

*facing the acts of prejudice to the automatic data processing systems -  
criminalization and punishment - with regard of the Algerian penal code*

.Benbouabdallah mounia<sup>1,\*</sup>

Faculty of Law University of Souk Ahras  
(Algeria<sup>1</sup>),

[m.benbouabdallah@univ-soukahras.dz](mailto:m.benbouabdallah@univ-soukahras.dz)

Received: 03 /11 / 2021 Accepted: 12 /05 / 2022 Published: 27 /12 / 2022

**Abstract:**

The Algerian legislator has dealt with crimes of prejudice to the automatic data processing systems in Chapter Seven bis of the Penal Code. These crimes, according to the Penal Code, are the illegal entry and stay in the automatic data processing system, and the intentional assault on the functioning of the automatic data processing system, The legislator also linked some terrorist activities such as financing and recruitment to the use of information and communication technology under Law 16-02 supplementing the penal code, and created another form of information crime under Article 394 8 Duplicate created under Law 02-16, with penalties for these crimes as a whole, misdemeanor, except for what is related to terrorist activity. Felonies are considered according to Articles 87 Duplicate 11 and 87 Duplicate 12 introduced in Law 02-16.

**Keywords:** Automated data processing, criminalization, punishment, cybercrime.

**المخلص:**

تناول المشرع الجزائري جرائم المساس بأنظمة المعالجة الآلية للمعطيات في الفصل السابع مكرر من قانون العقوبات، وتتمثل هذه الجرائم حسب قانون العقوبات في الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات، والاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات، كما ربط المشرع بعض الأنشطة الارهابية كالتمويل والتجنيد باستعمال تكنولوجيا الاعلام والاتصال بموجب القانون 02-16 المتمم لقانون العقوبات، واستحدث صورة أخرى للجريمة المعلوماتية بموجب المادة 394 مكرر 8 المستحدثة بموجب القانون 02-16، مع رصد عقوبات لهذه الجرائم في مجملها جنح إلا ما تعلق بنشاط ارهابي فتعد جنایات حسب المواد 87 مكرر 11 و 87 مكرر 12 المستحدثة بالقانون 02-16.

الكلمات المفتاحية: المعالجة الآلية للمعطيات، التجريم، العقاب، الجريمة الإلكترونية

\*Benbouabdallah mounia ( MCA)

## I. INTRODUCTION

Due to the spread of modern means of communication and their frequent use, and the almost total dependence on these means and various information networks, In its entirety, this constituted the necessity of the actual organization of this space and defining the circle of permissible and prohibited acts related to information and communication technology, This is based on giving meaning to every diamond act in these systems. The experts of the Organization for Economic Cooperation and Development (OECD) defined information crime, as "all illegal, unethical or unauthorized behavior related to the automatic processing of data or its transmission," as Professors Robert J.LINDQUIST defined it. Jack Bologna is "a crime in which the computer is used as a means or a tool to commit it, or it represents a temptation to do so or a crime in which the computer itself is a victim." As for the French jurist Vivant, "information crime" is a group of acts related to informatics that may be punishable(9 ص ن، دون س ن، قطب).

Based on these visions, the Algerian legislator amended the penal code according to Law No. 04-15 of 10/11/2004, and the seventh section added a duplicate on crimes against the automatic data processing systems, and clarified the penalties for each crime, But it is not known what is meant by information crime, due to the criticisms directed at the legislative deficiency in facing this crime, the legislator intervened to avoid this through Law No. 09-04 of 26/08/2009, It includes the special rules for the prevention of these crimes. Article two of it has mentioned "Crimes related to information and communication technology: crimes of infringing upon the automatic data processing systems specified in the Penal Code and any other crime committed or facilitated by an information system or an electronic communication system." This article clarifies the desire of the Algerian legislator to adopt the principle of flexibility in the legislative drafting, in order to accommodate electronic criminal activities that cannot be quantified, and to determine the rapid development of their methods as a result of technical development this gives the judge a wide freedom of appreciation, and the legislator, through this law, tried to keep pace with the information crime movement in Algeria(409 ص معاشي، 2018).

Despite the delay of the legislator in combating this type of crime, it tried to keep pace with international developments and issued an amendment to the Penal Code 16-02 which touched on some of the information crimes and even linked terrorism to this type of crime. What raises the following problematic: **Has the Algerian legislator agreed in defining these crimes and monitoring the appropriate penalties for them?**

The answer to this problem requires addressing the following axes:

The first axis: the limits of criminalizing acts affecting information technology and communication.

- The second axis: the forms of penalties imposed for crimes of compromising information and communication technology.

### ***1 the limits of criminalizing acts affecting information technology and communication.***

Information crime has many characteristics, among which are (102 ص نمبدلي، 2017):

-Information crime is a global crime with borders.

- The perpetrators of cybercrime have special characteristics, as the information criminal is a specialist and professional, and does not resort to violence as he has intelligence, skill, knowledge, and a high degree of culture.

-Cyber crime is a difficult crime to prove.

And every crime consists of elements, and because the information crime has been stipulated in many laws, and due to the multiplicity of its types and forms, so we will deal in the study only with what was mentioned in the Penal Code.

### 1.1 *the legitimate element of This crime:*

There is no crime and no punishment except by a legal text that defines that criminal behavior for us and the appropriate punishment for it. The legislator has interfered with regard to information crime and stipulated it in the penal code in Section Seven bis under the heading of prejudice to automatic data processing systems, And it decided the special penalties for each crime, and the criminal legal texts for acts affecting information and communication technology are represented in Articles 394 Duplicate up to 394 duplicate 8, and part of these crimes dealt with Articles 87 duplicate11 and 87 Duplicate 12.

On the basis that the automatic data processing system represents the primary condition, which must be fulfilled in order to search for the availability or non-availability of the elements of the crime of assault on this system, if it is proven that this initial condition is defective, then this research will not be possible(قارة، 2001، ص 32).

### 1.2 *the material element:*

We will deal with all the crimes mentioned in the seventh section, bis, for crimes of infringing upon automatic data processing systems, and articles 87 duplicat 11 and 87 duplicate 12 of the code penal.

#### **First – The illegal entry and stay in the automatic data processing system:**

Article 394 duplicate of the Penal Code stipulates: “Anyone who enters all or part of a system for automatic data processing or attempts to do so shall be punished with imprisonment from three months to one year and a fine from 50,000 to 100,000 DZD. The aforementioned acts resulted in sabotaging the system’s operation system. "The penalty is imprisonment from six months to two years and the fine is from 50,000 to 150,000 dinars."

\* This crime through Article 394 bis, we note that it has two forms, the simple image is merely illegal entry or stay, and the aggravated image is achieved by the availability of the aggravating circumstance for it, and it is in the case in which the unlawful entry or stay results in either deletion or change System data or sabotage the system's operating system.

**A- The first simple element:** represented in the mere illegal entry or stay in the automatic data processing system.

- The act of entering into this crime (which is the material pillar of the crime of assaulting the automatic data processing system). Entering here does not mean entering in the material sense, that is, entering a place, house or garden, but rather it must be seen as a moral phenomenon. The similarity to that which we know when we say entering into an idea or into the faculty of thinking in a person, i.e. entering into the mental processes carried out by the automatic data processing system, and the legislator did not specify the means of entry or the way in which to enter the system, so the crime occurs by any means or method. It is equal to entry directly or indirectly(قارة، 2001، ص 32).

It is noticed through this article that the Algerian legislator considered the crime of unauthorized entry as a formal crime (in which the physical element is not required to achieve the criminal outcome), meaning that it is an offense merely to enter the system of automatic data processing, in whole or to only part of it, provided that it is actually To enter without a permit is intended and is not just a coincidence or a mistake(براهيبي، 2016، ص 127).

Remaining unauthorized in the automatic data processing system means continuing to be present within the processing system without permission from its owner or has control over it, meaning that a person remains inside the treatment system the property of others after entering into it by mistake or by chance, despite knowing that his / her stay there is unauthorized, and the crime of unauthorized survival is realized according to Article 394.

The aforementioned repeater has achieved its material pillar represented in the act of staying without a face of hatred, regardless of whether this survival was intended by the perpetrator or

not intended, and the Algerian legislator considered the crime of the licentious baggage with this system of automatic data processing of formal crimes that do not require their occurrence to achieve a criminal result. To acknowledge the existence of the crime of complete existence and its foundations. (براهيبي، 2016، ص 130-131)

**B - The second aggravating element:** In order for the aggravating circumstances mentioned in Article 394 bis Paragraph 2 to be available, it is necessary to prove the existence of a causal relationship between the act of entering or remaining unauthorized, and the criminal outcome specified by the article in the erasure and modification of the system data or sabotaging the operation of the system itself, otherwise we were in the process of a crime in its simple aforementioned form. In the text of Article 394 duplicate 1 of the Penal Code, and perhaps the goal of this strictness is to limit the aggravation of information crime (براهيبي، 2016، ص 133)

***Second - Intentional attack on the automatic data processing system:***

The Algerian legislator stipulated it in Article 394 duplicate 2 of the Penal Code: “Anyone who, by means of fraud, introduces data into the automated processing system, or removes or modifies, by means of fraud, the data it contains shall be punished with imprisonment from six months to three years and a fine from 500,000 to 2,000,000 dinars.”

**A- The first type: Intentional attacks on the data within the system,**

The criminal activity in the crime of deliberate assault on data is embodied in one of the following three forms: L'intrusion, L'effacement, and Modification, and these images are not required to meet, rather it is sufficient for the perpetrator to issue one of them only in order for the material element to be available, and the acts of insertion, erasure and modification It involves manipulating the data contained in the automatic data processing system, whether by adding new incorrect data.

Or erase or amend pre-existing data, which means that the criminal activity in this crime is only in response to a specific place or topic, which is the data or information that has been processed automatically, which has become mere signs or symbols that represent that information, and not the information in itself as One of the elements of knowledge, and the place of this criminal activity is limited to the data within the system, that is, those that are contained in the system and form part of it (قارة، 2001، ص 51-52).

**B- The second type: Intentional attack on the system's external data.** The Algerian legislature provided criminal protection for the data in and of itself by criminalizing the following behaviors:

1- The text of Article 394 bis 2 aims to protect data as such, because it is not required that it be within the automatic data processing system or that it has been processed automatically, The subject of the crime is the data, whether it is stored on tapes or disks, or that is processed automatically, or that is sent through an information system, as long as it may be used as a means to commit the crimes stipulated in Section Seven bis of the Penal Code.

2- The text of Article 394 bis 2/2 criminalizes acts of possession, disclosure, publication, use, whatever the purpose of these acts that are contained in the data obtained, from one of the crimes mentioned in Section Seven bis of the Penal Code, with the objectives of unfair competition, espionage Terrorism, incitement to immorality (فشار، 2009، ص 30-31)...

***Third - Intentional assault on the functioning of the automatic data processing system:***

It was stipulated in Articles 05 and 08 of the International Convention on Information Crime (اتفاقية بودابست، 2001). The Algerian legislator did not provide a provision for intentional attacks on the functioning of the system, and it was satisfied with the provision for the intentional attack on the data within the system, This may be explained by the fact that the abuse of data may affect the system's ability to perform its functions. This material behavior is

the act of stopping the automated data processing system from performing its normal activity(28 ص 2009، فشار،)، and what it is expected to do (such as introducing a virus program, or making the system slow down in its performance of its functions. .), And either in the act of spoiling the activity or functions of this system, and it is not required that the act of disrupting or the act of corruption occur on all the elements of the system altogether, rather it suffices that it affects only one of these elements, whether the physical, the computer itself, communication networks, and transport devices. As for the moral, such as programs and data (47 ص 2001، قارة).

***Fourth - Crimes developed under Law 16-02 supplementing the Penal Code:***

Certainly, criminal justice is clearly embodied when the penal policy aims to organize three sides: the prevention policy, the criminalization policy and the punishment policy. The first steps of the penal policy are criminalization, which is assumed to be a reflection of the social, political and economic reality within the state, It seems that crime with its methods is subject to development and growth, which requires the lawmaker to keep pace with this development in an attempt to confront it. Crime has taken on a global dimension by expanding its scope and introducing technology to its methods, and because crime fighting takes place at two levels: international and national, and it is certain that the issuance of Security Council resolutions similar to the resolution No. 1377 of 2001, and Resolution No. 2253 of 2015, associated with the development of terrorism crimes, had a legislative effect in Algeria, through the Algerian legislator's issuance of Law No. 02-16 on June 19, 2016, which complements Order No. 66-156 containing the Algerian Penal Code. By adding new articles, they are: 87 duplicate 11, 87 duplicate 12, and 394 duplicate 8.

This law also included strengthening the response to information crime due to its connection with the practice of many new crimes. In the year 2016, in the context of the legislator's adaptation and updating of the provisions of the law related to information and communication technology, its legislative system, especially those related to combating terrorism, which is also known to be a remarkable development as the perpetrators of this type of terrorism crimes are adopted. He denied carrying out his information and communication technology crimes, and this is in Articles 87 duplicate 11 and after,

This is through the criminalization of the act of transferring Algerians or foreigners residing in Algeria legally or illegally to another country to commit, incitement or training in terrorist acts using information and communication technology or any other means, and criminalizing acts of recruiting people for the benefit of associations, organizations, groups or organizations. This law criminalizes the phenomenon of combatants who move to other countries for the purpose of committing terrorist acts and prohibits the financing of these acts.

Whereas Article 394 duplicate 8 introduced under Amendment 16-02 includes the penalties imposed on the Internet service provider, who, despite being notified by the National Commission for the Prevention and Control of Crimes Related to Information and Communication Technology, does not perform an order or court ruling obligating him to intervene to withdraw or store the contents. Which allows access to it or makes access to it not possible when it constitutes crimes stipulated in the law, and the service provider is also punished if he fails to put in place technical arrangements that allow the withdrawal or storage of these contents.

***1.3 The moral element of the crime:***

Clarifying this element is considered one of the important matters in determining the nature of the behavior committed, and adapting it to determine the material texts that need to be applied, and the moral element in the various attacks affecting information systems takes the form of criminal intent in addition to the intention to cheat. Intentionally, where the moral element in it takes the form of criminal intent with its two components knowledge and will, as for the intention of fraud, it appears through fraud with which the entry is made from a breach of the

regulatory system that protects the system, as for survival, it is deduced from the operations that took place within the system(اقولوي ، 2015، ص10).

## ***2. the forms of penalties imposed for crimes affecting information and communication technology***

Given the seriousness of the information crime, the Algerian legislator decided on the appropriate penalties for it, whether committed by a natural person or by a legal person, and each of them is subject to the penalty set for it.

### ***2.1 penalties imposed on a natural person***

We will discuss the original penalties to which the natural person is exposed, as well as the complementary penalties.

**First - Principal penalties:** We will deal with the punishment of each crime separately.

\* The crime of unlawful entry and stay in the automated data processing system in its simple form, is stipulated in Article 394 duplicate of the Penal Code, whereby it is punishable by imprisonment from three months to a year, and a fine from 50,000 to 100,000 DZD.

\* As for the penalty for the aggravation of the crime of illegal entry and stay in the automatic data processing system, Article 394 duplicate paragraphs 2 and 3 stipulated that “the penalty shall be doubled if this results in the deletion or change of the organization’s data, and if the above-mentioned acts result in sabotaging the system’s operating system, the penalty shall be detention. From six months to two years, and the fine is from 50,000 to 150,000 dinars.

\* Deliberate assaults on data, the Algerian legislator stipulated in Article 394 duplicate 1 of the Penal Code “shall be punished with imprisonment from six months to three years and a fine from 500,000 to 2,000,000 dinars. The data it contains.

\* As for the punishment prescribed for the use of data in committing one of the crimes affecting the information systems, as well as the possession, disclosure, publication or use of data obtained from one of the crimes affecting the information systems, it is imprisonment from two months to three years and a fine from 1,000,000 to 5,000,000 Algerian dinars, according to Article 394 bis 2 from penal code.

\* The penalties for these crimes are doubled if the crime targets the national defense or the bodies and institutions subject to public law, according to Article 394 bis 3 of the penal code.

\* In the crimes created under Law 16-02 supplementing the penal code, Article 87 bis 11 dealt with temporary imprisonment from 05 to 10 years and a fine of 100,000 to 500 thousand inflicted on every Algerian or even a foreigner residing in Algeria in a legal or illegal manner who travels or He tries to travel to another country with the intention of committing, planning, preparing, or participating in terrorist acts, or training to commit them, or to receive training thereon, and he shall be punished with the same penalty: the one who commits these acts shall be punished with the same punishment, and whoever uses information and communication technology to commit these acts shall be punished with the same punishment. Imprisonment from 05 to 10 years and a fine of 100,000 to 500 thousand anyone who uses information and communication technology to recruit people for the benefit of a terrorist or an organization or an organized group whose purpose is the purpose of direct or indirect terrorist acts.

As for Article 394 duplicat 8, it punishes from one year to 03 years or a fine from 02 million to 10 million whoever provides services(الفانون 04-09، 2009) who do not perform, despite his excuses, by the National Commission for the Prevention and Control of Crimes Related to Information and Communication Technology, and the issuance of an order or judicial ruling obligating him to intervene to withdraw or Storing the contents that can be viewed or making access to them not possible when they constitute crimes stipulated in the law, and the service provider is also punished if he fails to put in place technical arrangements that allow the withdrawal or storage of such contents.

## **Second - Supplementary Punishments:**

Such penalties were stipulated in Article 394 bis 6 of the penal code: "While preserving the rights of bona fide third parties, it is ruled to confiscate the hardware, software and means used and close the sites that are the subject of a crime punishable according to this section, in addition to closing the shop or place of exploitation If the crime was committed with the knowledge of its owner. "

Confiscation: It is a complementary punishment that includes the hardware, software, and means used to commit a crime involving information systems, taking into account the rights of others in good faith.

Closing down sites: This is about the sites (les sites) that are the subject of a crime, one of the crimes affecting information systems.

- Close the shop or the place of exploitation: if the crime was committed with the knowledge of its owner, for example the closing of the electronic café from which such crimes are committed, provided that the knowledge elements are available to the owner(34 ص 2009، فشار).

## **2.2 penalties imposed on the legal person**

The penalties applied to the legal person when committing any of the crimes affecting information systems:

5 times the maximum fine determined for a natural person, and this is according to Article 394 bis 4 of the penal code, which states: "A legal person who commits one of the crimes stipulated in this section shall be punished with a fine equivalent to five (5) times the maximum fine prescribed for the person. Natural. "

## **3. Conclusion:**

By analyzing the elements of this intervention, we reached the following conclusions:

- The legislator considers the crimes of infringing information and communication technology a misdemeanor, and this is in Section Seven bis concerning crimes of infringing upon automatic data processing systems under Law No. 04-15 amending and supplementing the Penal Code, However, through Law No. 09-04, the legislator adopted a flexible standard for defining information crime in order to be able to accommodate electronic criminal activities that cannot be counted, while imposing these penalties on the natural and legal person while respecting the privacy of the latter.

- Keeping pace with international developments and the growing phenomenon of terrorism with its varied forms such as the recruitment of foreign fighters and financing terrorist activities, and the use of information and communication technology in this, which prompted the legislature to harmonize the legislative system with Security Council resolutions through Law 02-16 supplementing the penal code, which came with 03 Articles 87 duplicate 11 And 87 duplicate 12 and 394 duplicate 8.

Complementing these results, we came to the following conclusions:

- The need to keep pace with the enactment of new rules to combat crimes against information and communication technology, which take into account the special nature of these in light of the rapid development of the field of science and communication technologies, especially since the Algerian legislator knows a certain delay in the enactment of these laws, in contrast to the speed and development of these crimes

## **Referrals and references:**

### **• International laws and agreements**

- - اتفاقية بودابست الأولى لمكافحة الإجرام عبر الإنترنت المنعقدة في 2001/11/23، تحت إشراف المجلس الأوروبي.

### **• Law**

- - القانون 04-09 المؤرخ في 05/09/2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها
- **Journal Article**
- - محمد علي قطب ( دون س ن) الجرائم المعلوماتية وطرق مواجهتها، الاكاديمية الملكية للشرطة، وزارة الداخلية، بدون سنة النشر.
- - سميرة معاشي(2018) الجريمة المعلوماتية ادراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة المفكر، العدد 17. الجزائر.
- - جمال براهيمي(2016) مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، المجلد 2، العدد 2، الجزائر.
- **Seminar article**
- - رحيمة نميدلي(2017) خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، طرابلس، 24/25 مارس ، ليبيا.
- - عطاء الله فشار (2017) مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا.
- -اقلولي أولد رابح صافية (2015) الطبيعة القانونية للجريمة المعلوماتية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر، بسكرة، يومي 15 و16 نوفمبر ، الجزائر
- **scientific thesis**
- - أمال قارة (2001) الجريمة المعلوماتية، رسالة ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة بن عكنون، الجزائر