ELWAHAT Journal for Research and Studies
Available online at:https://www.asjp.cerist.dz/en/PresentationRevue/2

ISSN : 1112-7163 E-ISSN: 2588-1892 Volume (18)/Issue (2) (2025):488-505

The Crime of Cyber Piracy in Algeria

Bouguetof Behdjet

University of Larbi Ben M'hidi, Oum El Bouaghi (Algeria), Laboratory of Legal and Political Studies, bouguetofbahdja@gmail.com

Received: 31-08-2025 Accepted: 10-10-2025 Published**:** 01-12-2025

Abstract:

Cyber piracy is considered one of the modern crimes due to its close connection with the technological and digital developments currently witnessed worldwide, which have facilitated and accelerated the circulation of information and data. Cyber piracy constitutes an act of trespass and aggression against such information and data. Given its particular nature and seriousness, the Algerian legislator has sought to confront this crime by enacting a set of laws aimed at combating and limiting its spread.

Keywords: Algerian law, combating, crime, cyber piracy, sanctions

1. Introduction

It is clear that modern technology, which is shown by the widespread use of advanced computers, sophisticated software, and communication networks, has brought millions of people closer together. It has made it easier to get and share information, to the point where our time is often called the "Age of Information." But this technology has also had bad effects, in addition to the good ones. One of the worst things about advanced technology is that it leads to computer-related crimes. These crimes attack important values that affect people, organizations, and governments in areas like security, culture, and the economy. They have also made people feel unsafe and untrustworthy, which is a threat to their safety and health.

This study is particularly significant due to the increasing diversity in the methods of execution of such crimes and the escalating severity of associated risks and losses. They are now a major threat to the economy and national security, especially in countries where technology in general and information technology in particular are very important to their interests. The world has moved to an information-based economy that depends on knowledge and

Corresponding Author: Bouguetof Behdjet, bouguetofbahdja@gmail.com

communication instead of just labor and people since the start of the information age. For instance, banks and other financial institutions now rely almost entirely on automated systems to run their businesses and keep track of their money. The same goes for people's privacy, financial integrity, and intellectual property. Because of this, these crimes have gone from being one-time attacks on the security of systems, networks, and data to a widespread problem that many people with the technical skills to use computers, run software, and navigate communication networks are getting involved in.

Algeria has always been one of the countries most affected by cyber piracy. In 2022, it was the third best in the Arab world and the 24th best in the world. By 2024 (Ministry of Post and Telecommunications, 2025), it had moved up to 19th place in the world.

The term "cyber piracy" itself may be unclear, especially since the word "piracy" used to mean people who attacked ships at sea to steal their money. In the field of information technology, however, the word has taken on a new meaning: it now means copying, taking, or using works or information without the owner's permission and without paying the rights owed. (Khalifa, 2009).

Cyber piracy crime or information technology crime is what computer crime used to be called. Back then, the only tool used was a computer. This change in language shows how electronic tools like smart computers, smartphones, electronic cards, and other advanced technologies have grown.

The treatment of this subject may be framed around the following central problem:

- What is meant by Cyber Piracy crime?
- What extent are the legal provisions in Algeria effective in combating it?

Since cyber piracy is so different from other types of crime, especially in terms of its ideas and terms, we need to start with a basic study that explains this new type of crime and what it is. Next, we will talk about two main things: first, the parts and methods that make up cyber piracy, and second, the Algerian legislator's point of view and the legal principles that Algerian law is based on. For this purpose, the following outline is suggested:

1. Definition and Characteristics of Cyber Piracy Crime:

1.1 Definition of Cyber Piracy crime:

It is challenging to create a complete and clear definition of computer-related crimes because they do not fit neatly into any one category (Shawa, 1994, p. 5). This difficulty arises from their ongoing evolution, the variety of methods used in their execution, the incessant emergence of new forms, and the diverse perspectives from which scholars and practitioners strive to delineate them.

These definitions may be classified into four principal approaches:

1.1.1. Based on the means of committing the crime:

Supporters of this approach base their definition of computer crimes on the means of committing the crime, requiring that the crime be carried out through the computer.

The jurist Tiedeman defines computer crimes as: “All forms of unlawful (or socially harmful) conduct that are committed through the use of a computer.”

Similarly, Tom Forester defines them as: “A criminal act carried out using the computer as the principal instrument.”

Both definitions necessitate the utilization of a computer as the principal method of perpetrating the offense, thereby categorizing it as a computer crime.

1.1.2 based on the Object of the Crime

Proponents of this approach characterize computer crimes by stipulating that the computer itself must be the subject of the offense. In other words, the illegal act must be aimed at the computer or its system. Rosenblatt is one of those who hold this view. He defines a computer crime as "an illegal act aimed at copying, changing, deleting, or getting to information that is stored on or sent through a computer."

Dr. Huda Qashqoush embodies this viewpoint within Arab legal scholarship. She contends that computer crimes are offenses intrinsically linked to informatics (Qashqoush, 1992, p. 05). She says that these are basically crimes that hurt information assets, which include the computer's programs, hardware, and other parts.

1.1.3 Based on the Perpetrator’s Knowledge of Information Technology

This method uses a subjective standard, which means that the person who commits these crimes must know about computers and how to

use one. The act cannot be classified as a computer crime in the absence of this component of expertise.

For example, David Thompson says that computer crime is "a crime in which the perpetrator must possess knowledge of computer technology in order to commit the offense." In the same way, the jurist Stein Schiölberg defines it as "any unlawful act in which knowledge of information technology is essential for its commission, investigation, and judicial prosecution."

1.1.4 The Fourth Approach: Based on Multiple Criteria

Other scholars adopt a composite approach, relying on several criteria rather than a single standard. Multiple definitions have emerged under this perspective.

Cybercrime is defined as "any act or omission that infringes upon material or immaterial property, resulting directly or indirectly from the intervention of information technology," according to Belgium's 1982 response to the OECD's (Organization for Economic Cooperation and Development) questionnaire on computer fraud.

The French jurist Masse described it as: “Legal infringements that can be committed through informatics with the aim of financial gain.”

Based on what has been said so far, computer crimes can be defined as "any act or omission that violates intangible assets (computer data) as a direct or indirect result of the use of information technology".(Abayneh, 2004, p. 19).

1.2 Characteristics of Cyber Piracy crime

Modern criminal policy necessitates the identification of the unique characteristics of cyber piracy to distinguish it from other forms of crime. This is necessary to create the right laws to deal with these new crimes that have come up with the rise of electronic computing and other technological and intellectual advances in the modern world.

Cyber piracy shares some characteristics with other crimes, but it also possesses unique features of its own.

1.2.1 Shared Characteristics

One of the most important things about cyber piracy is how dangerous it is and how much damage it can do. Cybercriminals today often go after banks and other financial institutions because they rely almost entirely on electronic funds transfer systems (Abayneh, 2004, p. 19).

Cyber piracy also damages scientific, cultural, and economic systems, making it much harder for them to grow. It also has a lot of risks, like making people less trusting of technology, putting intellectual property at risk, and stopping people from being creative and coming up with new ideas.

1.2.2 Distinctive Characteristics of Cyber Piracy

Computers, software, and communication networks—particularly the Internet—have rendered intellectual production inherently global. Literary and artistic works are no longer confined within the boundaries of a single state; rather, they are accessible to, and benefit, humanity at large.

In a parallel manner, the illicit use of computers has emerged as a global issue. Cybercrimes transcend territorial borders. For instance, cyber piracy may occur when an individual unlawfully accesses computers located in another country or destroys data stored abroad. Consequently, an attack might originate in one state while producing effects in another (Abayneh, 2004, p. 20).

In this respect, cyber piracy bears resemblance to other transnational crimes, such as drug trafficking and money laundering. However, it differs fundamentally in that its commission does not necessarily require physical cross-border movement. Cyber piracy can be carried out remotely, from a personal computer or other electronic devices such as smartphones. By contrast, drug-related crimes inevitably involve the transfer of physical goods across state lines.

The commission of cyber piracy presupposes both access to a computer and the requisite proficiency in its use. The computer thus becomes an indispensable tool in the perpetration of the crime. Moreover, such offenses require considerable knowledge in technical and specialized domains, including programming, computer systems, and data processing. Research and statistical evidence suggest that the majority of offenders are highly skilled in information processing. In particular, the rapid advancement of software development has played a critical role in the proliferation of these crimes.

Scholars generally distinguish between two principal categories of offenders (Batali, 2005, p. 15):

- Amateurs (Hackers): This category consists of individuals who gain unauthorized access to computer systems, typically for personal reasons or to cause disruption. They often take pride in their computer science knowledge and their ability to infiltrate networks without formal guidance. Hackers are predominantly teenagers or young adults.
- Professionals (Crackers): This category is largely composed of individuals over the age of 25 who possess advanced knowledge of computing, high levels of technical skill, and

considerable intellectual capacity. Their actions reflect greater danger and more deliberate criminal intent than those of amateurs. Many crackers are employed in organizations heavily reliant on computer systems, which grants them continuous and privileged access to networks and sensitive data. Their professional experience and technical expertise enable them to perpetrate highly sophisticated and damaging cybercrimes ((Batali, 2005, p. 16).

2. Constituent Elements and Techniques of Cyber Piracy crime

Like any crime, cyber piracy must satisfy certain fundamental elements.

2.1 Constituent Elements of Cyber Piracy crime

2.1.1 The Legal Element

Legal thought has come to an agreement on the need to make specific laws to deal with cybercrime and electronic piracy, especially since the Internet has made these crimes more common. As a result, states have begun to write laws to control this new kind of crime. But they have had trouble figuring out how to legally define it and where it fits into the traditional criminal law system. This makes me wonder: where should these kinds of crimes be put, and what kind of crime should they be?

In this regard, diverse hypotheses and viewpoints have surfaced. Some contend that it can be assimilated into the current classifications of the penal code. Some scholars propose categorizing it as a crime against property, since both the tangible and intangible elements of computers can be regarded as "property." Others suggest that it should be classified as a separate and distinct category of cybercrime or information crime, due to its unique economic value and characteristics (Amal, 2005).

Some people think that each type of cybercrime should be linked to its closest equivalent in traditional criminal law. For example, they think that forgery of documents on a computer should be treated as forgery of documents in general, and that attacks on data should be treated as destruction of property.

Law No. 04-15 of 27 Ramadan 1425 (corresponding to 10 November 2004) made this type of crime officially recognized in Algeria. It changed and added to Ordinance No. 66-156 of 18 Safar 1386 (corresponding to 8 June 1966), the Algerian Penal Code. Article 12 of Law 04-15 says: "A new Section Seven bis is added to Chapter Three of Part Two, Book Three of Ordinance No. 66-156, entitled 'Attacks on Automated Data Processing Systems'.

Articles 394 bis to 394 bis 7 are included in this section. Law No. 24-06 of 28 April 2024 (Official Gazette No 30 of the People's Democratic Republic of Algeria, 2024) made the most recent changes to these rules. It changed Ordinance No. 66-156 of the Penal Code even more.

Terminology is a problem that keeps coming up in this field. Cybercrime is inherently technical, introducing concepts that are not part of traditional legal language, which makes it hard to understand.

Different legal systems have dealt with this issue in different ways. Anglo-Saxon legal systems typically utilize the approach of offering clear definitions of technical terms within the legislation itself (Amal, 2005, p. 32). In contrast, the French method gives the courts the job of figuring out and defining technical terms. The Algerian legislator has emulated the French model by abstaining from delineating these terms within the legislative text. Because technology in computing changes so quickly, the penal code can't keep up with it very well, so this method is thought to be better.

As mentioned earlier, Law No. 04-15 introduced Section Seven *bis* of the Penal Code, which specifically addresses attacks on automated data processing systems. This section criminalizes several acts, including:

- Unauthorized access, whether successful or attempted, to all or part of a data processing system;
- Aggravated offenses where such access results in the deletion or alteration of system data;
- The fraudulent input of data into a system, as well as the fraudulent deletion or modification of existing data;
- Attempts to commit any of the aforementioned crimes, in addition to conspiracies to carry them out.

It is evident from the foregoing that the Algerian legislator did not provide an explicit definition of cyber piracy within the Penal Code itself. However, Article 2 of Law No. 09-04 of August 5, 2009—establishing specific provisions for the prevention of crimes involving information and communication technologies ((Official Gazette No 47 of the People's Democratic Republic of Algeria, 2009)—offers a broader definition. It characterizes such offenses as "crimes committed or made possible by an information system or electronic communications network, including offenses against automated data processing systems as specified by the Penal Code."

Thus, although the law does not employ the term *cyber piracy* explicitly, the legal element of this offense is affirmed by its implicit

inclusion within the general definition provided by Article 2 of Law No. 09-04.

2.1.2 The Material Element

Cyber piracy offenses may take a variety of forms, depending on how unlawful acts are directed against information technology systems. According to the Penal Code, these acts can be summarized as follows:

Article 394 *bis* criminalizes unauthorized access to automated data processing systems. The offense consists of entering or remaining within such a system unlawfully. The aggravated form of the crime, set out in Article 394 *bis* 2, applies when such access results in the deletion or alteration of system data.

It is important to note that "access" does not imply physical entry into a location. Rather, it should be understood more broadly as the act of engaging with the system's logical or intellectual processes (Amal, 2005, p. 39). The legislator does not specify the means by which access may occur; hence, the offense exists regardless of the method used—whether direct or indirect. Common techniques include:

- Trap doors (backdoors): hidden pathways intentionally left by developers in software, later exploitable for manipulation, sometimes discovered during system maintenance;
- Dumpster diving: retrieving sensitive information from discarded materials;
- Shortcut methods;
- Disguise techniques (Rosé, 1992, p. 49).

The crime is committed whether access involves the entire system or only part of it. Breaking into even a small section is sufficient. The crime is also complete even if no further action is taken: the offender does not need to steal, use, or alter the information. Even if the perpetrator does not know how to operate the system, the crime is still established (Mahmoud, 2002, p. 36).

The material element of cyber piracy may also consist of unauthorized presence in a data processing system against the wishes of the legitimate controller. This can occur independently or in conjunction with unlawful entry (Mahmoud, 2002, p. 38) (Mahmoud, 2002, p. 38).

- Staying as an independent offense: This occurs when the initial entry is lawful (for example, by accident, mistake, or negligence). In such cases, the person must leave immediately. If they remain, they are liable for unlawful presence, provided the required intent exists.

- Remaining as an extension of unlawful access: If someone knowingly enters a system without authorization, that constitutes unlawful access. If they then begin moving within the system, the crime of unlawful presence starts at the moment of this exploration, since they remain inside despite knowing they should not.

For example, if someone is authorized only to view data but prints a copy, they commit the crime of unlawful presence. The same applies if they continue navigating the system after their authorized time has expired.

To commit this crime, it is enough to remain in the system, whether in whole or in part. The mere act of remaining inside fulfills the material element (actus reus) of the crime; theft of information or causing damage is not required.

Article 394 bis 1 criminalizes using fraud to input data into an automated data-processing system, or to delete or alter data already in the system.

There are three ways the crime of intentional interference with data can occur:

- Insertion
- Deletion
- Modification

It is not necessary for all of these forms to occur at once; committing any one of them is sufficient for the crime to be complete. Inputting, deleting, or modifying data all involve altering the contents of an automated data-processing system, either by adding false data or by removing or changing existing data. The crime, in this case, targets a specific object: electronically processed data or information. It applies not only to information yet to be entered but also to information already stored.

Placing data into a storage medium, whether empty or already containing data, is considered *inputting*. This occurs, for example, when the lawful holder of a magnetic withdrawal card uses it at an ATM by entering their private code to withdraw an amount greater than their account balance. The same applies when the lawful holder of a credit card uses it to make payments exceeding their authorized limit (Batali, 2005, p. 30).

More broadly, inputting occurs whenever a credit or debit card is used abusively, whether by the lawful holder or by another person who has stolen, lost, or forged the card (Jaddi, 2013, pp. 64-63).

Inputting also includes introducing a foreign program (such as a virus, Trojan horse, or logic bomb), thereby adding new data.

- Deletion means removing some of the data stored in the system, destroying the storage medium, or moving or saving data into a reserved memory area (Jaddi, 2013, p. 65).
- Modification means altering existing data by replacing it with new data. Malicious software designed to modify data often deletes or changes it in some way. These actions may include using a logic bomb, erasure software, or viruses.

Article 394 bis 2 criminalizes designing, researching, collecting, providing, distributing, or selling data stored, processed, or transmitted through an information system if that data could be used to commit any of the crimes listed in this section.

The same article also criminalizes possessing, sharing, publishing, or using data obtained through any of the crimes in this section, for any purpose.

2.1.3 The Mental Element

Fraudulent access to or presence within an automated data-processing system is only punishable when executed through deceit.

The crime of unauthorized access or presence is a deliberate act, and the mental element is criminal intent (dolus). Criminal intent consists of knowledge and will; for the mental element to be present, the offender's will must be aimed at accessing or remaining within the system, while simultaneously being aware of their lack of legal entitlement to do so.

Consequently, the mental element is lacking if the perpetrator's access to or presence within the system was permitted or otherwise lawful. It is also absent when the perpetrator operates under a misconception of fact, such as unawareness of an access limitation or the erroneous belief that access was allowed (Jaddi, 2013, p. 71).

When criminal intent is present—through the interplay of knowledge and will—it is not influenced by the perpetrator's motive. So, intent is there even if the only reason is to show off skill or prove that you can get around the system's defenses.

General intent is inadequate; a specific intent, specifically fraudulent intent, is necessary. This idea does not mean that someone wants to hurt someone else, because that would create a conflict between the material element, which does not require a harmful result, and the mental element (Rabhi, 2018, p. 167).

The concept of fraudulent intent as defined in legal doctrine and jurisprudence is as follows:

"When the agent knew they were acting without permission, were unauthorized, or were going against the owner's wishes, access or continued presence is fraud (Vivant, 1991, p. 1551)."

Fraudulent intent in instances of unauthorized access is generally inferred from the security mechanisms safeguarding the system, whereas fraudulent presence is derived from the activities performed within the system. It is important to note that fraudulent access or presence does not always mean that the security device was literally broken; instead, it is shown by the person staying in the system without permission. The security device is only proof that access was not allowed by law.

The crime of interfering with an automated data-processing system assumes that the person who did it wanted to either disrupt or corrupt the system. The perpetrator must also know that their actions will cause this kind of disruption or corruption and that they are doing it without the permission of the person who owns the system. This crime is therefore considered an intentional crime (Rabhi, 2018, p. 168).

However, just doing something on purpose isn't enough; there also needs to be fraudulent intent. This necessity stems from the inherent nature of insertion, deletion, and modification as fundamental components of legitimate information-processing activities. So, the crime only happens when these actions are done with the intent to commit fraud and are not allowed (Rabhi, 2018, p. 169).

2.2 Techniques Used in the Commission of Cyber piracy crime

Cybercriminals use a lot of different methods to commit crimes. The following account describes the most common ways to break into a system without permission and to commit sabotage and corruption.

2.2.1 Techniques for Unauthorized Access

Use of emergency bypass: programs Some visible programs are made to get around technical protection systems in case of an emergency. Data processing needs security features to keep people from getting into systems without permission. However, when computers break down, administrators may need programs that let them get around these security features to keep computers running and safe. SUPERZAP is a well-known example. It is used a lot in IBM computing centers and works like a master key, letting you into all parts of the system. If these kinds of programs get into the wrong hands, they can be very dangerous because they can let people get into

even the most secure systems and do things they shouldn't be able to do (Amal, 2005, p. 50).

- Trapdoors During: software development, programmers often leave hidden points of access called "trapdoors." These let them change or change the program later on. Many times, these trapdoors are used as a normal part of making final adjustments, but they can also be used to allow illegal manipulation.
- Searching through dumpsters: People who work in computing units throw away carbon papers, regular sheets with data on them, and even magnetic tapes. These can be found and used to get information that criminals can use (Amal, 2005, p. 51).
- The shortcut method: This technique exploits vulnerabilities within internal control systems.
- Disguise method: Here, the hacker deceives the computer into recognizing them as an authorized user.
- Asynchronous act: This method takes advantage of weaknesses inherent at the level of the operating system.

2.2.2 Techniques of Sabotage and Corruption

We shall attempt to address the most important and prominent of these techniques (Batali, 2005, p. 40):

- Changing the input This means putting wrong or misleading information into the system, sending valid data somewhere else, or both. The first step in processing data, preparing the input, changes the data into a form that computers can read. This makes it very easy to fake. By giving false information or leaving out some entries, criminals can change the results. People think that more than half of all cybercrimes happen this way.
- Changing programs Unauthorized changes can happen when software is regularly fixed or updated. These changes could hide scams, like stealing money. One example is the "rounding trick," where changes are made to make small amounts of money disappear in repeated transactions, which adds up to a lot of illegal money.
- Malware: Not long after computers became common, bad software started to show up. They come in many forms and serve many purposes, from fraud and stealing money to showing off technical skill. Trojan horses, logic bombs, worms, and viruses are some of the most dangerous.

- A Trojan horse: is a type of malware that looks like a useful program but actually has harmful commands hidden inside it. It may, for example, present itself as a utility for organizing or compressing files, while its hidden function is to delete those files or manipulate stored financial data. The Trojan horse first showed up in the US in the late 1970s, around the same time that electronic bulletin boards were becoming popular. One early version, called ZAXOON, looked like a game at first, but when you ran it, it wiped out system disks (Amal, 2005, p. 60).
- Another program called FILER seems to organize file data, but it actually deletes them. There are also hidden instructions in programs that send periodic checks by mail to beneficiaries, like pensioners. These hidden instructions change the notification that is entered into the computer about the death of a beneficiary, which would normally stop the issuance of more checks. Instead, the instructions change the beneficiary's address for three months in a row. During this time, the computer keeps sending checks to the fake address. At the end of this time, the hidden instructions bring back the original data, including the notice of the beneficiary's death. This makes it very hard to find
- Logic or Time Bombs: Logic bombs, also known as time bombs, are programs designed to remain hidden and inactive for long periods, sometimes even years. They are usually triggered by a time flag, such as a specific date, after which the program activates and causes destruction (Amal, 2005, p. 65).

There are also worm and virus programs written in a way that allows them to control other programs (Batali, 2005, p. 68).

3. Combating Cyber Piracy in Algerian Legislation

This section addresses Algerian laws for dealing with and combating cybercrime. It focuses on the penalties provided in the Penal Code (as amended by Law No. 24-06) and in intellectual property law, since data is treated as intellectual property and therefore protected under that law.

3. Combating Cyber piracy crime in Algerian Legislation

This section talks about the laws in Algeria that deal with and fight cybercrime. It focuses on the punishments that are set out in the Penal Code (as changed by Law No. 24-06) and in intellectual property law.

This is because data is considered to be intellectual property and is therefore protected by that law.

3.1 Penalties for Cyber piracy crime under the Algerian Penal Code

Proofread Version

Law No. 04-15 adds a new Section Seven bis to Book Three, Chapter Three, Title Two. "Offenses against Automated Data Processing Systems" is the name of this section. It has Articles 394 bis to 394 bis 7 and lists punishments like jail time and fines.
The most recent change, Law No. 24-06, made these punishments worse. Article 394 bis says that anyone who illegally accesses or stays in an automated data-processing system, in whole or in part, or tries to do so, will be punished with six months to two years in prison and a fine of 60,000 to 200,000 Algerian dinars (DZD). Before this change, the penalties were a fine of 50,000 to 100,000 DZD and three months to a year in prison.
Law No. 24-06 says that if someone commits fraud by deleting or changing system data, they can go to jail for one to three years and pay a fine of 100,000 to 300,000 DZD. If these actions stop the system from working, the same punishment applies.
Anyone who fraudulently adds, deletes, or changes data in an automated processing system can be sent to prison for one to three years and fined between 500,000 and 2,000,000 DZD, according to Article 394 bis 1.
Article 394 bis 2 goes even further. It says that anyone who intentionally and fraudulently designs, researches, collects, provides, distributes, or sells stored, processed, or transmitted data through an information system can get one to five years in prison and a fine of 1,000,000 to 5,000,000 DZD. This applies because the data could help people commit the crimes listed in this section.
If you have, share, give away, or use data that you got from these crimes, the same punishments apply. Law No. 24-06 raised the minimum and maximum penalties by a lot. The minimum prison sentence went from two months to one year, and the maximum fine went from 1,000,000 DZD to 5,000,000 DZD.
If the crime is against national defense or public institutions that are subject to public law, the penalties are even worse. This does not prevent the imposition of harsher penalties when warranted. Article 394 bis 4 says that if a legal person (like a corporation) breaks these

rules, they will have to pay five times the maximum fine that a natural person would have to pay.

The law also punishes people who take part. Article 394 bis 5 says that anyone who helps plan one or more of these crimes with other people will get the same punishment as the crime itself, as long as the planning is shown by actions.

Article 394 bis 6 says that the tools, programs, and devices used to commit the crime can be taken away and the websites used for the crime can be shut down. If the owner of the property where the crime happened knew it was being used illegally, they may also be ordered to close the premises, as long as the rights of third parties acting in good faith are respected.

Lastly, Article 394 bis 7 says that attempts to commit misdemeanors under this section are punishable in the same way as completed offenses.

Law No. 24-06 made the punishments much worse, that's for sure. The amendment made prison sentences and fines higher than they were before. The reason for this rise is the sharp rise in cybercrime and the fact that earlier punishments weren't enough to stop the quick spread of these crimes.

3.2 Combating Cyber Piracy under Algerian Law on Literary and Artistic Property

The Copyright Law protects computer software by explicitly listing it as one of the protected works. Thus, infringing the economic or moral rights of a software author constitutes counterfeiting.

In this regard, the Algerian legislator, through Ordinance No. 03-05, explicitly acknowledged in Article 151 the crime of counterfeiting, which can appear in three main categories:

3.2.1 Offenses Related to the Author's Moral Rights

- Unlawful disclosure of a literary or artistic work (Article 22, Ordinance No. 03-05).
- Violation of the integrity of a literary or artistic work (Article 25, Ordinance No. 03-05).

3.2.2 Offenses Relating to the Author's Economic Rights

- Reproduction of a work in any form, such as making counterfeit copies. This type of offense is the most common in the digital world, particularly regarding the copying of computer programs.
- Unauthorized communication of a work: anyone who shares a work or artistic performance with the public through representation, public performance, audiovisual broadcasting,

distribution, or by transmitting signals carrying sounds, images, or both, or through any information system, commits the crime of counterfeiting.

3.2.3 Offenses Analogous to Counterfeiting

These include:

- Importation or exportation of counterfeit copies.
- Sale of counterfeit copies of a work (program).
- Rental or circulation of a counterfeit work (program).
- Assisting or participating in violations of the author's rights, as well as willfully failing to pay the author royalties owed under the law.

It is evident from these three categories that counterfeiting is a violation of the author's economic or moral rights without their consent. Moreover, criminal intent in counterfeiting is presumed.

A. Infringement of Economic Rights

- Violation of the Right of Reproduction (Articles 41, 46, 53, and 54 of Ordinance No. 03-05): Reproduction of a work means exploiting it, in its original or altered form, by fixing it on any medium or by any process that allows communication of the work and the creation of one or more copies, whether of the entire work or part of it. Reproduction rights therefore cover a broad scope, both regarding what is reproduced and the method used. A computer program may be included in the copied work.
- Violation of the Right of Communication to the Public (Article 150 of Ordinance No. 03-05): When communication occurs outside the family, it is considered "public." The right of communication covers all forms of communication, direct or indirect, including through fixations such as discs, films, or video recordings.
- Violation of the Right to Modify the Program: This refers to the author's exclusive right to use their work and authorize derivative works, such as adaptations, translations, or modifications (Mohieddine, 2007).

B. Infringement of Moral Rights

- Violation of the Right of Disclosure: The author of a program has the exclusive right to decide when and how it will be made public. Any unauthorized disclosure constitutes a violation.

- Violation of the Work's Integrity: The law protects the author's right to preserve the integrity of their work. If someone alters, transforms, deletes, or adds to the program without the author's permission, this constitutes infringement.

Any of these acts constitute the criminal conduct required to establish the offense of counterfeiting.

4. Conclusion

The examination of this topic leads to the conclusion that electronic piracy is distinct from other criminal behaviors due to its unique legal characteristics. This specificity arises from the fact that the safeguarded interest is information itself, the legal classification of which remains disputed. A lot of legal doctrine says that information can't be seen as having a material nature; instead, it recognizes that information is intangible. So, the kind of legal protection it gets must be different from the kind that applies to things that can be touched.

References

1. Abayneh, M. A. (2004). Computer crimes and their international dimensions. Dar Al Nashr.
2. Amal, Q. (2005). Cybercrime (Master's thesis in criminal law and criminal sciences). Algeria.
3. Batali, G. (2005). Cybercrime: A comparative study. Algiers: Algerian Publishing House.
4. Jaddi, N. (2013). Offenses affecting automated data processing systems (Master's thesis, Faculty of Law, University of Mentouri Constantine). Algeria: University of Mentouri Constantine.
5. Khalifa, M. (2009, September 15). The specificity of cybercrime and the efforts of the Algerian legislator in confronting it. Studies and Research, 1(1), 370–389.
6. Mahmoud, A. H. (2002). The theft of information stored in the computer (2nd ed.). Cairo: Dar Al Nahda Al Arabia.
7. Ministry of Post and Telecommunications. (2025, August 21). Official website of the Ministry of Post and Telecommunications. Retrieved from http://www.mpt.gov.dz
8. Mohieddine, O. (2007). Copyright in light of the new Algerian law (2nd ed.). Algiers: University Publications Office.
9. Official Gazette No. 30 of the People's Democratic Republic of Algeria. (2024). Official Gazette. Algiers, Algeria: Government Printing Office.

10. Official Gazette No. 47 of the People's Democratic Republic of Algeria. (2009). Official Gazette. Algiers, Algeria: Government Printing Office.
11. Qashqoush, H. H. (1992). Computer crimes in comparative legislation. Cairo: Dar Al Nahda Al Arabia.
12. Rabhi, A. (2018). Informational secrets and their criminal protection (Doctoral thesis, Faculty of Law and Political Sciences, University of Aboubekr Belkaid Tlemcen). Algeria: University of Aboubekr Belkaid Tlemcen.
13. Rosé, P. (2005). Computer crime on the horizon: Prospective analysis. Paris: L'Harmattan.
14. Shawa, M. S. (1994). The information revolution and its impact on criminal law. Cairo: Dar Al Nahda Al Arabia.
15. Vivant, M. (1991). Computer property items subject to fraud. In M. Vivant, Informatics and criminal law. Paris: Lamy Informatique.