THE MECHANISMS AGAINST THE ELECTRONIC CRIMES IN THE ALGERIAN PENAL CODE

[1]DR. CHIKH MOHAMED ZAKARIA, [2]BENMELOUKA KAOUTHAR
[1]faculty of law and political science, university center of maghnia (Algeria)
email: zakaria.chikh@cumaghnia.dz
[2]Phd student at the faculty of law and political science, university of oran 2 Mohamed ben ahmed (Algeria)
email: kaouthar.1988@yahoo.fr

Abstract:
The spread of modem technology and its uses that affected all the life aspects brought about positive and negative changes and transformations. Undoubtedly, the information revolution and the high techniques it is based on such as the computers and internet left positive effects and made a giant leap for the people's and states' lives thanks to the speed and exactitude of these systems. Moreover, these systems allow for storing information and exchanging them easily. Nevertheless, this technology led to many negatives such as the difficulty of achieving the information security due to the easy access to them, and the violation of information and their freedom.

The technological advance and the spread of the modern communication tools brought about a new form of crimes called the electronic crime. Therefore, the Algerian Legislator intervened against it to provide penal protection for the information systems through making amendments on the penal code to make it respond to the criminal developments in the field of information and communication technologies ICT. Besides, He enacted new laws to guarantee the penal protection to the electronic transactions. In this context, our study shall focus on the protection imposed by the Algerian Legislator on the information systems in the penal code.

Based on what was said, we raise the following questions: What is meant by the electronic crime? What are the mechanisms set against it by the Algerian Legislator in the penal code? To what extent did the Legislator succeed in fighting the electronic crime with all its forms and, thus, providing an effective penal protection to the information systems? This shall be answered through defining the electronic crime and showing its characteristics in the first chapter, and then identifying the mechanisms set by the Algerian Legislator in the Algerian penal code in the second chapter.

Key words: *mechanisms, characteristics, communication, amendments, communication*

CHAPTER ONE: DEFINITION AND CHARACTERISTICS OF THE ELECTRONIC CRIME:

It is a modern crime linked to the information technology. Because it is modern, there are two trends that defined it. This crime has distinct characteristics that are not found in the conventional ones. Therefore, we have to tackle its definitions and then show its characteristics.

SECTION ONE: DEFINITION OF THE ELECTRONIC CRIME:

It is one of the modern aspects because it is linked to the modern ICTs and computer. Besides, because of the continuous development of the information technology IT, it is not easy to set a comprehensive jurisprudent definition. Hence, the jurisprudence was divided into two trends: one narrows the concept of this crime while the second widens it. In this regard, the narrower define it as any illicit act where a huge knowledge about computers and technologies is necessary for the commission and for the prosecution[1]. This definition hugely narrows the electronic crime as

[1] Goura Naila, economic crimes of the computer, Vol. 01, Arab Renaissance house, Cairo, 2004, p. 21.

it conditions the existence of big knowledge about the computers and technologies, not only for the commission of the crime, but also for its prosecution.

On the other hand, some jurisprudence defines it as any crime against money related to the automized processing of information[2]. Besides, it is an illicit act that aims at copying, having access to, modifying, or deleting information stored in a computer or transferred via it[3]. We notice that these definitions give a narrow concept for the electronic crime as they do not consider many illicit acts where the computer is used.

In the same line, the wideners define it as any act or deliberate refrain resulting from the illicit use for the IT to violate the material or moral funds[4]. Furthermore, experts of the Organization for Economic Cooperation and Development defined it in 1983 as any illicit, unethical, or undeclared behavior related to the automized processing or transfer of information[5]. Besides, some others define it any criminal behavior with the help of the computer[6]. Or, it is any crime made in the environment of computers. The 10th congress of the UN against the criminals held in Vienna 2000 defined it as any crime that can be perpetuated via a computer system or net and covers all the crimes that can be perpetuated in an electronic environment[7].

These wide definitions tried to cover as much as possible all the criminal forms of the electronic crime. Any criminal activity, be it positive or negative (refrain) where the computer system plays a role, or takes place in an electronic environment, is an electronic crime. This trend did not limit the electronic crime to a narrow range so that many perpetuators of such crimes do not avoid prosecution.

SECTION 02: CHARACTERISTICS OF THE ELECTRONIC CRIME:

The electronic crime is distinct than the conventional one in many points as follows.

PART 01: OCCURRENCE OF THE ELECTRONIC CRIME IN THE ENVIRONMENT OF AUTOMIZED PROCESSION OF INFORMATION:

The electronic crime takes place during the automized procession of the computer information and data. This system is the main condition for the investigation and prosecution of the electronic crime against the data procession system; otherwise, the crime is not electronic[8]. In this regard, it is necessary to have collected data to penetrate the cyber system and process them electronically to correct, modify, delete, store, restore, or print data. These processes are tightly linked to the crimes' commission. Thus, the criminal must understand them when perpetuating forgery or imitation activities[9].

[2] This definition is made by the German Tiedmemann, and is qtd in: Ahmed Khalifa al Malat, the information crimes, university thought house, Alexandria, p. 94.

[3] Qtd in : Nahla Abdel Kader al Moumni, the information crimes, Vol. 01, culture house for publication and distribution, Jordan, 2008, p. 48.

[4] Sami Al Shawa, the information revolution and its implications on the penal code, Vol. 01, Arab renaissance house, Cairo, 1994, p. 07.

[5] Qtd in : Nahla Abdel Kader al Moumni, op. cit., p. 49.

[6] Khaled Mahmoud Ibrahim, the information crimes, university thought house, Alexandria, 2009, p. 74.

[7] This congress was held in Vienna from 10 to 17 April 2000 ; Mahmoud Ibrahim al Ghazi, the penal protection to the electronic trade and privacy, Al Wafa legal library, Alexandria, Vol. 01, 201, p. 118.

[8] Khaled Mohamed Kadfour al Mhiri, the crimes of the computer, internet, and electronic trade, al Gharir house for publication and distribution, Dubai, 2005, p. 135.

[9] Ahmed Khalifa al Malat op. cit., p. 105.

PART 02: THE ELECTRONIC CRIME AS A TRANSFRONTIERS CRIME:

The electronic crimes have international aims in general because the international nature of the internet which connects the whole world facilitates the commission of the crimes. In this vein, the electronic crime does not recognize the states and continents as it is transcontinental. The information system makes it possible to commit many crimes such as the violation of databases, falsifying and deleting the electronic documents, cyber fraud, and piracy[10]. This transfrontiers nature of the cyber crime left many problems regarding the identification of the competent state on this crime, the law to be enforced, and other issues related to the judicial prosecution.

PART 03: THE DIFFICULTY OF PROVING THE ELECTRONIC CRIME:

The electronic crime is hard to figure out. Even when discovered and declared, it is hard to be evidenced as it takes place in an unconventional environment outside the tangible reality. This makes it more complicated for the security, investigation, and prosecution bodies. In this environment, the data and information are just invisible electronic pulses that move through the information system making it easy for the criminal to eradicate the evidence[11]. Besides, the difficulty of evidencing the electronic crime is due to the fact that:

-This crime does not leave material evidences as there are no blood traces or dead bodies. The crime can be discovered by chance[12].

-It is easy to delete the evidence from the computer in a short time using special software, and it is hard to find it.

-The policemen and the justice bodies lack the technical experience while the computer and internet crimes require a good mastery of the computer techniques and information systems so as to be able to prosecute the offenders[13].

PART 04: THE SPECIFICITY OF COMMITTING THE ELECTRONIC CRIME:

The electronic crime differs than the conventional one regarding the commission method or the persons. It is a crime that does not require violence or hurting as is the case in the murder and kidnapping crimes. The electronic crimes have a calm nature and need only simple clicks by the cyber criminals who are more intelligent and have higher technical competencies than the conventional criminal.

PART 05: THE WEAK REPORTING OF THE ELECTRONIC CRIMES:

Often, people do not report the internet crimes because of not discovering it or fearing the defamation. The companies and businesses refuse reporting to avoid the bad reputation and defamation[14].

CHAPTER 02: MECHANISMS AGAINST THE ELECTRONIC CRIME IN THE PENAL CODE:

The Algerian Legislator added to the penal code articles that criminalize the violations of information. This was through Law 04/15 on the amendment of the penal cede mainly after the high increase of the violations of the cyber systems due to the development of communication and the websites. The Algerian Legislator enacted by Law 04/15 of 10 November 2004 on the penal code[15] a chapter entitled “the violation of the systems of the automized data procession” that includes the crimes that violate the systems of the automized data procession as follows.

[10] Khaled Mahmoud Ibrahim, op. cit., p. 77.

[11] Nahla Abdel Kader al Moumni, op. cit., p. 56.

[12] Ahmed Khalifa al Malat op. cit., p. 105.

[13] Khaled Mahmoud Ibrahim, op. cit., p. 77.

[14] Saidi Salima, Hejaz Bilel, the crimes of information and nets in the digital era, Vol. 01, university thought house, Alexandria, 2017, p. 63.

[15] Official Gazette 71 of 2004.

SECTION 01: THE CRIME OF UNAUTHORIZED LOG IN AND STAY:

Article 394 Bis of the penal code provided for sanctioning with jail from 03 to 06 months and with a monetary fine, between 50000 and 100000 Algerian Dinar, anyone who logs in, stays, or attempts to, through fraud, in each part of the system of the automized data procession. The sanction is redoubled if the data of the system are deleted or modified. This Article shows that the unauthorized crime of logging in is illegal- fraud-. This is because of the absence of the legitimacy of the person who logs in the system while aware about this.

Among the cases of the unauthorized log in to the information system is the log in without the knowledge of the system owner. The doer may be authorized to log in a part of the system; but not all of it. If he logs in another part, he shall commit a crime. This type of crime is often committed by the employees of the companies that have an information system. The unauthorized log in may take place by any means. It may be with the real password, hacking software, or the code number of any authorized person through the phone or internet[16].

As for the crime of illegal stay inside the information system, it refers to the existence in the system despite the refusal of the authority. This takes place when the criminal finds himself by error or chance in the system and decides to stay and refuse to log out. This can happen when a person wants to log in a system that he is authorized to, but ends up finding himself in another due to a wrong code[17]. We notice that the Algerian Legislator criminalized the log in or the stay in the information system even if it does not harm the system. Besides, he tightened the sanction if the crime results in the deletion or modification of the data.

PART 02: THE CRIME OF VIOLATION OF DATA:

Article 394 Bis 1 of the penal code provides for jailing from 06 months to 03 years and with a monetary fine, between 500000 and 100000 Algerian Dinar, any person who fraudulently enters, deletes, or modifies data of a system. The Legislator limited the forms of data violation in entering new wrong data to the existing ones in the system, deleting existing data, and modifying the data and substituting them through specific software. Thus, any person who commits such acts is indicted with the crime of violation. It is a crime independent from the crimes of unauthorized log in and staying because the violation may happen online after logging in or staying in the system using virus software.

PART 03: DEALING WITH ILLICIT INFORMATION:

Article 394 Bis 2 of the same law provides for sanctioning with jail from 02 months to 03 years and with a monetary fine, between 100000 and 500000 Algerian Dinar, any person who deliberately or fraudulently makes the following:

- Designing, researching, collecting, providing, publishing, or trading stored, processed, or transferred information via an information system that may result in the previous crimes.
- Possessing, disclosing, publishing, or using the data for the crimes mentioned above.

This shows that the Legislator wants to maintain the secrecy of the information after he had criminalized the acts through which the information are obtained as mentioned in Articles 394 Bis and 394 Bis 2. These Articles provide that dealing with illicit information takes two forms. The first criminalizes dealing with information to commit crimes through designing, looking for how to design[18], collecting, providing[19], publishing so that others can have access to[20], and trading them. The second criminalizes the transactions with information, obtained by a crime, that include possessing, disclosing, publishing, or using them for any purpose.

[16] Aouda Youcef Suleiman, the crimes affecting the private life that take place through the modern information technology, p.10.

[17] Nahla Abdel Kader al Moumni, op. cit., p. 161.

[18] Such as designing software with a virus known as the malicious software.

[19] Through reference to software connected to another software that ruins the data for instance.

[20] This behavior includes a clear violation of the privacy.

Article 394 Bis 06 adds that in addition to the monetary fine and the jail, all the used devices, software, and tools shall be confiscated and the sites of the crime shall be deleted. Besides, the shop or the location shall be shut down if the crime is perpetuated with the knowledge of its owner.

CONCLUSION:

Upon this study, we showed that despite the positive sides of the information systems, there are negative ones resulting from the use of IT by criminals to facilitate their works. Besides, the information system became a subject for violation and misuse. Because the electronic crime is a modern criminal phenomenon that targets the information stored or processed in the system of the computer or exchanged via the nets, its distinct nature made it difficult to include it in the conventional descriptions of the national and international penal laws. Therefore, new laws are need against this crime.

In this regard, the Algerian Legislator made sure to keep up in pace with the technological revolution and included amendments on the penal code to make it respond to these developments. In this line, He enacted many laws to guarantee the penal protection to the electronic transactions. The last law was 18/07 in 2018 on the protection of the electronic transactions and the processed information of the personal nature in the context of respecting the private life of individuals. This legislative variation efficiently contributes to facing the electronic crimes in Algeria.

We must recognize the efforts of the Algerian Legislator against the electronic crimes which aim at keeping up in pace with the theoretical and scientific trends and simulating the technological advance. Nevertheless, the efforts are still not sufficient to achieve the information security due to the fast development of the electronic crime and its international and transfrontiers nature. Hence, it is necessary to consolidate the international cooperation judicially and procedurally against the electronic crimes and to study and follow the international news.

Based on what was said, we recommend the following points against the electronic crimes:

-It is necessary to consolidate the international cooperation judicially and procedurally against the electronic crimes and to study and follow the international news.

-It is necessary to have policemen specialized in electronic crimes and in dealing with the computers and the internet.

-It is necessary to train the security and justice men on the computers and internet in specialized training workshops.

-It is necessary to teach modules related to the legal protection of information and all what is related to the computer and the internet at the Faculty of Laws.

Bibliography:

[1] Ahmed Khalifa al Malat, the information crimes, university thought house, Alexandria.
[2] Khaled Mahmoud Ibrahim, the information crimes, university thought house, Alexandria, 2009.
[3] Khaled Mohamed Kadfour al Mhiri, the crimes of the computer, internet, and electronic trade, al Gharir house for publication and distribution, Dubai, 2005.
[4] Sami Al Shawa, the information revolution and its implications on the penal code, Vol. 01, Arab renaissance house, Cairo, 1994.
[5] Saidi Salima, Hejaz Bilel, the crimes of information and nets in the digital era, Vol. 01, university thought house, Alexandria, 2017, p. 63.
[6] Goura Naila, economic crimes of the computer, Vol. 01, Arab Renaissance house, Cairo, 2004.
[7] Aouda Youcef Suleiman, the crimes affecting the private life that take place through the modern information technology, p.10.
[8] Nahla Abdel Kader al Moumni, the cyber crimes, Vol. 01, culture house for publication and distribution, Jordan, 2008.