Journal of Legal Studies and Researches
e-ISSN: 2676-1688 p-ISSN: 2437-1084
Vol: 10 N° 2, June 2025, p. 27–42

The Legal Nature of Cybercrime

Yourmeche Mourad
Faculty of Law and Political Sciences, University of M'sila, Algeria
mourad.yourmeche@univ-msila.dz
https://orcid.org/0000-0002-1450-0220

Received:08/05/2025 | *Accepted:08/06/2024* | *Published*: *20/06/2025*

Abstract:
Cybercrime is considered one of the most dangerous crimes witnessed by the modern world. Its seriousness lies in its special nature and distinctive characteristics, as it differs from traditional crimes that occur in the physical world. Cybercrime is the type of crime that takes place in cyberspace, also known as the virtual world, represented by the internet and its electronic components. Therefore, it is closely linked to the World Wide Web, which in turn complicates matters and makes it more challenging for the authorities responsible for combating and addressing this type of crime, whether at the level of security agencies or judicial bodies.
Keywords: cybercrime; the internet; security agencies; judicial authorities

1. INTRODUCTION

The tremendous and rapid technological advancement witnessed by the world since the early 1990s, particularly in the field of information and communication technology, has led to the emergence of modern means of communication, most notably the Internet — also known as the World Wide Web. The Internet has become the most widely used and widespread means across various aspects of life due to its numerous advantages. However, its use has not been confined to positive purposes; it has also become the preferred tool for certain groups to commit illegal acts that pose threats to the security and safety of individuals and states interacting through the network, such as fraud, credit card forgery, personal data espionage, infringement of intellectual property rights, sabotage of information systems, and other criminal acts.

Since these illegal acts are committed through the Internet, the resulting crimes are termed "cybercrimes," "information crimes," or "electronic crimes." Legislators in various legal systems have addressed these crimes with special legal provisions to combat and prevent them, due to their differences from traditional crimes recognized in conventional legal systems. Additionally, international agreements specializing in this field have been concluded.

Referring to the Algerian legislator, it can be noted that they have addressed this type of crime through Ordinance No. 04-15, which amended the Penal Code, and Law No. 09-04 of 2009, which defines the specific rules for the prevention and fight against crimes related to information and communication technologies.

The main issue posed here lies in identifying the essence of cybercrime, as it is a newly emerged crime that appeared with the advent of the information network. Can it be classified within traditional crimes, or does it possess a distinct nature?

To answer this problem, the descriptive and analytical method was adopted to explore aspects related to the legal nature of cybercrime. The topic is divided into two sections: the first section discusses the concept of cybercrime, which includes the definition of cybercrime and its

characteristics. the second section deals with the legal qualification of cybercrime through its classifications and the elements constituting cybercrime.

2. The Concept of Cybercrime

The concept of cybercrime remains one of the modern concepts due to its connection with one of the most significant innovations of contemporary technology (the World Wide Web – the Internet). Consequently, it differs from traditional crimes. Cybercrime can also fall under several different designations, such as: cybercrimes, computer crimes, high-tech crimes, Internet crimes, and electronic crimes. All these terms are new and are linked to the means used in committing the crime, namely Internet networks.

To clearly define the concept of cybercrime, it is first necessary to provide a definition of this type of crime and then address the main characteristics that distinguish it from traditional crimes.

2.1 Definition of Cybercrime

Given that cybercrime is a newly emerging form of crime, coupled with the difficulty of confining it within specific temporal and spatial boundaries, and the lack of consensus on a unified terminology to describe it, establishing a comprehensive and precise definition of cybercrime has proven challenging, whether in national or international legislation. Therefore, it has become necessary to turn to legal scholarship to address this issue. Scholars have been divided into two main approaches regarding the definition of cybercrime: some adopt a narrow definition, relying on one of two criteria — either an objective criterion, focusing on the subject matter of the crime, or a personal criterion, focusing on the perpetrator of the crime. Others, however, adopt a broader definition, based on the integration of multiple criteria. These approaches will be explored in the following discussion.

A. The Narrow Definition of Cybercrime

Proponents of this approach define cybercrime based on the objective criterion, meaning the subject matter of the crime. They describe it as: "Any

unlawful activity aimed at copying, accessing, altering, or deleting information stored within a computer."[1]

It is also defined under this approach as: "A crime resulting from the insertion of falsified data into systems and the misuse of outputs, in addition to other acts that form more technically complex crimes, such as modifying a computer."[2]

The United Nations has aligned with this approach, describing crimes committed via the Internet as: "Any unlawful act aimed at performing electronic operations that impact the security of information systems and the subjects they process."[3]

Additionally, within the framework of the narrow definition of cybercrime, there is another perspective that relies on the personal criterion for defining cybercrime. According to this view, it is defined as: "Any unlawful act where knowledge of computer technology is significantly necessary for its commission, both for prosecution and for execution.[4]" It is also defined as: "A crime committed when an individual uses their knowledge of computers to perform an illegal act."[5]

This approach has faced criticism, notably the argument that it is not feasible to define this type of crime solely based on the personal criterion, i.e., the characteristic traits of the perpetrator, which would require significant knowledge of information technology. It is insufficient to rely solely on the personal criterion as the foundation for defining cybercrime; other considerations, such as those related to the subject matter of the crime, must also be taken into account.[6]

B. The Broad Definition of Cybercrime

The proponents of this approach define cybercrime by integrating several criteria (personal criterion, objective criterion, means of committing the crime). They consider that cybercrime is: "A crime in which the computer is used as a tool or means to commit it, or represents an inducement to commit it, or a crime in which the computer itself is the victim."[7]

It is also defined according to this approach as: "Crimes that occur through the global network, in which the computer and its global networks

are used as an assisting means to commit the crime, such as using it in fraud, money laundering, defamation, and slander."[8]

Among the definitions within this approach, there is also the definition of the Organization for Economic Cooperation and Development (OECD) in its 1982 report on fraud. The report, issued by Belgium as a member of the organization, [9]states that cybercrime is: "Any act or omission that could harm material or immaterial property as a direct or indirect result of the intervention of information technology."[10]

In another definition, the OECD describes the crime committed online as: "Any illegal, immoral, or unauthorized behavior related to the automatic processing or transmission of data."

The definitions of cybercrime according to this approach have been subject to several criticisms. Among them is the lack of precision in defining cybercrime. According to these definitions, it is sufficient for the act or behavior to be socially unacceptable or unethical, or to be committed against society for it to be considered a cybercrime or an information crime. Another criticism directed at these definitions is that they rely on describing certain criminal acts rather than defining the essence of the crime itself. Furthermore, the descriptions contained in these definitions cannot be used as a basis for determining cybercrime because the forms or descriptions of cybercrime cannot be fully enumerated, considering both the specific nature of cybercrime and the ever-evolving nature of technology. Additionally, the criterion of describing the crime is not a sufficient or reliable measure to determine the criminal act.[11]

Despite these criticisms directed at the wide definitions of cybercrime, they can still be relied upon to categorize cybercrimes, albeit relatively, since they combine several criteria in defining cybercrime. [12]In contrast, proponents of the narrow definition of cybercrime rely on a single criterion (the subject of the crime) to define cybercrime, which results in limiting the crime to a narrow scope and potentially allowing many acts and behaviors to evade punishment.[13]

2.2 Characteristics of Cybercrime

Since cybercrime is one of the newly emerging crimes resulting from

the tremendous development in the field of information and communication technology, and it is a crime committed in cyberspace, it has distinctive characteristics that set it apart from traditional crimes committed in the physical world. This is what we will attempt to address as follows.

A. The concealment of cybercrime and the rapid development in its commission

Crimes arising from the use of the internet (cybercrimes) are characterized by being hidden and concealed in most cases, as the victim does not have the ability to notice or monitor them while they are being committed. This is because the perpetrator possesses high technical skills and capabilities that enable them to commit the crime with precision. Examples of this include sending destructive viruses to information programs, stealing money by transferring it from the victim's accounts to the perpetrator's account, spying on or destroying private data, and other criminal acts.[14]

B. It is considered a "clean" crime

The commission of cybercrimes does not require violence or significant effort; they are carried out with minimal effort compared to traditional crimes, which often require substantial physical exertion and take various forms that generally involve the use of violence. In contrast, internet crimes are inherently quiet crimes; they do not require the exercise of violence to commit. Instead, all that is needed is the ability to handle a computer and control information technology via the internet.[15]

C. Cybercrime is a Transnational Crime

With the emergence of the World Wide Web (Internet), there are no longer any visible or tangible boundaries that prevent the transfer and circulation of information across all parts of the world.[16] This development facilitates and aids the perpetrator in committing their crime and achieving their unlawful goals from any location without exerting any significant effort.

D. Non-reporting of Cybercrime

In many cases, internet crimes are not reported by the victims, either because the victim is unaware of the crime or due to fear of public

exposure. As for the crimes that are discovered, they are often found by chance, and it usually happens after a long period following the commission of the crime. It is important to note that the number of internet crimes that have been discovered is much lower than the actual number of crimes that have not yet been uncovered, especially in the absence of sufficient legal and institutional frameworks to combat and fight this type of crime.

E. Ease of Concealing the Evidence of Cybercrime and Difficulty in Tracking Perpetrators

Cybercrime occurs outside the framework of tangible physical reality, as its elements exist in an informational environment consisting of a computer and the internet. This makes it easier for the perpetrator to erase traces of the crime, thereby complicating its discovery. Additionally, it makes it difficult to track the offenders. In internet crimes, the perpetrator possesses the technical skills and knowledge in the field of information that allow them to erase any evidence entirely. This can be achieved simply by using passwords or specific codes, deleting the software programs used in committing the crime, or resorting to encryption methods to prevent access to any evidence that may incriminate them.[17]

F. Sixth: Jurisdiction and International Nature of Cybercrimes

Cybercrimes are characterized by their international nature, as these crimes are often committed by individuals from one country, while the crime itself occurs in another. Therefore, these crimes do not recognize geographical boundaries, as their core is the information. This raises questions regarding jurisdiction over such crimes. Moreover, the extension of activities such as monitoring, investigation, and the execution of searches beyond national borders requires comprehensive international cooperation aimed at investigating and combating these crimes, while respecting the national sovereignty of the involved states.

J. Lack of Expertise Among Security and Judicial Authorities and Inadequate Existing Laws

Cybercrimes are emerging crimes, and due to their unique nature, they differ from traditional crimes. This has led to a complete change in the methods of investigation and evidence collection used by relevant

authorities in monitoring and investigating these crimes. Furthermore, detecting and apprehending perpetrators of these crimes requires modern methods that are appropriate for the nature of such offenses.

Since these crimes require advanced technologies for their commission, discovering and investigating them also requires sophisticated tools and techniques. This demands specialized investigative methods, which have not been fully met by security and judicial authorities, either at the national or international levels. The reason for this is partly the nature of the crime itself and the lack of technical knowledge necessary to address this phenomenon, which presents a multi-dimensional risk: socially, economically, security-wise, and politically.[18]

Regarding the existing laws, they have proven inadequate in confronting this type of crime due to their connection to information technology. This highlights the need for legislators to enact modern laws that align with the nature of these crimes, alongside enhancing cooperation and coordination efforts between various national and international legal bodies, including experts specialized in informatics, within the framework of combating cybercrimes.

3. Legal Qualification of Cybercrime

Researching the legal qualification of cybercrime requires, first, its classification, and then identifying the elements on which it is based.

3.1 . Classification of Cybercrime.

Cybercrimes are numerous and diverse, reflecting the variety of human activity in cyberspace. Among the most common forms that represent typical cases of cybercrime, we mention the following.

A. Crimes of Infringement on Digital Intellectual Property Rights

Intellectual property represents the highest form of ownership, and this elevation is evident through the connection of the rights associated with this property to the most valuable asset a person possesses: the mind, in its creations and intellectual manifestations [19] .Since works related to intellectual property are often presented digitally on the internet today, such as digital works, trademarks, industrial designs, etc., they have become

susceptible to cyberattacks in various forms, depending on the targeted work. These attacks may include downloading or publishing a book under someone else's name, selling a product bearing a counterfeit trademark, or infringing on the author's rights and related rights through copying or piracy.

B. Crimes Against Property

Among the common cybercrimes are those committed with the intent of obtaining money through fraud and deception, which are the most prevalent, or through information falsification, counterfeiting, or embezzlement, especially in light of the growth of e-commerce and the emergence of modern tools and methods for conducting it, such as electronic funds transfer technology and the use of electronic cards. Cybercrime can occur through the use of expired payment cards, counterfeit credit cards, or electronic payment cards, or by attacking funds using a computer to input false data, modify, or delete existing data with the intent to steal or transfer money.

C. Money Laundering Crimes

Money laundering refers to the process of making money obtained from illegal sources appear legitimate by investing it in legal fields, the most significant of which include banking and real estate investments. With the advancement of information and communication technologies and the emergence of the internet as one of its manifestations, money laundering crimes have increasingly been carried out via this network, using the technique of electronically transferring illicit funds between banks. This has made tracking the movement of money much more difficult, thus complicating the detection of such crimes.[20]

D. Crimes Against the Sanctity of Private Life

The existence of computers and the internet has made it easier to violate privacy than ever before. This is something that various comparative legislations have sought to address by protecting personal data stored in information programs. They have imposed restrictions on governments, public and private administrative bodies, and individuals regarding the creation of information systems. These restrictions prohibit the storage of

personal data that infringes on freedoms and private life, the violation of confidentiality and privacy, or the misuse of electronic commerce data for purposes other than those for which they were intended.[21]

E. Human Trafficking Crimes

Human beings have become commodities to be bought and sold by organized crime syndicates. The scope of this crime has expanded to become an international offense, especially with the availability of the internet. Human trafficking crimes are now being carried out through this network, starting with advertisements and promotions as a preliminary stage before contracts are made and carried out by these specialized criminal groups, who are spread across various countries around the world. However, the common link that brings them together and facilitates the commission of their crimes is the internet.

F. Crimes of Data Breach

The information and data stored in electronic computers constitute a vast and highly significant informational wealth. As such, some individuals attempt to breach protection systems and access this data, uncovering its secrets or completely or partially destroying it. Violating this informational wealth results in heavy losses due to the enormous costs of storing it. Therefore, most legislations aim to protect websites by establishing certain controls or monitoring mechanisms for activities conducted through these sites, such as criminalizing intentional access or unauthorized persistence in data processing systems.[22]

G. Crimes Against Electronic Signatures

An electronic signature is defined as: "Any personal mark in the form of letters, numbers, symbols, signs, sounds, or others, with a unique character indicating its association with the signer and accredited by a certification authority."[23]

The electronic signature has become essential in the field of electronic contracts and all legal acts carried out via the internet, as it enables the identification of the signer. In addition, it serves as a means of proof. Therefore, many countries have enacted laws specific to electronic signatures, criminalizing all forms of attacks on them, such as stealing or

forging electronic signature codes, or using them without the authorization of their rightful owners.[24]

Finally, other forms of cybercrimes can be added, such as crimes promoting actions that violate values and ethics, as well as crimes of sexual exploitation of minors.

3.2 Elements of Cybercrime

Cybercrime is based on three elements, similar to other crimes. These are the legal element, which falls under the principle of the legality of the crime and its prescribed punishment; the material element; and the moral element.

A. The Legal Element

The legal element of a crime refers to the existence of a legal provision that criminalizes the act and specifies the punishment associated with it at the time the act occurs. This is referred to as the "principle of criminal legality," which means that there is no crime and no punishment without a legal provision.

Legal thought has settled on the necessity of having specific legal provisions to address cybercrime, especially with the emergence of the internet, which has dangerously contributed to the spread of such crimes. This was reflected in the European Council's adoption of recommendations in 1989, urging member states to adopt specific penal provisions for cybercrime.

As for comparative legislation, the United States is among the pioneering countries that enacted several laws in different stages in response to the rise of cybercrime. Among these laws was the one issued in 1976 for the protection of computers and networks, followed by another law in 1986 that defined all the necessary terms for applying crimes related to information systems and networks.[25]

The French legislator also enacted a specific law regarding cybercrime in 1988, which was incorporated into the Penal Code under the title "Crimes in Information Materials."[26]

As for the Algerian legislator, it first addressed cybercrime in 2004 through Ordinance No. 04-15, which amended the Penal Code under the title "Violation of Automated Data Processing Systems.[27]" However, due to

the development and seriousness of cybercrime, the legislator issued a specific law concerning this type of crime, namely Law No. 09-04, which sets forth the special rules for preventing and combating crimes related to information and communication technologies.[28]

B. The Material Element

The material element in any crime is represented by the criminal act or behavior carried out by the perpetrator to commit the crime. However, determining the material element in cybercrime poses several challenges due to the nature of the crime and the environment in which it is committed, specifically the technical domain. [29]In addition, it is difficult to determine the criminal result and the causal link between the criminal behavior and the crime's outcome.[30]

The material element in cybercrime consists of acts such as embezzlement, fraud, and theft committed against the physical components of an information system, including devices and their accessories, as well as data stored on physical media, such as disks and tapes, which are transferred or seized without the original owner's authorization. Furthermore, the criminal behavior in cybercrimes is related to the information stored in a computer or the violation of an individual’s privacy. The criminal behavior is realized by simply pressing a button on the computer, which can destroy the information system, commit forgery, or steal data, such as when infiltrating a bank's customer account system.

As for determining the result arising from the criminal behavior and the causal link between them in crimes committed over the internet, this is a complex issue due to the intricacies of computer technology and the internet network, as well as the diversity of communication methods available on the network. Also, considering the multiple stages that commands go through in computer systems to ultimately achieve the desired result, all these factors make it difficult to identify both the result and the true cause(s) linked to it.[31]

Third: The Mental Element

The essence of this element lies in the principle that "no one can be punished unless they have committed the act with intent and conscious

will." It is not sufficient for a crime to exist legally based merely on the physical element; these unlawful physical acts must stem from a free and conscious will, fully aware of the gravity of the crime, and must be morally linked to the act in a way that allows us to say that the criminal act is the result of free and conscious will.

Referring to Algerian legislation, the mental element in various crimes affecting information systems takes the form of criminal intent, along with fraudulent intent. For example, the act of accessing, staying in, or attempting to access or stay in any part of an automated data processing system with fraudulent intent constitutes the mental element of the crime. Similarly, the mental element of such crimes exists in cases where data is entered, removed, or modified in an automated processing system with fraudulent intent. Additionally, some types of crimes related to information systems require the mental element to involve criminal intent, as well as fraudulent intent, as stipulated by the Algerian legislator.[33] Cybercrimes are considered intentional crimes, requiring the presence of general criminal intent, which consists of two main elements: knowledge and will, i.e., the intent of the perpetrator.

4. CONCLUSION

Through the study of this topic, it is clear that cybercrime is one of the most dangerous crimes committed using electronic means, resulting in damage with multiple dimensions, considering its nature and the characteristics that distinguish it. At the end of this research, we present the most important findings and proposed recommendations as follows:

First - Findings:

1. Detecting cybercrime and pursuing those who commit it is a difficult issue due to its connection with the information network.

2. Cybercrime differs from traditional crimes that occur in the physical world, as well as the difficulty of identifying the actions that lead to the commission of this crime and the difficulty in classifying them.
3. Weakness or limitation of legal, institutional, and even human resources dedicated to fighting and combating cybercrime.

Second - Recommendations:

1. Establish mechanisms for continuous training for security agencies and specialized groups in combating cybercrime.
2. Enhance cooperation and efforts between countries through a shared strategy to provide the necessary legal protection to face cybercrime.
3. Promote digital culture to combat and prevent cybercrime as a preventive tool.
4. Strengthen legal and judicial assistance between countries through international mechanisms that help define and limit cybercrime and impose appropriate penalties, especially as it is of a technical and evolving nature.

5. Endnotes

[1]Mahmoud Ahmed Abayneh,(2005) "Computer Crimes and Their International Dimensions," Dar Al-Thaqafa for Publishing and Distribution, Jordan, , p. 17.
[2] Younes Arab, (2002)"Computer and Internet Crimes," Abu Dhabi, p. 8.
[3] Chawki Mohamed."Essai sur la notion de cyber criminalité. 2006. P07.
[4] Naila Qura, (2004)"Economic Computer Crimes," Dar Al-Nahda Al-Arabiya, Cairo, Egypt, , p. 20.
[5] Mohamed Adel Rayan, "Computer Crimes and Data Security," Article published on the Algerian El-Nahar Channel website, Article 06.
[6] Mahmoud Ahmed Abayneh, Op. Cit., p. 19.
[7] Ghazi Abdul Rahman Hayan Al-Rasheed, (2004) "Legal Protection from Cybercrimes (Computer and Internet)", PhD Thesis in Law, Islamic University, Faculty of Law, Lebanon, pp. 108-109.
[8] Op. Cit, p. 112
[9] Naila Qoura, (2005) "Economic Cybercrimes: A Theoretical and Practical Study," Halabi Legal Publications, p. 32.

[10] Younes Arab, (2006) "Forms of Cybercrimes and Trends in Classifying Them," Legislative Development Workshop, Workshop on Developing Legislation in the Field of Combating Cybercrimes, Telecommunications Regulatory Authority, Oman, p. 06.
[11] Mahmoud Ahmed Abayneh, Op. Cit, p. 22.
[12] Saghir Youssef, (2013) "Crime Committed via the Internet," Master's Thesis in Law, Faculty of Law and Political Science, Mouloud Mammeri University, Tizi Ouzou, p. 14.
[13] Mohamed Obaid Al-Kaabi, (2008) "Crimes Resulting from the Illegal Use of the Internet," Dar Al-Nahda Al-Arabiya, Cairo, Egypt, p. 18.
[14] Op. Cit., p. 22.
[15] Dhiab Mousa Al-Badaina, (2006) "The Role of Security Agencies in Combating Cyber Terrorism Crimes," Kingdom of Morocco, p. 20.
[16] Nahla Abdelkader Al-Momani, (2008) "Cybercrimes," Dar Al-Thaqafa for Publishing and Distribution, First Edition, Amman, p. 51.
[17] Op. Cit, p. 54
[18] Mohammed Obaid Al-Kaabi, Op. Cit, p. 41.
[19] Khaled Mamdouh Ibrahim, *Intellectual Property Rights*, Al-Dar Al-Jami'ya for Publishing and Distribution, 1st Edition, Alexandria, Egypt, 2010, p. 36.
[20] Khaled Hamad Al- Hamadi, (2006) "Money Laundering Crime in the Era of Globalization," pp. 34-35.
[21] Mohammed Hussein Mansour, (2006) "Electronic Liability," Manashet Al-Ma'arif, Alexandria, Egypt, p. 149.
[22] Op. Cit.p164
[23] Op. Cit.p166
[24] Algeria is one of the countries that issued a law related to electronic signatures, which is Law No. 15-04 dated February 1, 2015, outlining the general rules concerning electronic signatures and certification, Official Gazette No. 06, issued on February 10, 2015.
[25] Mohammed Hussein Mansour, Op. Cit, p. 110.
[26] Mohammed Hussein Mansour, Op. Cit, p. 110.
[27] Ordinance No. 04-15, dated November 10, 2004, amends and supplements Ordinance No. 66-156, which contains the Penal Code, Official Gazette No. 71, issued on November 12, 2004.
[28] Law No. 09-04, dated August 5, 2009, contains the special rules for the prevention and combating of crimes related to information and communication technologies, Official Gazette No. 47, issued on August 16, 2009.
[29] Mohammed Hussein Mansour, Op. Cit, p. 115.

[30] Mansour bin Saleh Al-Salmi (2010), The Civil Liability for Privacy Violations in the Saudi Cybercrime Law, Master's Thesis in Criminal Justice, Naif Arab University for Security Sciences, College of Graduate Studies, Riyadh, , p. 76.
[31] Op. Cit, p. 78
[32] Mohammed Hussein Mansour, Op. Cit, p. 117.
[33] Look at Articles: 394 bis, 394 bis 1, 394 bis 2, Algerian Penal Code.