Science of Law, 2026, No. 2, pp. 50-54
DOI: 10.55284/yrd1c495

The National Criminal Pole for Combating Crimes Related to Information and Communication Technologies as a Legal Mechanism to Counter Cybercrime in Accordance with Order No. 21-11

Tarafi Sadek

University of Bouira, Algeria.

Keywords:
Combating cybercrime,
Investigation and proof,
Criminal pole,
Criminal policy,
Cybercrime.

Abstract. This research paper aims to examine the current state of criminal law's response to cybercrimes in Algeria, as well as the future prospects for addressing such offenses within the Algerian criminal justice system. It does so by anticipating an effective criminal policy capable of mounting a genuine confrontation against one of the most dangerous types of contemporary crimes. Cybercrimes represent one of the most severe security challenges facing the international community. These offenses are highly complex, perpetrated through advanced technologies by highly intelligent offenders, rendering investigation and proof exceptionally difficult. Traditional investigative procedures conducted by authorities responsible for criminal inquiry and detection are ill-suited to the nature of cybercrimes. Consequently, the Algerian legislator introduced Order No. 21-11, which provides for the establishment of a National Criminal Pole dedicated to combating crimes in the field of information and communication technologies. This constitutes a significant achievement and a qualitative addition to efforts aimed at countering this form of crime.

1. INTRODUCTION

The tremendous development in the field of information technology and its integration into all aspects of life has led to an unbounded expansion of its role. Computers, electronic technologies, and the Internet have become the language of the era—an indispensable tool. Reliance on these means has grown substantially in managing the most precise details of economic, social, military, medical, and other facilities. These tools have attained such critical importance that the need to provide the highest levels of protection around them has intensified, in order to prevent disruption to the functioning of these facilities or attacks that could affect the fundamental interests in individuals' lives.

With the widespread dissemination of these modern technological means among members of societies, their common use, and the expansion of interactions through them, every individual has acquired the ability to interact and communicate without barriers of borders or geography. This is facilitated by the ease and speed of transferring and receiving information, technologies, and accessing data and programs. While the emergence of these new and advanced fields of science and knowledge has brought numerous benefits and advantages, it has also been accompanied by the emergence of many problems and negative phenomena in the form of crimes committed by some technology users. These crimes are characterized by their gravity, ease of commission, and the challenge of crossing national borders; they may be termed cybercrimes.

Like other societies, Algerian society is significantly affected by the rapid and widespread proliferation of cybercrimes. It is therefore imperative to confront these crimes through diverse means of social defense, including penal legal protection, which remains one of the most important mechanisms available to society for preserving its existence and safeguarding its interests. However, given the novelty of these crimes and the relative recency of the penal legislation regulating criminal protection across various fields in Algeria, shortcomings persist in delineating the boundaries of this protection from a penal perspective. This necessitates heightened awareness and urgent action to establish sound legal frameworks and clear procedural references for combating this particularly dangerous category of crimes.

Daily observations highlight the substantial expansion in the use of computers and the Internet across all segments of society, as well as heavy reliance on them in numerous areas of life—economic, social, and communicative. This grants them considerable importance for individuals across all categories, rendering them deserving of protection due to their direct impact on many fundamental interests in societal life. Accordingly, criminal protection must be extended to matters affecting or relating to electronic domains. Thus, the core research question can be formulated as follows:

What is the current reality and future prospects of penal protection in the electronic and Internet domain in Algeria, in terms of criminalization, combating, and proof?

Cybercrime constitutes an emerging form of offense, and its legal treatment must therefore adopt a comprehensive approach. The principal axes of penal protection are inherently interconnected: the specificity of criminalization necessitates corresponding specificity in proof and prosecution alike.

The specificity of criminalization stems primarily from the fact that most such crimes occur in the virtual rather than the physical realm. Even when certain offenses touch the material world, they retain distinctive characteristics that differentiate them from traditional crimes, requiring tailored criminalization to prevent perpetrators from evading punishment. To this end, the Algerian legislator has enacted a series of laws to counter this crime, which has reached advanced levels, including Order No. 21-11. This Order explicitly provides for the creation of a National Criminal Pole dedicated to combating crimes in the field of information and communication technologies.

As regards the specificity of proof in this category of offenses, it is fraught with significant difficulties in detecting and preserving

evidence obtained from the crime scene—whether physical or virtual. Digital evidence is difficult to secure, easy to erase or disappear, and susceptible to manipulation regarding its discovery or content.

The specificity of prosecution arises from the technical nature of these crimes, which demands specialized capabilities on the part of those responsible for follow-up and pursuit. It also requires appropriate legal mechanisms to assist in searching for electronic evidence, ensuring the legitimacy of procedures for uncovering such evidence, in addition to the legitimacy of the evidence itself.

Accordingly, this study is divided into two main sections. The first section addresses the current state of Algerian criminal law's confrontation with cybercrimes at the level of criminalization. The second section examines the role of the National Criminal Pole for Combating Crimes Related to Information and Communication Technologies in addressing cybercrime, through the anticipation of an effective national criminal policy aimed at achieving a genuine response to one of the most serious contemporary crimes.

2. THE CURRENT STATE OF ALGERIAN CRIMINAL LAW'S CONFRONTATION WITH CYBERCRIMES AT THE LEVEL OF CRIMINALIZATION

The legitimacy of criminalization and punishment constitutes one of the most fundamental principles underpinning criminal law in its endeavor to protect society's core interests. Criminalization is the distinctive feature that enables criminal law to safeguard those interests, distinguishing it from other branches of law that merely censure acts or behaviors. Through criminalization, criminal law reinforces the legal protection afforded by those other laws, manifesting the coercive force underlying legal rules to render them binding and thereby capable of regulating communal life.[1]

2.1. Defining Cybercrimes

In general, a crime may be defined as "an act prohibited by criminal law, emanating from a faulty will, for which the legislator prescribes a penalty," or as "an act or omission to which the law attaches a criminal penalty." Thus, crime represents disobedience seeking to rebel against the collective will, rendering it incompatible with the law's will, which defines the offending act and the consequent punishment based on collective intent.

Cybercrime can be defined as an assault targeting stored computer data or transmitted information across information systems and networks, foremost among them the Internet. It is a technical offense committed clandestinely by intelligent criminals possessing advanced technical knowledge, directed against the right to information.[2]

The Algerian legislator defined information-related crimes in Article 2, paragraph (a) of Law No. 09-04 dated 5 August 2009, which sets forth special rules for the prevention of and fight against crimes related to information and communication technologies, stating: "Crimes related to information and communication technologies are: crimes affecting automated data processing systems as defined in the Penal Code, or any other crime committed or facilitated through an information system or electronic communications network."[3]

To elucidate the nature of cybercrimes, it is essential to encompass the general meaning of the means through which they are committed, their object, and the legal interests deserving criminal protection. Accordingly, we first address the definition of electronic means, then the object of the assault, and finally the interest warranting criminal protection.

2.1.1. Definition of Electronic Means

Electronic means refer to those associated with the use of modern technologies, generally considered as applications of the computer in a broad sense. They are linked to contemporary communication technologies and information technology, and thus are connected, directly or indirectly, to the computer or electronic system (the computer). The computer, as an information system, constitutes the central axis of electronic transactions, regardless of the form in which it manifests. Beyond this, there exists what connects the realms of computer communication, namely the Internet. Therefore, it is essential to clarify the meaning of the computer (or electronic computer) in order to identify the primary tool in cybercrimes, as well as to explain the concept of the Internet network.

Specialists define the computer as “an electronic device composed of interconnected components directed by specific commands to process and manage information in a particular manner, through the execution of three fundamental operations: receiving input data (acquiring raw facts), processing data into information (performing calculations, comparisons, and input transformations), and displaying output information (obtaining results).” Some define it in terms of its mechanism or operational system as “a set of devices that function integrally with one another to process incoming data according to a pre-established program in order to produce specific results,” or as “an electronic calculating machine that receives data and, with the aid of specific programs, processes these data to arrive at the desired outcomes.” In simple terms, it can be described as a device designed to process data in a pre-programmed automated manner, enabling the results of this process to be obtained on demand.[4]

Consequently, the computer as an integrated system operates within a tripartite equation: it consists, first, of a collection of physical devices that form the tangible hardware of the computer system (referred to as *Hardware*); second, a set of information, commands, instructions, or programs (referred to as *Software*); and third, the human element—the individuals who interact with the software and utilize it according to their respective objectives. This third component imparts real value to both the hardware and software.[5]

---

[1] Muhammad Najib Hosni: Explanation of the Penal Code – General Part, 1st ed., Dar al-Nahda al-Arabiyya, Cairo, 1989, p. 7.

[2] Abdel Fattah Hijazi: Emerging Crimes, 1st ed., Mansha'at al-Ma'arif lil-Nashr, Alexandria, 2009, p. 6.

[3] Law No. 09-04 dated 5 August 2009, containing special rules for the prevention of and fight against crimes related to information and communication technologies, published in the Official Gazette No. 47 dated 16 August 2009.

[4] Qashoush Huda Hamid: Computer Crimes in Comparative Legislation, Dar al-Nahda al-Arabiyya, Cairo, 2002, p. 8.

[5] Nahla Abdel Qader Al-Momani: Information Crimes, 1st ed., Dar al-Thaqafa lil-Nashr, Amman, 2008, p. 28.

2.1.2. The Object of Cybercrime

It can be stated that the computer constitutes the foundation of electronic and informational transactions and therefore serves as the primary axis around which cybercrimes revolve. Among the most prominent threats to information systems and computers are: attacks on the physical entity of the computer through damage, theft, or seizure; and attacks on the informational framework, which may occur through alteration of programs, introduction of faulty programs such as viruses, unauthorized access to or viewing of information, intentional or unintentional unauthorized entry into networks or databases, insertion of data with the intent of falsification or forgery (whether in bad faith or good faith), deletion, concealment, or failure to enter data, alteration of data, and interference with encryption keys or passwords.

In summary, the object and subject matter of these crimes are computer data and information, which are generally targeted by offenders' attacks. Such crimes are committed either *on* the computer itself or *by means of* it—sometimes treating the computer as the direct object of the crime, and at other times as the instrument used to commit the offense against another object, namely electronic information and data.[6]

2.2. The Legal Interest Deserving Criminal Protection through Electronic Criminalization

The starting point for identifying these interests lies in protecting computers and electronic devices, as well as ensuring the security of information uploaded to the Internet and stored on connected computers. The components of the security of such information and devices can be reduced to several highly significant aspects:

- Confidentiality of information: encompassing necessary measures to prevent unauthorized access to confidential or private information.
- Integrity of information: including measures required to protect information from unauthorized alteration.
- Availability of access to information and computer resources: covering protection of the ability of authorized persons to access information.
- Integrity of computer hardware, electronic equipment, and the programs, information, and data residing thereon.

Given that computers and the Internet primarily concern the collection, storage, and circulation of information, ensuring the security and protection of this information has become an imperative necessity. To this end, specialists in information technology and related fields have developed techniques and software that perform this protective function from a technical standpoint. These make computers and networks a virtual space containing a quantity of personal information for each individual—analogous to a person's financial estate—which may appropriately be termed the "informational estate" or "technological estate." Ultimately, this estate cannot maintain its integrity except through the conferral of legal protection, which reaches its highest degree through the imposition of criminal law safeguards.

Accordingly, the interests deserving criminal protection can be summarized as follows: • Protection of the right to confidentiality and the sanctity of private life. • Protection of intellectual and informational property rights, which may be designated as the "informational estate" or "technological estate," in conjunction with the enactment of specific laws that recognize and safeguard these rights. • Protection of tangible property rights over devices, equipment, and all material elements susceptible to attack through electronic means. • Protection of the electronic public order as an integral part of the administrative and economic public order of the state, consistent with modern state trends toward what is known as e-government, which advances electronic administration and the delivery of numerous services and transactions through comprehensive electronic systems.[7]

3. THE ROLE OF THE NATIONAL CRIMINAL POLE FOR COMBATING CRIMES RELATED TO INFORMATION AND COMMUNICATION TECHNOLOGIES IN COUNTERING CYBERCRIME

Since its entry into the era of digitalization and the adoption of the e-Algeria project, Algeria has sought to confront cybercrime. A comprehensive arsenal of legal texts has been enacted, while others have been amended. In this context, a National Criminal Pole for Combating Crimes Related to Information and Communication Technologies was established pursuant to Order No. 21-11. This represents a legal mechanism and a national achievement aimed at providing a strong impetus to counter this form of crime. To clarify this, the following points may be noted:

- The Algerian legislator has kept pace with developments in the field of crime and aligned with international legislation by establishing numerous specialized criminal poles to address certain serious offenses, including those affecting automated data processing systems. This approach culminated in the creation of the National Criminal Pole specialized in combating crimes related to information and communication technologies, pursuant to Order No. 21-11.[8]

This Pole is a judicial body established at the level of the court attached to the Algiers Court of Appeal, specialized in the prosecution, investigation, and adjudication of crimes related to information and communication technologies and associated offenses.

Crimes related to information and communication technologies are defined as any offense committed or facilitated through the use of an information system, an electronic communications network, or any other means or mechanism connected to information and communication technologies.[9]

Pursuant to Article 211 bis 02 of Order No. 21-11, the Public Prosecutor attached to the Criminal Pole for Combating Crimes Related to Information and Communication Technologies, the Investigating Judge, and the President of the same Pole hold exclusive jurisdiction over the prosecution, investigation, and judgment of crimes related to information and communication technologies involving the following:

- Crimes affecting national security and national defense.

---

[6] Muhammad Al-Qahtani: Information Security in Simple Language, King Saud University, Riyadh, 2009, p. 7.

[7] Abdel Fattah Hijazi, op. cit., p. 12.

[8] Order No. 21-11 dated 16 Muharram 1443 AH, corresponding to 25 August 2021, amending and supplementing Order No. 66-155 dated 18 Safar 1386 AH, corresponding to 8 June 1966, containing the Code of Criminal Procedure, Official Gazette No. 65 of 2021.

[9] Article 211 bis 22 of Order No. 21-11.

- Crimes involving the dissemination and promotion of false news to the public that may undermine security, public tranquility, or societal stability.
- Crimes involving the dissemination and promotion of false news and malicious information affecting public order and security, whether organized in nature or transnational.
- Crimes of human trafficking, trafficking in human organs, or migrant smuggling.
- Crimes affecting automated data processing systems related to public institutions.
- Crimes of discrimination and hate speech.

3.1. The Role of the National Criminal Pole in Combating Cybercrime

The National Criminal Pole operates in the field of combating crimes related to information and communication technologies—crimes that are particularly complex in legal terms due to the multiplicity of perpetrators, accomplices, or victims; the geographical expanse of the crime scene; the gravity of their consequences or resulting damages; their organized or transnational character; or their impact on public order and public security. Such crimes require the use of specialized investigative methods, technical expertise, or recourse to international judicial cooperation.

The establishment of a specialized criminal pole for crimes related to information and communication technologies forms part of the state's comprehensive strategy to address this category of offenses. It represents an additional step in the ongoing effort to counter cybercrimes, following the legislator's creation of a National Authority responsible for the prevention of and fight against crimes related to information and communication technologies, which was classified among the "independent administrative authorities," in contrast to the Criminal Pole, which possesses a judicial character.

3.2. Toward an Effective Criminal Policy for Combating Cybercrimes – An Analytical Reading

Legislative policy may be defined as the principal ideas and objectives sought to be achieved, which guide the law in its creation and application. Criminal policy, in turn, comprises the set of rules and principles that determine the formulation of criminal law provisions, whether concerning criminalization, prosecution, or prevention.

The realization of criminal policy principles with respect to a specific phenomenon first requires thorough monitoring and in-depth study of that phenomenon to ensure the availability of comprehensive information surrounding it. This is followed by delineating the features of legal protection for the phenomenon, identifying the interests orbiting its regulation, and ultimately pinpointing deficiencies in criminalization texts so that criminal protection can be extended to those significant and deserving interests—all while taking into account prevention and deterrence factors.

Accordingly, the criminalization and prosecution of this emerging phenomenon are of paramount importance in order to combat it and mitigate the resulting harms. This requires anticipating the necessary procedures to be implemented to achieve effective confrontation and suppression of this novel form of criminality, which demands substantial and multifaceted efforts from various entities. There is a need for legal criminalization, informational protection through the adoption of protocols and the establishment of specialized bodies, as well as societal and institutional awareness-raising regarding informational protection measures.

4. CONCLUSION

In conclusion, this research paper demonstrates that the Algerian legislator has successfully established a legal arsenal to counter cybercrime, particularly through the National Criminal Pole for Combating Crimes Related to Information and Communication Technologies. This Pole constitutes one of the most important legal mechanisms relied upon to combat this serious category of crimes, especially given their proliferation, evolving levels, and diverse forms. It may therefore be regarded as one of the valuable national gains that will provide a strong impetus to efforts to confront cybercrimes. On this basis, the following conclusions are reached:

- The National Criminal Pole represents a significant achievement and qualitative addition to the fight against cybercrime.
- This Pole exercises broad jurisdiction over offenses affecting automated data processing systems, constituting one of the most important steps toward preserving confidentiality and privacy.
- The computer, as an information system, constitutes the central axis of electronic transactions regardless of the form in which it appears. It is defined as a device concerned with processing data in a pre-programmed automated manner, enabling the results of this process to be obtained on demand.
- The object and subject matter of cybercrime are computer data and information, generally targeted by offenders' attacks. Such crimes are committed either *on* the computer itself or *by means of* it—treating the computer at times as the direct object of the crime and at other times as the instrument for committing the offense against another object, namely electronic information and data.
- The interests deserving criminal protection in the context of electronic criminalization include the protection of the right to confidentiality and the sanctity of private life; the protection of intellectual and informational property rights (which may be termed the "informational estate" or "technological estate"); the protection of tangible property rights over devices, equipment, and all material elements susceptible to attack through electronic means; and the protection of electronic public order as an integral part of the state's administrative and economic public order.
- Law No. 09-04 dated 5 August 2009, containing special rules for the prevention of and fight against crimes related to information and communication technologies, remains relatively recent, as it addresses the technical aspects of communications processes themselves, as well as the regulatory framework, monitoring, and penalization of violations and crimes committed through the misuse of communication technologies. Nevertheless, while certain provisions criminalize behaviors falling within the scope of cybercrimes, the law as a whole does not provide sufficient criminal protection to encompass all acts committed in the context of cybercrimes.
- Genuine confrontation with any type of crime occurs when specialized bodies and regulated procedures exist, demonstrating the capacity for prosecution, detection, evidence gathering, and proof of the crime or unlawful conduct before the competent judicial authorities, paving the way for trial and the imposition of deterrent penalties on the perpetrator.

- Units combating electronic crimes face numerous obstacles, whether related to capabilities or procedural and legal impediments concerning the legitimacy of procedures and extracted evidence, necessitating the enactment of laws on criminalization, prosecution, and proof.
- It is essential to establish a set of rules governing the mechanisms for collecting, storing, processing, and transmitting data, as well as rules granting individuals informational rights related to computers, information systems, and the Internet—rights that regulate access to their private sites, ensure the integrity and accuracy of such sites, and enable owners to modify or amend them.
- The enactment of substantive criminal rules that define acts constituting assaults on informational rights, criminalize such acts, and prescribe appropriate penalties capable of achieving general and special deterrence against their perpetrators.
- Computer and Internet crimes present numerous procedural challenges to judicial police authorities, owing to their virtual nature, which distinguishes them from traditional crimes.

REFERENCES

Abdel Fattah Hijazi. (2009). *Emerging crimes* (1st ed.). Mansha'at al-Ma'arif lil-Nashr.

Al-Momani, N. A. Q. (2008). *Information crimes* (1st ed.). Dar al-Thaqafa lil-Nashr.

Al-Qahtani, M. (2009). *Information security in simple language*. King Saud University.

Hosni, M. N. (1989). *Explanation of the penal code: General part* (1st ed.). Dar al-Nahda al-Arabiyya.

Law No. 09-04, dated August 5, 2009, containing special rules for the prevention of and fight against crimes related to information and communication technologies, Official Gazette No. 47 (August 16, 2009).

Order No. 21-11, dated Muharram 16, 1443 AH (August 25, 2021), amending and supplementing Order No. 66-155 dated Safar 18, 1386 AH (June 8, 1966), containing the Code of Criminal Procedure, Official Gazette No. 65 (2021).

Qashoush, H. H. (2002). *Computer crimes in comparative legislation*. Dar al-Nahda al-Arabiyya.