Legal rules for preventing and combating cyber crimes in Algerian legislation

Received: 19/05/2024; Accepted**:** 02/09/2024

Kamel BELLAROU *

University of Constantine 1, Algeria, bellaroukamel@gmail.com

Abstract

This study seeks to shed light on the legal mechanisms to prevent and combat cyber-crimes Of Technological development Supernatural that The entire world has known it, especially the enormous information wealth and economic liberation in the context of globalization, the widespread spread of electronic networks and the emergence of modern means of technology and communication that have imposed themselves in all aspects of life. This development has been accompanied by the emergence of new types of innovative crime that differ in terms of their nature and their perpetrators. And the methods of committing them compared to traditional crimes,a resultano The widespread use of the World Wide Web, which allowed individuals to exchange and circulate information And follow digitization systems in all fields Without knowing any spatial or temporal limits, which resulted in compromising the interests of individuals, institutions, and basic interests protected by law.
And we aim for This study sheds light on information crime to identify it and explain its legal framework, in addition to examining the legal mechanisms to combat information crime at the level. The shop And international.

Keywords

New crime;
Virtual environment;
Systems Digitization;
Prevention and control rules;
cyber crime.

القواعد القانونية للوقاية من الجرائم السيبيرانية ومكافحتها في التشريع الجزائري

ملخص

تسعى هذه الدراسة إلى تسليط الضوء على الآليات القانونية للوقاية من الجرائم السبيرانية ومكافحتها نظرا للتطور التكنولوجي الخارق الذي عرفه العالم بأسره لاسيما الثروة المعلوماتية الهائلة و التحرر الاقتصادي في إطار العولمة، إلى انتشار واسع للشبكات الالكترونية و بروز وسائل التكنولوجيا و الاتصال الحديثة التي فرضت نفسها في جميع مناحي الحياة، و صاحب هذا التطور ظهور أنماط جديدة من الإجرام المستحدث تختلف من حيث طبيعتها و مرتكبيها و أساليب ارتكابها عن الجرائم التقليدية، نتيجة الاستخدام الواسع للشبكة العنكبوتية التي أتاحت للأفراد تبادل و تداول المعلومات وإتباع انظمة الرقمنة في جميع المجالات دون أن تعرف حدودا مكانية أو زمانية ، و هو ما انجر عنه المساس بمصالح الأفراد و المؤسسات و مصالح أساسية محمية قانونا ، ونهدف من هذه الدراسة تسليط الضوء على الجريمة المعلوماتية للتعرف عليها وبيان إطارها القانوني، بالإضافة التعرض بالدراسة إلى الآليات القانونية لمكافحة الجريمة المعلوماتية على المستوى المحلي والدولي.

الكلمات المفتاحية

الإجرام المستحدث ؛
البيئة الافتراضية ؛
الأنظمة الرقمنة ؛
قواعد الوقاية والمكافحة ؛
الجريمة السيبيرانية .

* *Corresponding author.E-mail: bellaroukamel@mail.com*
Doi: https://doi.org/10.34174/0079-035-004-013

I- Introduction :

tomay beIt was shortened aFor technology AModernThe distance between peoples, so the world became a small village and thus eliminated the difficulty of human communication between peopleIndividuals, given whatto attestHThe modern erafromSignificant development in means of communication and informationIn preparation for what became known as the era of globalizationWith these devices being connected to the Internet, which covers most regions of the globe, It has become very easy for even ordinary people who have no experience in this field to use these technologies.

FThe technological and information revolution and tremendous scientific progress In light of the political, economic, social and even legal transformations that the world witnessed and their repercussions on interactions between people, which led to the expansion of the circle of various transactions and actions, the transition from the real world to the virtual or informational world, and the emergence of the state.DigitizationChanging the pattern of transactions and actions from the traditional style to electronic transactions and actions. This is what made technology occupy a special place in people's lives and interactions, such that technology such as computers, mobile phones, etc. became widely used..

thatThe widespread use of information technology, modern technology, the Internet, and computers has created a type of non-traditional crime, which is called crime.Informatics orModernorTechnology crimesorCyberneticism, which came as a result of scientific and technological progress.

The importance of this study lies in identifying the seriousness and effects of these new crimesIt threatens the stability of societies as a result of violating and violating the rights of individuals and states, and it also constitutes a threatonIts legal security is that it is new crimes of a different legal nature that go beyond the traditional legal protection stipulated in internal legislation. This is what prompted countries to search for new and innovative mechanisms and tools in an effort to keep pace with this technological development, and this is through updating their legislation to be able to confront this technological revolution and its repercussions on people's rights. Especially electronic crime, which is considered the most dangerous and most widespread among countries, as it has a specificity that distinguishes it from other crimes, and this is what made it a subject of interest and research by scholars of jurisprudence, law, internal legislation, and international agreements.

On this basis, he hastenedaFor a legislatorAlgerian stylerestLegislationOther modern approaches require setting rules and mechanisms Legal of Okay aTo combat electronic crimeIn line withKeeping pace with technological development.

The aim of this study is to clarify the nature of information crimetheCybernetics and its legal natureLegal mechanisms to combat cybercrime in Algerian law

This is what prompts us to raise the following main questions:

How adequate are the legal mechanisms to combat crime?CyberneticsIn Algerian legislation?

This problem includes several sub-questions:

The nature of the crimeSpeeronic?whatsheThe legal nature of the crimeSpeeronic? What are the mechanisms?And the rulesLegal to combat crimeSpeeronicIn Algerian law?

In order to answer this main problem, we have relied on the analytical approach as we are analyzing new legal texts related to the subject of the study, as well as the comparative approach when comparing the legal texts regulating some old and new bodies.

Accordingly, we will try to answer the problem by studying the frameworktheConceptual and legal crimeCyberneticsinthe hubthe first,As for AFor an axisthe secondWe will devote it to demonstrationtherulesLegal to prevent and combat electronic crimeGet lostintheAlgerian legislation.

We ended our study with a conclusion in which we discussed the most important results reached through this modest study and suggestions

II– The concept and elements of cyber crime

We will eat Through this the hub development Concept Cyber-crime Then explain its pillars.

II.1– The concept of crime Cyber netics

We will address it firstThe development of the concept of crimecybernetics orInformatics due to its association with the development of the computerAnd alsoBased on the difference in its features.

II.1.1- The development of the concept of crime Cybernetics Due to the development of the computer

Coinciding with the development of the electronic computer industry, where the previously used mechanical method became incapable of performing advanced operations, therefore this device was developed, which included changing the central processing unit and memory.[1].

As a later stage, industry was reached A computer that is compatible with technological development, accompanied by the emergence of giant companies specialized in the field of these industries that dazzled the world with the information technologies they provided, as they witnessed amazing development and intense competition between them.[2]

II.1.2- Definition of crime aFor cyberneticismBased on the difference in its features

The jurist Mirao knew herMerew is the criminal act that uses the computer as the main tool, or it is the various forms of criminal behavior that are committed using automated data processing.[3]

As the jurist Parker knew itParker means that it is every illegal act for which knowledge of automated technology to a great extent is necessary to commit it on the one hand and to pursue and achieve it on the other hand.[4]

However, a trend in jurisprudence gave information crime a broad meaning to include all forms of illegal behavior or action committed by means of a computer.[5]

While some jurisprudence considers that the definition adopted by the United Nations at its Tenth Crime Prevention Conference on Computer Crimes and Networks, which was held in Vienna on April 10, 17, 2000, can be considered as a definitional summary of the above, as it defined it as “a crime that can be committed by means of a computer system or computer network.” Or within a computer system and includes, in principle, all crimes that can be committed in an electronic environment.”[6]

Accordingly, although a comprehensive and comprehensive definition of the concept of information crime has not been reached, the agreement is that it is every illegal act that aims to change data or information, whatever this change may be, whether it is by means of a computer, or it may be by using another technological device, and this suggests A new problem.

Confining information crime to the computer was not, until recently, a subject of jurisprudential controversy in light of the development of this device, but with the intervention of other devices resulting from this sweeping technological and technical development, it emphasized the necessity of information crime to include everything related to the illegal use of any technological means transmitting information and not Confined to the computer.

II.1.3- Definition of crime SpeeronicFocusing on its topic

Much of jurisprudence has focused on the subject of crimeCybernetics (informatics)Without focusing on the tool used for this, such as these juristsRosamblatt, where he considered computer crime to be an illegal activity directed at copying, changing, deleting, or... Access to information stored within the computer or Which is through him.

II.2- Elements of the crimeSpeeronic

In addition to the legal, material and moral pillaryEvery crime has it, but information crime requires an additional element, which is the hypothetical or assumed element.

II.2.1- The default element of the crimeSpeeronic

To provide an information crimeIt does not require the presence of an automated data processing system, so we will discuss...toThe concept of this system, focusing on its definition and the technical protection of the information system as a condition for criminal liability.

-Definition of an automated data processing system

Some jurisprudence has defined it as a mechanism and organized procedures that allow the collection, classification, and sorting of data, processing it, and then transforming it into information that a person retrieves when needed to enable him to accomplish a job, make a decision, or perform any function through the knowledge that he obtains from the information retrieved from it. This system .[7]

Many jurisprudents considered that reference is made to the relationship of this part to the system, if it is independent from it, and from it we are not faced with an information crime if individual elements are attacked, as is the case in the case of attacks on programs offered for sale, or computer devices that have not been put into service or in service. A trial case, or those information systems that have gone out of service[8].

The Algerian legislator, by amending the Penal Code of 2004 and adding it to Section 7 bis, entitled "Infringement of automated data processing systems," did not do so.[9]When he stipulated the type of crimes with the task of defining, he left that to jurisprudence and jurisprudence, reviewing the images of attacks on this regime, drawing on the experience of his French counterpart, who also did not undertake this task, after it was abandoned by the National Assembly, which completely rejected and dropped the Senate's proposal. On the occasion of the amendment to the French Penal Code, it was one of the preparatory works that defined this system.[10]

Returning to the definition proposed by the French Senate, it includes specific areas, as it considered that an automated data processing system is "every complex consisting of a unit or group of processing units, each of which consists of memory, programs, data, input and output devices, and linking devices that connect them." A set of relationships through which a specific result is achieved, which is data processing, provided that this component is subject to technical protection."[11]

It is noted that this definition is more precise and comprehensive than the previous definition, and in addition to specifying the data elements precisely, it stipulates that the necessary technical protection for this data be available, otherwise it is no longer an information crime.

Therefore, it is possible that the legislator's inclusion of the idea of definition in the first place is a violation of the concept of the system itself, since this system is in continuous development due to its connection to purely technical elements, and therefore leaving the task of defining jurisprudence and the judiciary is an idea worthy of attention, and some jurisprudence sees it.[12]

-Technical protection of the information system as a condition for criminal liability

Legal jurisprudence has differed in the extent to which security protection for the automated data processing system is considered a necessary condition for this system to receive criminal protection or not. Part of French jurisprudence considered not requiring the availability of technical protection for the information system for an information crime to occur.[13]This is due to the fact that the technical or technical security and protection system does not

It has only a positive role, and proof of the bad faith of the violator of this system and his entry into it illegally is basically available.[14].

While another trend of jurisprudence that adheres to the necessity of having an adequate scope of security protection for the various information systems processed automatically, divided the latter into 03 categories:

- Systems open to the public.
- Systems that are limited to those who have the right to them, but without technical protection.
- Systems that are limited to those who have the right to them, while providing technical protection for them.

This jurisprudence considered that the last type of information systems is the one that enjoys criminal protection, and their argument for that is that criminal protection should be limited to technically protected systems, because it is natural for anyone to exploit them, so the criminal law only protects people who have the keenness to on their money and with the provision of security protection, even to a minimal extent[15].

II.2.2- General elements of crimeCybernetics

Subject to crimetheThe legal, material and moral pillar.

- The legal element of the crimeCybernetics:

The lawmaker mediates to criminalize destructive acts agreeing to a legitimate content that indicates the destructive or criminal act and the punishment endorsed for its commission. The Algerian administrator given a extraordinary area to influence mechanized information handling frameworks, which is the seventh segment, bis, with the substance of Article 394 bis to 394. bis 7 compatible to Law No:04-15 dated November 10, 2004 The Algerian administrator was not substance with forcing criminal assurance on the private lives of people through Law No. 06-23 of December 20, 2006, which influenced Article 303 and its endorsement of Article 303 bis 3. Usually in reaction to the terrible utilize of present day innovation implies, this implies that the administrator stipulated the criminalization of The act committed "There is no wrongdoing, no punishment, or security measures but by a stipulation.

The French lawmaker isolated the violations of assaulting the mechanized information preparing framework from the violations of fashioning and utilizing mechanized information handling archives, as well as criminalizing all assaults on the computerized preparing framework and utilizing them.

After the default and fundamental condition for data wrongdoing is met, which is the computerized information preparing framework, its lawful column shows up, which is the nearness of legitimate writings that go up against the crawl seen by the violations that have influenced the Web and the assaults that included the protection of people and bodies, as most national enactment turn to forcing its censorship. And criminalizing different angles of data wrongdoing.

Whereas in Algeria, the lawmaker stipulated the battle against data wrongdoings by revising the Correctional Code of 2004, and including it to Area 7 bis beneath the title “Abusing mechanized information handling systems.”"These programmed frameworks are utilized in donnes",.

It is famous that The subject of data cash and its security is the subject of these writings, which is what legal law and law have set up on the need of considering the security of robotized information handling frameworks a authoritative need within the larger part of nations.

It ought to be famous that a difference emerged over the integration of the unused legitimate writings related to cybercrime into the Corrective Code or into a extraordinary law. A few showed up to coordinated them into cash wrongdoings, considering that it is conceivable to grant the character of cash to the physical and ethical substances of the computer, whereas others favored to coordinated them inside the system of the portion related to wrongdoings. Against proprietorship, considering that the physical substance of the computer is fabric components that can be claimed, fair as the ethical substance falls inside the system of mental property. There are those who see including another portion to data wrongdoings free of the conventional parts, considering that these wrongdoings are related to a unused financial esteem that encompasses a extraordinary character. The third slant accepts that it is fundamental to add Each data wrongdoing has its comparable within the traditional penal code, such as: setting the wrongdoing of data imitation within the area on archives, ambushing information coming about in destruction...etc. [16].

-The physical element of information crime

Law specialists characterized it as each act that comes about within the mechanized information preparing framework halting its ordinary execution. In spite of the jurisprudential discussion that went with the concept of the data framework, whether or not it incorporates most of its components, the lion's share of jurisprudence believes that it isn't vital to stipulate that the act of disturbance or harm to the framework happen as a entire. Or maybe, it is adequate for it to influence as it were one of its components, such as the computer itself or amplifying to communication systems or programs and information. [17]

In like manner, we are confronted with the fabric component of an data wrongdoing in case the framework for mechanized data handling or its judgment is assaulted, as we are within the case of unlawful section and remain in this framework or cancellation or alter or information, and attack or any harm to the working framework can be considered physical assaults (Article 394 bis QAA C).

All of these pictures were included by the Algerian lawmaker through the corrected Correctional Code of 2004, and numerous physical pictures were included to them adequate to set up the fabric component of the data wrongdoing, such as entering data into the mechanized preparing framework or evacuating it (Article 394 bis).

F) The material component is the activities and behaviors issued by a sound individual and his information of the starting of the movement, starting it, and accomplishing a result. Preliminary work in conventional wrongdoing isn't culpable by law, not at all like electronic wrongdoing, where the matter is diverse. Obtaining creative programs, interpreting hardware, and passwords, or having pictures of child prostitution could be a wrongdoing in itself without entering. Within the action of committing a wrongdoing, the act of committing a positive activity or going without from a negative act causes a result, which is the hurt of a protected or legitimate right. In cybercrime moreover, there must be a physical act, and the nearness of the advanced environment and the Web must happen, and the information that he has started to commit the act and will orchestrate a result on the off chance that vital. Accessibility:

- **Material behavior**: There's no discipline for the considerations, creative ability, and contemplations that run through the individual's soul unless there's positive fabric behavior by performing the act and going without from it, which decides the wrongdoing of the act. In cybercrime, the computerized environment must be show, which is the scene and apparatus of the wrongdoing, and the Web must be display.

-Direct technical activity: Physical behavior alone isn't adequate for the presence of cybercrime. A specialized movement must be attempted with illicit section into a processing framework or information bases. As before long as there's section into the framework, it is considered criminal behavior indeed in case the frameworks and information were not compromised. The action he carried out by utilizing the computer and getting to the Web. It constitutes an action or portion

of it, and observing this get to is considered a wrongdoing. Criminal movement incorporates getting to private correspondence and email or giving untrue information.[18].

-The moral element of information crime

The nearness of the ethical component of any wrongdoing is considered a vital component for the foundation of criminal obligation, which is criminal aim. Be that as it may, due to the specificity of data wrongdoings, statute has dug into the specificity of each wrongdoing independently; in arrange to discover the nearness of this component or not, whereas a few other law has proposed the plausibility of isolating criminal aim. The private versus the open for these wrongdoings.

A drift of statute accepts that the American legal has not settled on a few violations committed utilizing the Internet,In terms of the degree to which it is decided whether it requires common or particular expectation, particular expectation is show in a few data wrongdoings, particularly since data violations are based on the nearness of common expectation, that's , the offender's information of the substance of his act that he is committing an unlawful act, and the association of this information to the will.[19] An illustration of usually what the French Court of Cassation ruled with respect to the presence of the purposeful of transitory ownership within the wrongdoing of taking data from a computer. What is adequate for this deliberate to be confirmed is the robbery and ownership of archives amid a certain time without the will of their legitimate proprietor or holder of them forever or incidentally, that's , the nearness of the deliberate to take part in Advantage from it. [20]

The same applies to the wrongdoing of data imitation, with the culprit having an extra deliberate to utilize the manufactured report, but it was not really utilized. Within the final case, we are confronted with a probabilistic deliberate upon information of the plausibility of causing hurt. [21]

All of this brings us to a circumstance where it is troublesome to demonstrate particular criminal aim, and hence the trouble of demonstrating the ethical component of an data wrongdoing, which is one of the foremost vital characteristics.associated with this wrongdoing.

III-the rules Legal crime prevention Informatics And combat it.

Combating this sort of wrongdoing requires upgrading corrective enactment, particularly since this sort of wrongdoing is reasonably later, because it showed up with innovative improvement and the development of what is known as the world of data and digitization. Undoubtedly, this sort of wrongdoing, given its specificity of being wrongdoings that cross universal borders, influence all parts of the world and cause genuine harm to them,[22].

Combating and standing up to it requires worldwide participation and concerted worldwide and territorial universal endeavors in arrange to stand up to it, and typically what we'll attempt to get it through this article. The hub is as takes after:

III.1 -Provisions Legal National Crime Prevention Cybernetics And combat it

The Algerian legislator has considered computer programs as a written literary work that is legally protected under Law 03-05 relating to copyright and related rights through the text of Article 04, and even stipulated penal provisions regarding the misdemeanor of counterfeiting and the penalties prescribed for it under Articles 151 to 160 of the same law as its direction. To confront this type of crime, which is characterized by informational or electronic specificity, he has proposed a set of special rules to prevent crimes related to information and communication technology on the one hand, and he has made a set of amendments to the general rules for preventing and combating crimes, and this is what we will try to clarify during this requirement:

III.1.1- Modify the rulesSubstantive and procedural To prevent crimes Cybernetics And combat it

In arrange to stand up to this sort of wrongdoing, the lawmaker worked to bring almost a bunch of alterations to obstacle laws, the foremost critical of which are the Corrective Code and the Code of Criminal Strategy, in this way making up for the legitimate vacuum that they were carrying.

- In terms of substantive rules: A uncommon area related to robotized information preparing frameworks was included beneath Law No. 04-15 of November 10, 2004. At that point revisions taken after and a few criminal behaviors related to that were included beneath Law No. 06-23 of December 20, 2006, counting entering and remaining through extortion in all or portion of the framework. For mechanized handling of information, or false section of information into an robotized handling framework, or false expulsion or adjustment of a few information, or within the case of planning, inquiring

about, collecting, giving, distributing, or exchanging in information put away, prepared, or sent through an data framework or ownership. Or disclosing, distributing, or utilizing data fraudulently. The penalty is additionally expanded within the occasion of erasing or changing information, or subverting a system.WorkThe framework. [23]

It is throughinductionTexts of Articles of Law 04-15 We discover that, through Article 394 bis, the lawmaker has considered expelling or adjusting information contained within the framework by extortion a criminal act and has stipulated a punishment of three months to one year detainment for the culprits, in expansion to a fine of 50,000 DZD to 100,000 DZD, and the punishment will be doubled if This come about within the cancellation or alter of framework information. Be that as it may, in the event that the previously mentioned activities result in disrupting the system's working framework, the punishment should be detainment from six months to two a long time and a fine from 50,000 DZD to 150,000 DZD. [24]

Anybody who falsely enters information into the robotized preparing framework or falsely evacuates or modifies the information it contains should be rebuffed with detainment from six months to three a long time and a fine evaluated at 500,000 DZD to 2,000,000 DZD. [25]

The legislator-commission made this a crime.Any plan, investigate, compilation, arrangement, distribution, exchange in put away information, preparing, or correspondence through an data framework seem, in the event that done with aim and misdirection, commit the same, in case not more, of the violations recorded within the Corrective Code's segment on causing hurt to mechanized information handling frameworks. The wrongdoers confront fines extending from 1,000,000 to 5,000,000 DZD in expansion to terms of detainment extending from two months to three a long time. [26]

The punishments for culprits of the previously mentioned wrongdoings might be multiplied on the off chance that the wrongdoing targets national defense or bodies or teach subject to open law, without preference to the application of more extreme punishments. [27]

In expansion, it is through modification06/23Regarding the Corrective Code, we discover that the lawmaker has proceeded to proposed to combat this sort of wrongdoing by criminalizing acts that abuse the sanctity of private life, because it shows up from the content of Article 303 bis that it is culpable by detainment from six months to three a long time and a fine evaluated at 50,000 to 300,000 DZD. Anybody who intentioned abuses the sacredness of people's private lives, by any innovation, by capturing, recording, or transmitting private or secret calls or discussions without the consent or assent of their proprietor, or by taking or recording a picture of a individual in a private put without the consent or assent of their proprietor. [28]

B/ **in terms of Procedural rules:** The administrator has apportioned this sort of wrongdoing to a set of uncommon strategies, maybe the foremost unmistakable of which is amplifying nearby locale to each of the legal police officers, the exploring judge, and the open prosecutor when it comes to organized wrongdoing, wrongdoings of mechanized information handling, fear mongering, cash washing, and trade wrongdoings, and maybe receiving territorial ward. The scope is to successfully stand up to a extend of genuine organized wrongdoings that are complex, indeed if they veer off from the initial jurisdictional criteria.[29]

In expansion to this strategy, the Algerian administrator has presented a set of extraordinary strategies that are congruous with the virtual world, which incorporate capture attempt correspondence, taking pictures, and recording votes, andaAs a result of the spill, the Algerian lawmaker permitted such methods for the necessities of examination and examination and solely for particular wrongdoings, counting wrongdoings related to robotized information preparing frameworks. Particular legitimate conditions must be taken into consideration, specifically authorization, the nature of the wrongdoing, and the privacy of proficient privileged insights. A report should be drawn up by the legal police officer authorized to carry out the operation. [30]

III.1.2- Special rules for crime prevention Informatics And combat it

We discover that the Algerian lawmaker has tended to the issue of anticipation and security from electronic violations in numerous uncommon writings, maybe the foremost conspicuous of which is the Law on the Anticipation and Combat of Violations Related to Data and Communication Innovation (09/04), as well as the Law on Scholarly and Imaginative Property (03/05) and the writings Related to electronic signature, security from such crimes moreover shows up within the law relating to mail, broadcast communications, etc., and other extraordinary laws that expressly or certainly address security from hones related to electronic or cybercrime, in any case of their names.

Arrange 03/05 with respect to copyright and related rights extended the list of secured works by consolidating data programs into the initial works, which were communicated in database works and data programs. It moreover fixed the punishments for damaging authors' rights, particularly advanced works secured by security. [31]

The Algerian lawmaker issued Law 03/15 related to the modernization of equity. Within the moment chapter, it tended to the central data framework of the Service of Equity and the certification of the genuineness of electronic

documents. It too tended to, within the fifth chapter, the corrective arrangements for securing electronic marks and verification, as Article 17 It rebuffs anybody who illicitly employments individual components related to making an electronic signature related to the signature of another individual, and Article 18 rebuffs anybody who holds an electronic certificate and employments it after it has lapsed or been cancelled.[32]

As for the law 09/04 It is the law directing spaceAl-SiberianIn common, combating the related criminal field through rules that permit for the follow-up of this sort of wrongdoing and its culprits in a way that ensures the authenticity of the measures taken., whereThe law comprises of six chapters that incorporate the definition of electronic wrongdoing, which does not contrast significantly from its definition inside the Corrective Code. It moreover incorporates procedural rules for reviewing the data framework, in expansion to building up the National Specialist for the Avoidance and Combat of Wrongdoings Related to Data and Communication Innovation in agreement with the content of Article 13 of it: A national body for the anticipation of related wrongdoings should be built up Data and communication innovation decides the composition of the body, its organization, and how it works through control.[33]

The control was issued in 2019, which is Presidential Declare 19/172 of June 6, 2019, which decides the composition of the National Specialist for the Anticipation of Wrongdoings Related to Media Innovation andConnectionAnd combating it, organizing it, and how it works,The to begin with article stipulates the foundation of this body, whereas the moment article stipulates:(The body could be a open institution of an authoritative nature, invested with lawful identity and money related freedom, and put beneath the specialist of the Service of National Defense).[34]

This specialist attempts the errand of preventive observing of communications inside the system of avoiding violations depicted as fear based oppressor acts and assaults on state security. It moreover does not work in segregation from major government goals. The administrator has relegated this specialist numerous powers that concern the method of examining wrongdoings that influence the security of the nation. The state is like secret activities and tall treachery utilizing electronic implies.

The specialist is composed of a controlling board and a common directorate. [35] The Controlling Board is chaired by the Serve of Defense National ismIt comprises of the taking after services: The Service of National Defense ,Service of CountstoThe Service in charge of the Insides, the Service in chargeCommunicationsWired and remote. This body is additionally given with a common secretariat put beneath the specialist of the Service of National Defense,This body works to implementstrategyEffective in anticipating and combating crimesRelatedWith media innovation andConnectionBy giving its Common Directorate with a set of powers, counting planning the Authority's budget, enacting, planning, taking after up and observing the exercises of the Authority's structures, and preparingMeetingsGuidance Board in expansion to preparingMeetingsThe Controlling Chamber, in expansion to planning yearly reports on the Authority's movement.

At last, we note that the lawmaker has attempted to accommodate the part of the specialist with its powersrespectThe private life of people, because it expressly stipulates that the Specialist helps the legal police offices in understanding with what is stipulated within the Code of Criminal Strategy and is authorized by the Open Prosecutor and obligating the legal police officers and officers and the individuals of the Specialist carrying out the strategy to stay professionally secret.[36]

In arrange to combat cybercrimes, the Algerian administrator set up specialized corrective shafts and a national correctional post to combat violations related to data and communication advances in agreement with Arrange 21/11 revising and supplementing the Code of Criminal Strategy (Article 211 bis 02 thereof).

III.2- International efforts to combat crime Cybernetics

This wrongdoing is characterized by its worldwide character and its amazing quality of the borders of a single nation. Undoubtedly, commonsense reality has demonstrated that it isn't conceivable to stand up to it with the endeavors of person nations. Or maybe, the circumstance requires the escalated of a gather of international efforts, and usually what was deciphered by the work of the Joined together Countries and the Worldwide Media transmission Union, as well as the endeavors of the Universal Criminal Police Organization, Interpol, and In expansion to a few territorial endeavors, such as the Middle easterner Assention to Combat Data Innovation Violations, the endeavors of the European Union, and the endeavors of the African Union,We will clarify this as takes after:

III.2.1-United Nations efforts to combat crime Cybernetics

The organization has held a few conferences within the setting of confronting information wrongdoing, and usually apparent through the twelfth conference from April 12 to 19, 2010 in Brazil beneath the title "Comprehensive Procedures for Worldwide Challenges," organized to avoid wrongdoing and accomplish criminal equity and its improvement in a changing world. The conference procedures included eight things: among them cybercrime, where the Wrongdoing Avoidance and Criminal Equity Committee called for a assembly of a group comprising of government specialists, which is an open-ended universal assembly to comprehensively ponder the issue of cybercrime and measures to address it.

The organization too held the Thirteenth Congress on Wrongdoing Avoidance and Criminal Equity from April 12 to 15, 2015 in Qatar.[37] The most topic of the conference was "Integrating wrongdoing anticipation and criminal equity into the broader Joined together Countries plan to address social and financial challenges and fortify the run the show of law at the national and universal levels, and open participation." The Common Get together, in its determination (67/184), chosen to consider the taking after:

Building up workshops, counting fortifying wrongdoing anticipation and criminal equity measures, to address advancing shapes of wrongdoing, counting cybercrime.

The organization's endeavors were deciphered into issuing numerous resolutions and suggestions, counting: Determination (45/121) of 1990, as well as the distribution of a direct to avoiding and combating wrongdoings related to computers in 1994.

III.2.2- Efforts of the International Criminal Police Organization Interpol

The organization's goal is to create and encourage cooperation between police agencies in member states in an effective manner in combating crime, through the national central offices of the International Police located in the territory of some countries and exchanging them among themselves, in addition to cooperation in arresting criminals with the help of police agencies. The police in member states and provide them with the information available to them on their territories, especially in cases such as cybercrimes, as the Internet facilitates their passage across countries.

III.2.3- Efforts of some regional organizations

A special force was established to combat cybercrimes in the European Union countries on September 1, 2014, by Europol, the European law enforcement agency that specializes in fighting crimes and terrorism in EU member states. As part of the European Council's efforts, this force also works in other EU member states. Since 1976, computer crimes have spread internationally, and in 1996, the European Committee on Crime Problems formed an expert committee to address cybercrime.[38]

As for the African level, we find that the African Union has requested an extraordinary conference of the Union Ministry responsible for information and communications technology, held in South Africa from 02 to 05 November 2009, for the African Union Commission to jointly prepare with the United Nations Economic Commission for Africa an agreement on judicial legislation based on the needs of the African Union. The continent and compliance with the legal and regulatory requirements for electronic transactions, electronic security and personal data protection. In June 2014, the leaders of the African Union, consisting of 54 African governments, met at the 23rd summit of the African Union, and agreed to the African Union Agreement regarding the field of cybersecurity and personal data protection.

IV- Conclusion:

You will be saved at the end of thisthe studytoSaying thatthe crimecybernetics orElectronic crime is one of the new crimesWhich was the resultTechnological and scientific development, As you promiseOne of the most difficult challenges of modern technology today is that it is linked to information systems that are easy to obtain and use, such as computers. However, jurisprudential concepts differed and were divided over the concept ofHa, between its narrowing and expanding directionHowever, the computer is its basis.

As TDiversity andTMultipleFor reasonsAnd the motives for committing it are as followsExcellenceWith a set of characteristics that differ from the characteristics of traditional crimes and differencescharacteristicsThe electronic offender is different from other traditional criminals,It is also considered a stand-alone crime that requires the fulfillment of its three legal, moral and material elements.

It also has many forms that differ according to the field and target group, and this is what Making its legal nature different from other traditional crimes and more dangerous, whether for individuals or the stateAnd even on its legal securityThis

is what prompted the Algerian legislator to address it by amending laws in an effort to create...Mechanisms and rulesTo combat and prevent electronic crimeWithin the rulesPublic and private law reflects the extent to which laws keep pace with the technological development taking place. This is evident in its amendment to the Algerian Penal Code No. 04/15 and the issuance of Law No. 09/04.under which it was establishedA national body for the prevention of crimes related to information and communication technologyAnd the establishment of specialized penal poles and a national pole.

The state cannot confront such challenges aloneIn isolation from this other worldOn the one hand, and the international nature of cybercrime on the otheraAnother,Therefore, international efforts must be intensifiedAnd regionalContinental and global in order to confront thisTechnological developmentsWhich harms its various interests, especially financial and economicKUnited Nations effortsAndInternational Criminal Police OrganizationaNetball.

ButDespite the Algerian legislator's attempt to confront this new crime and create a legislative and institutional system, this phenomenon is spreading horribly, which confirms the relativity of these challenges.Legalresulting from this technological development and thisWhat makes us say thatLegislative textsNot enough forKeeping up with technological challenges.

Therefore, for the sake of protectionEffective He meantConfronting crimescybernetics orInformaticscan be suggestedRecommendationsnext:

_It is necessary to define a comprehensive and unified concept of electronic crimeOr cybercrime so as not to violate the principle of legality.

_ Enacting a special law in which legal texts were collected to prevent and combat cybercrimes, as was done with the crimes of speculation, narcotics, psychotropic substances, and forgery. This is in view of the seriousness of cybercrimes and the effects resulting from them intentionally. MGo aheadHModern technological challengesoccurring in various fields.

_thEffective search and investigation rules that keep pace with the techniques used in the commission and location of crimese.

-Using advanced means, information systems, and modern technologyAnd digitization.

_Improving and training users, law, judiciary and security personnel in the field of electronic control and prevention of information technology risks.

_Activating the role of civil society in the awareness-raising processAnd awarenessAbout the risks of using information technology and electronic transactions.

_YCare must be taken of the human element specialized in combating these crimes, whether in terms of training or in terms of follow-up and keeping up with the various comparative criminal systems, as well as developing the process of exchanging experiences and competencies between various countries, especially neighboring countries.Leader in this field.

Referrals and References:

1- Baqiqi Abeer, Combating cybercrime in Algerian and Emirati legislation - a comparative study -, doctoral thesis in law, specializing in the penal system and contemporary penal policy, Faculty of Law at Mohamed Kheidar University in Biskra, Algeria, 2018, p. 11.
2- Baqiqi Abeer, Previous reference, p. 11.
3- Tariq Ibrahim Al-Desouki Attia, Information Security, The Legal System for Information Protection, New University Publishing House, Egypt, 2015, p. 153.
4- Ibid, p. 154.
5- Lawrence Saeed Al-Hawamdeh, Information crimes, their elements and the mechanism of combating them, a comparative analytical study, Al-Mizan Magazine, Volume 4, Issue 1, International Islamic Sciences University, Jordan, 2017, p. 189.
6- Zabiha Zidane, Information Crime in Algerian and International Legislation, Dar Al-Huda, Algeria, 2011, p. 43.
7- Saidani Naeem, Mechanisms of Research and Investigation of Information Crime in Algerian Law, Master's Thesis in Legal Sciences, Specializing in Criminal Sciences, Hajj Lakhdar University, Batna, Algeria, 2013, p. 42.
8- Qarat Amal, previous reference, p. 28.
9- This is in accordance with Law 04-15 amending the Penal Code, Official Gazette No. 71 dated 11/10/2004, p. 8.
10- Qarat Amal, previous reference, p. 26.
11- Saeedani Naeem, previous reference, p. 43.

12- Saeedani Naeem, previous reference, p. 43.
13 -Ibid., p. 45.
14Ahmed Hossam Taha Tammam, Crimes resulting from the use of computers - a comparative study -, 1st edition, Dar Al Nahda Al Arabiya for Publishing and Distribution, Egypt, 2000, p. 264.
15- Qarat Amal, op. cit., p. 29.
16- Faith Baghdadi, The impact of amending the Algerian Penal Code in combating electronic crime, Afaq Journal for Research and Political Studies, international peer-reviewed, Illizi University Center, Algeria, issue June 4, 2019, p. 188.
17- Qarat Amal, previous reference, p. 41.
18- Nabila Heba Harwal, Procedural Aspects of Internet Crimes in the Evidence-Gathering Stage, Dar Al-Fikr University, Alexandria, D.D., 2006, p. 47.
19- Lawrence Saeed Al-Hawamdeh, previous reference, p. 207.
20- Lawrence Saeed Al-Hawamdeh, previous reference, p. 208.
21- Qarat Amal, previous reference, p. 57.
22- Mahdi Reda, Cybercrimes and mechanisms to combat them in Algerian legislation, Eliza Journal of Research and Studies, Volume 06, Issue 02, 2021, p. 114.
23- Mahdi Reda, previous reference, p. 115.
24- Article 394 bis of Law 04-15 amending and supplementing Order 66-156, dated November 10, 2004, containing the Penal Code, Algerian Official Gazette, issued on November 10, 2004, No. 71, p. 113.
25- Article 394 bis 1, Law 04-15, op. cit., p. 113
26- Article 394 bis 2, Law 04-15, op. cit., p. 113.
27- Article 394 bis 3, Law 04/15, previous reference, p. 113.
28- Article 303 bis, of Law 06-23 containing the Penal Code, dated December 20, 2006, Official Gazette of the Algerian Republic, No. 48, p. 112.
29- Saida Bouznon, Combating cybercrime in Algerian legislation, Journal of Human Sciences, Constantine Mentouri Brotherhood University, Faculty of Law, Issue 52, December 2019, p. 50
30- Reda Mahdi, previous reference, p. 117.
31- Farouk Khalaf, Legal Mechanisms to Combat Information Crime, Journal of Rights and Liberties, No. 2, 2015, p. 18.
32- Ibid., p. 18.
33- Article 13 of Law 09-04 of August 5, 2009, containing special rules for preventing and combating crimes related to information and communication technology, Algerian Official Gazette No. 46, issued on August 16, 2009.
34- Article 2, Law 19/172, dated June 6, 2019, determines the composition of the National Authority for the Prevention, Combat, and Regulation of Crimes Related to Information and Communication Technology, and how it operates, Algerian Official Gazette, No. 37, issued on June 9, 2019.
35- Article 04, Law 19/172, op. cit.
36- Suhaila Bouzbara, The National Authority for the Prevention and Combat of Crimes Related to Information and Communication Technology: Between the Confidentiality of Personal Data and Combating Cybercrimes, Critical Journal of Law and Political Science, Volume 07, Issue 02, 2022, p. 569
37- Farouk Khalaf, previous reference, p. 11.