

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

**Confronting cybercrime through money crimes stipulated in the
Algerian Penal Code**

T.D.: si Abdel Qader Hanan*

Faculty of Law and Political Sciences in Sousse, (Tunisia)

toufik.khadidja82@gmail.com

Date of send: 03 / 06 / 2024	date of acceptance: 01 / 08 /2024	Date of Publication: 01/09/2024
------------------------------	-----------------------------------	---------------------------------

* **Corresponding author**

Abstract:

Information and communications technology has brought about a comprehensive revolution in all aspects of life, and the dominance of information and communications technology in the general way of life has increased. The emergence of the computer and the expansion of the use of the Internet in various areas of life has led to the emergence of some negative effects and risks resulting from this great expansion, as the greater the dependence As these technologies develop, the risks related to Protecting information have increased, and with the increasing global dependence on information and communications technology, exposure to cybercrimes has also increased. As cyberspace has become vulnerable to violations by network hackers, whether they are countries or others that possess these information technologies, attention has been drawn to cybersecurity, and preserving it has become a matter of preserving the national security of countries.

Keywords: For electronic crime; computer; information criminal; Money.

introduction:

The emergence of informatics and its multiple applications led to the emergence of new legal problems, that is, the emergence of the so-called crisis of criminal law in the face of the reality of informatics. Its solution required research into the existing legal conditions and their suitability to confront these problems, and since the criminal judge was restricted, when considering the criminal case, to the principle of the legality of crimes, He will not be able to criminalize acts not stipulated by the legislator, even if they are reprehensible acts and of a high level of criminal danger..

To what extent is it possible for the judge to use the traditional penal code to provide protection for this new economic value, which is automated media money, in light of the traditional texts? Especially since the legislator did not have in mind at the time of drafting the traditional texts this type of new investment, and here lies the danger of the attempt because the criminal law has its principles and origins, most important of which is the principle of legality, from which branch the principles of narrow interpretation and the danger of analogy in the field of criminalization.

The problem at hand is: Can the criminal judge, through the current texts for money crimes, achieve criminal information protection without overthrowing the established principles on which the criminal

law is based? For this purpose, we decided to focus our study on two main points:

- 1- The extent to which information technology is considered a subject of money crimes.
- 2- The extent to which information technology is subject to criminal activity for money crimes.

First: The extent to which information technology is considered a subject of money crimes:

To determine the extent to which attacks on automated media funds can be subjected to the traditional texts of money crimes, it is necessary:

➤ **The extent to which the description of money applies to informatics:**

Information money means the computer with all its components. It is a group of entities that allow information to be entered, processed, stored and retrieved upon request. It consists of two entities::

-A physical entity

-A moral entity

The physical entity includes various physical devices, which are the input device, the output device, and the central operating units through which information is processed, stored, and output. As for the moral entity, it includes the various programs through which the computer performs its various functions, in addition to the information that actually needs to be processed¹

If the physical devices of computers do not need special texts to protect them criminally, as they are included in the texts of traditional crimes, then the matter is different with regard to the moral entity of those computers, because crimes of assault on funds usually require that their subject be something physical, and the nature of the moral entity is not like that, and therefore the question arises about the extent of its consideration. The moral entity of the computer is money.²

Money is everything that is suitable to be the subject of a right that has financial value, and the thing is the subject of the right. Things are divided into material things and non-material or moral things, noting that money from the traditional point of view does not relate to material things. This is why the definition of money in relation to money crimes is: "Every material thing is suitable to be the subject of a financial right."³

But with development, intangible things increased in number and some of them surpassed material things in terms of their value, which

necessitated searching for another criterion other than the nature of the thing to which the financial right is attributed, so that the quality of money could be given to the intangible thing.

Among these intangible things of high economic value are computer programs - these programs are usually installed on a support or standSUPPORT- Such as disks or magnetic strips made of plastic, cardboard, or any other material.

The program, which is independent of its support, is indisputably an intangible thing, and therefore it cannot be described as money according to the traditional definition of money, which requires that its object be a material thing. However, if the program is recorded or engraved on its support, then that support, with the programs on it, is suitable to be the subject of money crimes. Although the pillar is separate from the program, it is considered of little value when compared to the value of the program, and despite the fact that attacking it is not an end in itself, rather the motive for doing so is the program itself, not its pillar. However, these motives have no effect in criminal law.⁴

In this case, the attack on the support is considered to have occurred on a material thing, which can be classified according to the criminal activity as one of the money crimes whose model matches this activity. However, if the attack on the program occurred independently of its support, the matter is different as it may have occurred on an intangible thing. This The intangible thing must first be proven as money so that the possibility of money crimes being committed against it can then be investigated.

In this regard, jurisprudence has divided into two directions:

The first trend: the jurisprudence that supports adding the description of money to the program

A part of jurisprudence believes that information is valid to be subject to attack as long as this information reflects the personal opinion of its owner and does not stop at the scope of general information, on the basis that this information is issued by its owner, meaning that it is linked to his personality and he is the one who thought about it, or this means that it is from Rights related to the personality of its owner, and this information itself is the subject of this right, and one of its characteristics is the ability to transfer it. This means that there is another party who receives this information, and from here relationships are established either between it and its owner or between

its owner and others. Information, as a mental product of the one who gives it the form of information, is considered the focus of Relationships such as those that arise between the owner and what he owns, in which he has the right to transfer, deposit, preserve, rent, and sell them. An example of this information is computer programs, as these programs grant rights to their owner and authorize him to conclude contracts related to them, such as rent, sale, preservation, and any other form of exploitation, because one of their characteristics is transferability.

All of these actions and rights are what prompted some parts of jurisprudence to say that information is money, not only because there is a relationship of special exclusive rights over it, but also because it is considered an economic value. It is put on the market for trading, just like any commodity, and it has a commercial market that is subject to the laws of the economic market.

If traditional jurisprudence excluded information from the category of money on the basis that it is immaterial, meaning that the immateriality of information is what led to it not being recognized as money, modern jurisprudence sees, on the contrary, that the criterion for considering a thing as money is not on the basis of its being a physical entity, but rather On the basis of its economic value, and that a law that refuses to give the character of money to something that has economic value is indisputably a law that is completely divorced from reality.⁵

As long as programs, at their core, are information processed in some way and have economic value, they should be treated as money ⁶.whatThis meaning confirms that the modern legislator recognizes to the owner of this information what is called the right to intellectual property, and had the information not been property, the legislator would not have been able to grant this right to her, even if the nature of this ownership is the subject of jurisprudential controversy.⁷.In any case, it is a type of ownership or right that gives its owner the right to monopolize the exploitation of this intangible property, that is, information, including computer programs.

- The second trend: the jurisprudence opposing adding the description of money to the program

The other side of jurisprudence believes that information is not valid to be subject to attack, as one side of jurisprudence in France held that information in its abstract state and the idea in itself do not accept ownership and exclusivity, and that its circulation and benefit from it is

the right of all without discrimination and therefore cannot be the subject of intellectual property⁸.

Others differentiate between information and data that has been processed electronically, seeing that the former, given that its basic element is the meaning and not the pillar that embodies it, has an immaterial nature and there is no way to misappropriate it. As for the data that has been processed electronically, it is identified in a physical entity represented by pulses or signals. It is magnetic and can be stored on certain media, transmitted, exploited and reproduced, in addition to the possibility of quantifying it and measuring it. Therefore, it is not a moral thing like rights, opinions and ideas, but rather something that has a material existence in the external, tangible world. According to this view, if information is not processed automatically by a computer, it is not considered money. Subject to criminal protection, given that this processing takes place in the form of electronic pulses, which can be said to mean that for this processing process, it transforms moral funds into material funds, which subjects it to the traditional texts of money crimes, and takes the same ruling as data stored whether in computer programs or in its memory, and thus It takes computer programs, data, and money on it, and thus enjoys the criminal protection assigned to it.

Considering information as property that can be owned or exploited, as we previously explained, removes a major obstacle before us. Possession. This type of money is part of the group of funds protected by the criminal law, which is that the money that is the subject of crimes of assault on funds must be a movable property owned by others. It can be protected by traditional texts on the basis that these texts are general and do not require that money crimes occur against Material movable. Therefore, it is conceivable that these crimes occur in a non-material sphere as long as their quality of money and ownership is recognized. The French Court of Cassation has followed this trend in many of its rulings.^{9.1-2} The extent of computer programs based on this characteristic under the concept of something that is suitable as a subject for money crimes?

➤ **The extent to which information technology is considered money in relation to money crimes:**

We mentioned in the previous section that computer programs, according to the prevailing jurisprudence, are described as money. If the information is a movable thing and not owned by others, but it is an

intangible thing, are programs based on this description included under the concept of a thing that is suitable as a subject for money crimes?

A / The extent to which the program is considered money in connection with the crime of theft:

According to Article 350 of the Algerian Penal Code, “Anyone who embezzles something that does not belong to him is considered a thief.” The text of Article 350 does not explicitly stipulate that the property subject of the crime must be physical, which makes the occurrence of the crime of theft on intangible property a matter that does not conflict with the principle of the legitimacy of crimes and punishments.

This opinion finds its justification in the fact that the thing that is the subject of theft, as described by its model in Algerian legislation, is not limited to the use of the word without an adjective or specification only to physical, embodied things, but also includes intangible things as well, and this is the most likely interpretation in jurisprudence, but considering the program as a subject of theft remains inconclusive and valid. Only the door of possibility.

B/ The extent to which the program is considered a source of fraud:

According to Article 372 of the Algerian Penal Code, “Anyone who obtains or receives money, movables, bonds, transactions, securities, promises, releases, or a release from obligations, or to obtain any of them, or attempts to do so, and this was done by fraud in order to plunder all the wealth of others.” Or some of them, or initiating them, either by using false names or descriptions, or imaginary authority, or imaginary financial credit, or by creating the hope of winning anything, or in a severe event, or any other imaginary event, or fearing that any of them will occur, shall be punished with imprisonment for a period of at least one year to a maximum of five years. And a fine of 500 to 20,000 DZD.”

We conclude from the text of Article 372 that not every material and movable thing is suitable to be the subject of the crime of fraud, but rather it must be among the things exclusively enumerated in Article 372.

It should be noted that the text on movable material was mentioned without specifying its nature and without the legislator restricting it to be material, which allows this text to be interpreted in a way that allows computer programs to be included among the things on which the crime of fraud is committed. However, even if we take this interpretation, we are faced with the lack of tangible material activity. It is delivered and

received, and even assuming that the delivery has taken place, the victim is not deprived of possession of the program and data that remain under his complete control.

C/ The extent to which the program is considered a subject of the crime of breach of trust:

According to Article 376 of the Algerian Penal Code, “Anyone who embezzles or dissipates in bad faith commercial papers, money, goods, securities, receipts, or any other documents containing or proving an obligation or release that were not delivered to him except by way of authorization, deposit, agency, or Mortgaging or unusable property, or to perform work, whether paid or unpaid, on the condition that it be returned or presented, or to use it, or to use it in a specific work, and that is to the detriment of its owners, those who seized it, or those in possession of it, is considered to be committing the crime of breach of trust.....”

It can be concluded from the text of Article 376 that embezzlement occurs on movable property delivered to the offender pursuant to a contract of trust, and therefore the crime of breach of trust does not occur on property other than material movable property.

Article 376 specifies the things that are suitable as a subject for this crime, which are, but are limited to, commercial papers, money, goods, securities, receipts, and documents that contain or prove a commitment or release. Accordingly, subjecting attacks on informational property to the provisions of breach of trust raises some legal problems due to their nature. Immaterial values in the field of information crime.

The only solution is to imitate what the French judiciary has adopted as some values in the information field, such as (goods), that is, expanding the concept of goods. Accordingly, the application of the breach of trust provisions in the information field is within a limited scope and only as a matter of possibility.

D/ The extent to which the program is considered a subject of the crime of destruction:

According to Article 407 of the Algerian Penal Code, “Anyone who deliberately vandalizes or destroys the property of others stipulated in Article 396 by any other means, in whole or in part, shall be punished with imprisonment from two to five years and a fine from 500 to 5,000 DZD.”

Article 412 of the Algerian Penal Code also stipulates: “Anyone who intentionally destroys goods, materials, engines, or devices, whatever

they are, used in industry, by means of destructive materials or by any other means, shall be punished by imprisonment from 3 months to 3 years and a fine from 500 DZD to 5,000 DZD.”

Referring to the text of Article 412, we find that it specifies the things subject to destruction, and therefore it includes the physical components of the computer, whether as devices or goods. Also, a logical entity can be subject to this criminal text as money due to its economic value.

Second: The extent to which information technology is subject to criminal activity for money crimes:

What is being researched is the extent to which computer programs or information in general are subject to criminal behavior through which the material element of the crimes of theft, fraud, breach of trust, and destruction is achieved.

➤ **The extent to which information technology is subject to criminal activity in the crime of theft:**

With regard to the criminal activity that constitutes the crime of theft, which is embezzlement, and its application to computer programs or processed information in general, we note that even if the perpetrator is responsible for the programs that he seized, he does not remove these programs from the responsibility of their legitimate owner, as they remain despite his direct actions. Embezzling them under the latter's control without detracting from their content. It is also noted that the appropriation of programs as information can only be imagined at first glance as a transfer of this information from mind to mind or from memory to memory.¹⁰ This is a second obstacle. Thirdly, it should be noted that the information contained in the programs is of a non-material nature, that is, it is a moral thing. How can it be imagined that the embezzlement, which is of a material nature, would respond to something moral, and this is a third obstacle. As a result of these obstacles, it is not easy to apply theft provisions to computer programs, especially in the following cases:

A/ Theft of information through illegal copying of electronically stored data:

That is, by reproducing the document or the support it contains, in an attempt to apply theft provisions to cases of illegal copying. We can adopt the findings of French jurisprudence in this regard by explicitly declaring that the information that was copied or reproduced is the one that was stolen, and it did not deviate from the principle of legality. Moreover, the ruling's acknowledgment of the misappropriation of

information by reproducing the document that contains it carries within it a hidden but profound wealth because it allows punishment for reproduction that cannot fall under the penalty of the crime of imitation. It should be noted, however, that the crime of stealing information through illegal copying should not be confused with the crime of imitation, because theft contains data in itself, while the protection that the legislator guarantees to works by criminalizing their imitation is focused on the way of expressing the author's ideas.¹¹.

B/ Stealing machine time:

Criminal law jurists consider it the theft of use, and in this case it is not easy to extend the provisions of the crime of theft to machine time because the Algerian legislator does not accept what is called the theft of service, and therefore it requires legislative intervention similar to what the French legislator did by criminalizing the illegal presence in the system of automated data processing. Although this crime aims primarily to directly protect the automated data processing system, it also indirectly achieves protection of the information itself.

C/ Mental capture of data:

For example, a person captures information that appears on a computer screen and saves it and stores it in his memory. This behavior could be embezzlement even though he did not respond to the material of the document. Rather, the embezzled thing was limited to the content of the document while it remained in the possession of its owner, because this content is a movable thing owned by an exclusive third party. In the benefit of the document as part of its owner's right to ownership, however, the Algerian legislator does not consider theft of use and therefore there is a need for legislative intervention that includes both cases of mental capture of data and the case of theft of data without copying it and without compromising its integrity or authenticity.¹²

D/ Adapting aerial capture of electronically processed or transmitted data:

It is known that energy and natural or industrial forces are considered transferable property and are suitable for theft. However, we cannot apply the provisions of energy theft to the radiation, waves and pulses emitted from the computer during its operation, even though they are electrically measurable, quantifiable and of value.¹³

For this reason, we conclude that theft did not occur in the previous cases because the nature of the programs and information prevents taking or embezzlement in its precise sense recognized in the crime of

theft, which means seizing full possession of the thing without the consent of its owner or previous possessor. Because if we imagine the embezzlement occurring through copying or photocopying the information, then This same original information remains at the same time as it was before under the control of its original owner and does not go out of his possession, and since the Algerian Penal Code does not criminalize the theft of use in general, the only way out is only with explicit intervention by the legislator, to avoid controversy over the theft of information and theft. Machine time or theft of the use of the asset and achieves direct protection of programs and information.

- The extent to which computer programs are subject to criminal activity in crimes of fraud, breach of trust, and destruction:

A/ Implementing the criminal activity of the crime of fraud in the information field:

We find that if the perpetrator resorts to one of the fraudulent methods and forces the victim to hand over to him a material support with a program installed on it and then the perpetrator takes possession of it, the criminal activity in the fraud crime is achieved. But is it conceivable that the criminal activity of the fraud crime is achieved through the fraudulent methods that the perpetrator resorts to, which Does it result in the victim making a mistake that leads him to convey to him orally, that is, by saying, the contents of his program, which the offender picks up and stores in his memory?

Is transfer by word equivalent to extradition based on a mistake stipulated in Article 376 of the Penal Code? Is the perpetrator's capture or hearing of information equivalent to seizure?

There is no physical activity through which the delivery and receipt is achieved in the crime of fraud, and even if we assume for the sake of argument that the delivery and receipt can occur, this will not result in the victim being deprived of the information that he conveyed verbally. Rather, it remains under the control of the person who transmitted it and in his possession, which is something that is consistent with the nature of the programs and information, except It is not consistent with the nature of the criminal activity in the crime of fraud, and this means that the programs are not fit to be subject to the criminal activity in the crime of fraud.

B/ By applying the criminal activity of the crime of breach of trust in the information field:

We find that it is a relative application, so there is no doubt that the crime of breach of trust has occurred with regard to the supports on which the programs and information are installed, in the case in which the trustee copies the program for his own account, bypassing the agreement that binds him to the owner of the program, as through this copying the act of use is achieved, which means the trustee uses the money in a way that depletes all of its value. Or some of them, while its substance remains the same. However, it is difficult to say that the crime of breach of trust has occurred in the case of programs and information independent of the support, because it is not possible for the criminal activity of the crime to occur, which is delivery based on a contract of trust, because there is no physical activity through which the act of receipt is achieved, which Prevents the ability of software and information to be subject to criminal activity in the crime of breach of trust¹⁴.

C/ By applying the criminal activity of the crime of destruction in the information field:

We find that the Algerian legislator did not restrict criminal activity in the crime of destruction by a specific means, as it is one of the crimes of a free nature. Therefore, there is nothing preventing the crime of destroying computer programs from occurring, especially since the Algerian legislator did not specify a specific method for the crime to occur and did not specify a single specific result for its occurrence. It is conceivable that the offender will direct his criminal activity to the program and the support on which they are registered together, or to the program only without the support, and the crime may occur through direct contact with the device, or it may occur through remote communication.

Therefore, the crime of destruction stipulated in the Penal Code provides complete criminal protection for computer programs, unlike other money crimes, which provide only relative protection.

Conclusion:

thatCybercrime is considered one of the contemporary information crimes that has accompanied the era of technological progress, especially after the emergence of the international information network “the Internet”. Due to the scientific progress achieved, it has helped to

spread and diversify this criminal behavior, which has become a threat to humans in various fields, especially economic, social, cultural, and moral. Even religious beliefs, in light of the widespread spread of this very sophisticated criminal pattern, in which the latest high and advanced technological technologies are used, and the speed, resourcefulness, and ingenuity of its perpetrators always allow them to escape punishment in the absence of physical evidence of the crime, in addition to the absence of a national legislative system that defines the act, criminalizes it, and then determines the punishment. appropriate to the perpetrator. This was negatively reflected at the international level. Despite the existence of many international agreements related to cybercrime that were previously discussed, they remain insufficient in the absence of concerted international efforts, which seek in their entirety to take the necessary measures to reduce these crimes in view of their special nature. It is considered an international crime that crosses borders.

And it canComing up with the following set of suggestions:

- the jobTo conclude bilateral and multilateral international agreements to contain and mitigate crime;
- Supporting and developing international cooperation systems in the field of combating cybercrime.
- All countries must seek to amend their internal laws and make them keep pace with scientific and technological development.
- The need to activate effective protection and defense systems for the information system, and control and control of media technologiesConnection.

-
- ¹-Dr.. Muhammad Fathi Abdel Hadi, Introduction to Information Science, Gharib Library, Cairo 1984, p. 217.
- ²- Amal Qara, Criminal Protection of Information Technology in Algerian Legislation, Houma Printing and Publishing House, Algeria 2006.
- ³- Dr. Ahmed Abd al-Razzaq al-Sanhouri, Al-Waseet fi Sharh al-Civil Law, The Right to Property, Part Two, Dar Ihya al-Turath al-Arabi, Beirut 1952, p. 09.
- ⁴- Dr. Ali Abdullah Al-Qahwaji, Criminal Protection for Computer Programs, University Press and Publishing House, Beirut, 1999, p. 7..
- ⁵- Amal Qara, previous reference, p. 18.
- ⁶- Amal Qara, previous reference, p. 18
- ⁷- Dr. Abd al-Rashid Mamoun, The Author's Moral Right, General Theory and Its Applications, Dar al-Nahda al-Arabiya, Cairo 1978.
- ⁸- Dr. Hisham Farid Rostom, Penal Code and Information Technology Risks, Typewriter Library, Assiut, 1995 edition, pp. 256-257.
- ⁹- Dr. Ali Abdul Qadir Al-Qahwaji, previous reference, p. 23.
- ¹⁰- Dr. Ali Abdul Qadir Al-Qahwaji, previous reference, p. 95.
- ¹¹- Amal Qara, previous reference, p. 26.
- ¹²- Amal Qara, previous reference, p. 23.
- ¹³-Dr. Hisham Rustom, previous reference, p. 456.
- ¹⁴- Amal Qara, previous reference, pp. 45-60.