distinguishing between assault On the data and attack the system on the basis of whether the attack is a means or an end."If the attack on the data is just a means, then the act constitutes a crime of willful attack on the electronic banking system, but if the attack on the data is an end, then the act constitutes the crime of intentional attack on the data"[(39)].

There are many ways that the abusers use to access the electronic banking system and disrupt its work, to[(40)]:

-Occupying the bank's website in a way that prevents access to it via the Internet, such as an attempt to send a huge amount of e-mail messages to the bank's website that are greater than the bank's ability to absorb, in a way that causes flooding and makes the website unable to deal.

-Preventing communication between the work points on the site in a way that prevents access to the services provided by these points, such as deleting the communication links that link the bank's home page to the sub-pages of the banking services provided by the bank.

-Preventing the banking service from reaching a particular institution or to a particular individual, by cutting off the means of communication that link the bank and one of the institutions that receive a specific service from the bank, such as one of the stores that are linked to the bank's website, and that accept payment with credit cards issued by the electronic bank .

4. CONCLUSION

During its various stages, this study reflected the paramount importance of the electronic bank on the Internet, as an effective economic institution in the field of electronic commerce, and it touched upon the images of attacks targeting the security of the bank, and how the legislator was exposed to these crimes and the penalties prescribed for them, in maintaining the continuity of banking operations and the relationship The electronic bank with its clients.

The abuser on the security of electronic banks uses all electronic methods and media to enter their systems and websites to obtain information and data that facilitates them to commit crimes affecting the safety and health of banking operations, and thus takes advantage

of the lack of control and protection that electronic banks must adopt to achieve their security via the Internet.

*** Results:**

-In committing these attacks on the bank's electronic security, the abusers depend on some technical and security gaps, which the bank must fill in order to secure the client's transactions, and work to maintain and treat any penetration or attack in the shortest possible time.

-The bank's preventive measures to protect its information system are of the nature of its legal obligations with regard to securing its website, and securing its banking transactions on the Internet.

-The attack on the bank's electronic security constitutes any activity that threatens the security and integrity of the bank's systems and what it contains of information and personal data of clients. For this reason, only clients who have the password for dealing with the bank are allowed to enter the websites of banks.

-The special nature of the banking business imposes on it some obligations towards its clients, in maintaining the confidentiality and security of banking transactions, which are related to the existence of the bank, and strict legal concepts have appeared in securing the work of electronic bank systems, in order to be in line with its requirements and the nature of its work.

*** Recommendations:**

- The electronic bank must secure the physical and intangible components of the system in which it operates, and it must surround all parts of the network and its components, including hardware, software, and means of connecting the network, with an appropriate security wall that ensures that the electronic bank's systems are not attacked.

-The bank must conduct a periodic examination of all network components and the data they contain to avoid any damage or modification that may have occurred to the information and data of the electronic banking systems, and may expose the personal data of clients for penetration or disclosure.

-The electronic bank must provide the access system to the bank's internal network with special protection means and applications, through numbers and identification codes specific to each client, or by resorting to strong encryption systems.

ISSN: 2352-975X _____EISSN: 2588-2368

-Drawing a clear legal framework that defines banking operations on the Internet for banks only, and not allowing anyone other than the electronic bank to operate in them, given the fact that it enjoys exclusive legislative and supervisory guarantees, and its great importance in economic life.

References:

(1)-Al-Tamimi Alaa,The Legal Regulation of the Electronic Bank on the Internet, New University House, Alexandria, 2012, p.533.
(2)-Ordinance 05-03, relating to copyright and related rights. J.R. No. 44, 2003, July 19.
(3)-Deedan Mouloud; Shariqi Nasreen,Intellectual Property Rights- Copyright and Neighboring Rights-, Dar Belqis Publishing, Algeria, 2013, p.20.
(4)-Ghanem Sherif Muhammad,The Bank's Responsibility for Computer Errors in the Electronic Transfer of Money, Dar Al-Nahda Al-Arabiya, cairo, 2010, p.69.
(5)- Ordinance 05-03.
(6)-Al-Qahwaji Ali Abdel Qader, Criminal Protection for Computer Programs, Dar Al-Jamaa for Printing and Publishing, Lebanon , 1999, p.20.
(7)- Al-Manasah Osama Ahmad; Al-Zoubi Jalal Muhammad,Electronic Information Systems Technology Crimes, House of Culture for Publishing and Distribution, Jordan ,éd. 6th, 2012, p.212.
(8)-Salma Imad Muhammed,Legal Protection of Computer Programs and the Problem of Software Piracy, Wael Publishing House, Jordan , éd. 1st ,2014,p.80.
(9)- Al-Qahwaji Ali Abdel, Op.Cit,p.20.
(10)- Al-Manasah Osama Ahmad; Al-Zoubi Jalal Muhammad, Op.Cit, p.212.
(11)- Salma Imad Muhammed, Op.Cit, p.36.
(12)- Al-Tamimi Alaa, Op.Cit, p.590.
(13)- Al-Tamimi Alaa, Op.Cit, p.592.
(14)- Law No 04-15,the Penal Code. J. No. 71, 2004, November 10.
(15)-Law No 04-19,relating to the installation of workers and the control of employment. J.R. No. 83, 2004, December 25.
(16)-Law No 09-04,containing special rules for the prevention and control of crimes related to information and communication technology. Jr. No. 47, 2009, August 05.
(17)-Law No15-04, relating to the general rules relating to electronic signature and certification. J.R. No. 06n,2015, February 1.
(18)-Bainbridge David,Hacking The Unauthorised Access of Computer Systems. T. M. Review, Éd. 52, 1989,p.237.
(19)-Adel Muhammad Farid Qora Naila,Economic Computer Crimes- A Theoretical and Applied Study-, Al-Halabi Human Rights Publications, Lebanon, 2005,p.319.
(20)- Ibid,p326.
(21)- Law No15-04.
(22)- Fachar Atallah Confronting Information Crime in Algerian Legislation. Maghreb Forum on Law and Informatics, 2009, October, p.23.
(23)-Al-Kaibi Muhammad Obaid,Criminal Protection for E-Commerce éd, 1st, Dar Al-Nahda Al-Arabiya, Cairo, 2010,p.439.
(24)- Adel Muhammad Farid Qora Naila Op.Cit, ,p321.

(25)-Abdel Qader Al Momani Nahla,Information Crimes éd, 2nd,House of Culture for Publishing and Distribution, Jordan,2010,p.158.
(26)- Al-Kaibi Muhammad Obaid, Op.Cit, pp. 439-440.
(27)- Adel Muhammad Farid Qora Naila, Op.Cit, p329.
(28)- Al-Qahwaji Ali Abdel Qader, Op.Cit,pp. 119-120.
(29)- Adel Muhammad Farid Qora Naila, Op.Cit, pp. 330-331.
(30)- Law No 04-15.
(31)- Al-Qahwaji Ali Abdel Qader, Op.Cit, p.52.
(32)- Abdel Qader Al Momani Nahla, Op.Cit, p. 161.
(33)- Law No 04-15.
(34)- Adel Muhammad Farid Qora Naila, Op.Cit, pp. 330-331.
(35)- Law No 04-15.
(36)- Fachar Atallah, Op.Cit, p. 30.
(37)- Ibid, p. 30.
(38)- Ibid, p. 31.
(39)- Ibid, p. 41.
(40)- Al-Tamimi Alaa, Op.Cit, p. 568.