

Images and Manifestations of Electronic Fraud on Persons and Funds through Digital Data

Mamene Besma*

Abbas Leghrour University Khenchela- Algeria

Submission date: 30-09-2024

Acceptance date: 21-01-2025

Publication date: 01-03-2025

Abstract:

Fraud in the digital environment is considered one of the most dangerous types of digital corruption. This new phenomenon has allowed its perpetrators to enter homes and offices, cross borders, and reach victims with great ease, especially with the spread of the Internet as an important means of providing financial and banking services. Meanwhile, electronic fraudsters invent new methods daily to deceive their victims and ensnare them. At a time when Internet hackers and professional electronic fraudsters work around the clock to innovate new methods and find vulnerabilities through which they can carry out their tasks, information security companies, along with banks and financial and banking institutions, have created specialized technical departments to protect customers and secure their financial transactions over the Internet.

On a daily basis, bankers and computer experts discover many methods used in fraud operations, including those related to email messages and others related to daily conversations conducted by users and other types of communication.

Thus, electronic fraud is considered one of the most important and dangerous forms of digital corruption that various international and national efforts have sought to combat. The aim of this study is to shed light on the various forms of electronic fraud.

Keywords: Digital fraud; Digital data; Persons; Funds; Digital corruption.

*Corresponding author (Mamen.besma@univ-khenchela.dz); (Sécurité étatique et sociétale: santé et sécurité alimentaire).

© Mamene Besma - Creative Commons - Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)

Introduction:

The world today has witnessed the birth of modern technological means and advanced techniques, which has prompted this same human being who was the cause of their emergence to violate and assault the property of others, using those devices that his mind created and his superior genius invented. The spread of media, the Internet, computers, high-quality digital cameras, techniques for recording and transmitting images and sound, and satellite channels were a direct cause of this assault, especially since the user did not realize the flow of information and communications across borders without any consideration for geographical or political boundaries. Individuals give information to various entities that may be internal or external, and perhaps entities that have no known location, which raises risks of misuse of this data, especially in countries where legal protection levels for digital data are not available, making it pose a serious threat to individuals and society.

Fraud in the seventh decade of the twentieth century using computers was one of the first crimes that began to be widely recognized as a new type of crime. As a result, the first legislative confrontation of these crimes took place during the Florida Computer Crimes Act, which is the first law that criminalized computer fraud and was issued in 1978 after a famous incident in one of the sporting events where some people printed forged cards at that time. With the beginning of the eighties, most governments of the world began to adopt similar laws. Canada was one of the first countries to enact a federal law addressing computer crimes, and in 1990 in Britain, the Computer Misuse Act was issued, which criminalized fraud in the third chapter.¹ From here, the idea of Internet fraud emerged, and in this context, there were multiple definitions of Internet fraud.

Some defined it as any fraudulent behavior that adopts the computing approach with the intention of obtaining a financial advantage. Others defined information fraud as: the deliberate manipulation of information and data representing material values stored by the computer system, or the unauthorized entry of correct information

¹Mohamed Tarek Abdel Raouf, Internet Fraud Crime, Al-Halabi Legal Publications, Lebanon, 2011, p. 36, 37.

and data, or manipulation of commands and instructions that govern the programming process, or any other means that would affect the computer to carry out its operations based on this data, commands, or instructions in order to obtain an illegal profit and harm others.

Information fraud crime has been given many jurisprudential and other classifications, which leads us to pose the following problem:

To what extent is there a sufficient legislative response to digital fraud offenses in Algerian legislation?

In this study, we will focus on the tripartite classification of information fraud, given that it is the broadest and most accurate, as it included most types of digital fraud.

In this type of classification, information fraud took two groups, depending on whether it occurs on funds, individuals, or data, as follows:

I. Crimes that occur on material wealth through digital data.

However, it is characterized by some features that distinguish it and make it of a special nature due to its association with automated accounts and information technologies. On this basis, some have defined it as “a behavior that ensures the deception of the victim in order to seize his money, as it is a behavior that involves fraud, deception and fraud. On this basis .¹ Crimes of attacking money through the information network are not limited to misusing technological advancements against individuals alone, but extend to affect the financial integrity of others, constituting an assault on their financial resources. If this attack is within the realm of automated processing, whether informational or digital, it targets the computer itself and its peripherals, considering the computer as a negative tool for committing crimes against individuals when used through the network as a means to execute crimes and attacks on the money of others. Hence, we have divided this issue into two branches. In the first branch, we address crimes that affect material wealth through digital data, and in the second branch, crimes that affect moral wealth through digital data.

¹ - Ammar Abbas Al-Husseini, *Computer and Internet Crimes*, Zain Law Publications, Edition 02, 2019, p. 272

1- Cyber Fraud Tactics

The last century witnessed a revolution of an unprecedented nature,¹ termed the Information and Communication Revolution. The latter has achieved tangible success in dealings between individuals and major economic companies, leading to a change in the nature and pattern of economic life for all consumers, whether in advanced or developing countries alike. On the other hand, the emergence of global financial, banking, and commercial institutions that constantly seek increasing intervention in economic life in general, and individuals' lives in particular, has led to the appearance of electronic cards, known as credit cards, providing services and advantages to all users.

1 – 1 Credit Card Fraud:

Credit cards first appeared in America² and have come to occupy a large space in individual transactions at the expense of other payment methods. This spread, both locally and internationally, has led to the emergence of methods and ways to manipulate and defraud using them. This has resulted in difficulty for customers to prove their identity and led to the illegal exploitation of the card, which constitutes a new crime involving a new criminal, a new concept of crime, and a vast stage that includes all countries of the world. This spread has created an opportunity for professional thieves and forgers to use credit cards for fraud and manipulation, especially since this type of card relies on an information system where data and information flow, and where money is in the form of electronically encrypted symbols and data that computer crime professionals can decode and forge to obtain funds illegally. Electronic payment card crimes have become a threat affecting the cardholder and all parties involved in card operations worldwide and simultaneously. Counterfeit cards are prepared and lost in one country, while the necessary information about the valid payment card is collected in other countries, and the counterfeit cards are promoted elsewhere in

¹ - Osama Ahmed Al-Manasseh, Jalal Mohammed Al-Zoubi, *Electronic Information Systems Technology Crimes, a comparative study*, Dar Al-Thultha for Publishing and Distribution, Jordan, second edition, 2014, p. 209

² - Osama Ahmed Al-Manasseh, Jalal Mohammed Al-Zoubi, *Electronic Information Systems Technology Crimes, a comparative study*, Dar Al-Thultha for Publishing and Distribution, Jordan, second edition, 2014, p. 209

the world. Modern technology such as fax, internet, advanced communication means, and globally distributed automated credit information have all provided forgers with the opportunity to steal others' rights anywhere in the world.

1-2 Fraud Using Electronic Payment Cards:

The electronic payment card is defined as “a rectangular plastic card bearing the name of the issuing organization, its logo, the signature of the holder, and in particular - its number, the name of the holder, the account number and the expiration date, and thanks to this card, the holder can withdraw cash from automatic distribution devices and obtain the goods and services he needs without having to pay for them immediately.”¹

This type of crime relies on electronic payment cards during transfer operations from the customer's card account to the merchant's bank balance through the electronic voice network of international organizations such as Visa Card and MasterCard. This card allows the customer to obtain goods and other services on the network through written or telephone authorization to deduct the value from the card account.² From here, hackers use credit card numbers through operating programs that allow the creation of specific bank cards by forging the account with a number specific to the card-issuing bank and using it illegally in the marketing process via the network. Stealing credit cards is not a difficult matter; credit card thieves can now steal hundreds of thousands of card numbers in one day through the Internet, and then sell this information to others.

MSNBC has practically demonstrated how easy it is to obtain credit card numbers from the Internet. They displayed lists containing more than 6,500 credit card numbers obtained from seven e-commerce sites using commercially available databases. It wasn't difficult for any intruder or hacker using this primitive method to access and seize

¹ - Abdelkafi Mariam, Bourbaba Souria, The crime of computer fraud on electronic financial cards, *Journal of Law and Political Science*, Vol. 08, No. 01, 2022, p. 408

² Mohamed Saleh Al-Alfi, Crimes of Assault on Credit Cards as One of the New Criminal Patterns, a working paper published on the following website <http://www.eastlaws.com>, accessed on 20/06/2017, p07.

numbers and use them in purchase transactions where the real cardholders pay the price. The matter extends to the risks that the current credit card can be exposed to. We are now at the beginning of a technological revolution called "electronic money," which is predicted to complement paper money. It is also expected that reliance on this new and modern type of money will increase and that it will gain the trust that traditional money holds.¹

Criminals rely on several methods to seize data and secret numbers of credit cards to use them in fraud. The most important of these methods are:

* **Impersonation method:** This method is done by creating fake websites on the information network, similar to the websites of original companies and commercial institutions on this network. This fake site appears as if it is the original site providing that service. After creating the fake site, the perpetrators receive all financial and commercial transactions that the original site usually provides to its customers via the Internet. They receive and view electronic messages related to the original site, and then seize the data of credit cards or electronic payment cards. In one case in Egypt, a gang of three people was arrested for designing sites that resemble the sites of some banks, then sending random messages via email to real customers who are deceived and write their data and follow the steps specified by the accused. After identifying the secret data of customers, especially secret passwords, the balances of these victims are seized.

* **Espionage method:** In this method, perpetrators use programs to hack into the information systems of companies and public commercial institutions on the information network. These criminals can then access the data and commercial information of these companies, including information related to credit cards or electronic payment used in e-commerce over the network. This allows the perpetrator to seize valid card data and use it over the Internet at the expense of the legitimate cardholder. For example, in 1997, a person named "Carlos Sadalgo" seized 100,000 credit card numbers and other data by hacking

¹ Mohamed Saleh Al-Alfi, Crimes of Assault on Credit Cards as One of the New Criminal Patterns, previous reference, p08.

into a group of Internet service providers. He put these numbers on a CD, then encrypted it and offered it for sale for \$250,000. Federal investigation agents discovered this crime, and he was tried and sentenced to 30 months in prison.¹

* **Skimming method:** This involves printing the details stored on the magnetic strip of a credit card by passing the card through an electronic reader. Once the card details are obtained, such as the cardholder's identification number and the card's expiration date, the fraudster can create a card identical to the original one for use in transactions conducted on the Internet. The danger of this type of card data seizure is that the cardholder does not know that their card has been hacked, so they do not report it for cancellation. Thus, the fraudster can use the forged card for a long period. This is unlike the traditional method of seizing card data, which is stealing the card. In 2005, four members of a card skimming and money withdrawal gang in England were sentenced to four years in prison for committing fraud estimated at £200,000. It's worth noting that there is a mechanical method for seizing credit card data, where the details engraved on the plastic card are mechanically transferred from one card to another. This method is easier than stealing the entire card while it's being transferred between the bank and the customer.²

* **Generating card numbers:** This method is based on generating credit card numbers using mathematical and statistical equations, with the aim of obtaining credit card numbers owned by others, which is all that's needed for purchasing over the information network. This method relies on mathematical bases in permuting and combining numerical digits, ultimately leading to a specific result, which is the secret number of a circulating credit card. It is then used over the information network.³

2- The second type of cyber fraud crime

¹Mohammed Tarek Abdel Raouf, Internet Fraud Crime, previous reference, p. 82

² Mohammed Tarek Abdel Raouf, Internet Fraud Crime, same reference, p. 84.

³Mohammed Tarek Abdel Raouf, previous reference, p.85.

2-1 The crime of bank robbery:

The crime of bank robbery is embodied through a person using a computer to access the Internet and illegally access banks, exchanges, and financial institutions. This involves transferring funds from customer accounts to other accounts by entering false data or modifying or deleting existing data with the intent of embezzling, transferring, or destroying funds. This technique is based on seizing very small amounts of money from large accounts so that the decrease in these funds is not noticed. It occurs through the embezzlement of data and benefiting from it by using the embezzler's personal information such as name, address, and secret numbers of the victims, and the illegal use of the victim's identity to begin the process of covert theft via the Internet, leading others to provide funds to the perpetrator through bank transfer.¹

The Internet has given several advantages to those who carry out money laundering operations, including extreme speed and crossing border barriers between countries, avoiding laws that some countries might impose to hinder their activities, as well as encrypting their operations, which gives them a greater degree of secrecy.² The use of the Internet in money laundering has many aspects, such as using a credit card to purchase jewelry and then paying the bill with cash returns from drug trafficking, prostitution, and other crimes.

Also, the spread of e-commerce across the information network is the best aid for those conducting money laundering operations. E-commerce and its spread worldwide has greatly assisted in money laundering operations due to the speed of agreeing on and completing deals through it, often without being under strict legal supervision. Even in the case of legal supervision, it is possible to avoid that supervision and complete these deals by agreeing on steps and arrangements that are implemented via the Internet and through complex encryption methods

¹Saghir Youssef, *Crime Committed via the Internet*, Master's Thesis in Law specializing in International Business Law, University of TiziOuzou, 2013, p. 46

² Munir Muhammad Al-Junbihi, Mamdouh Muhammad Al-Junbihi, *Internet and Computer Crimes and Methods of Combating Them*, Previous Reference, p.79.

that cannot be solved, and thus it is not possible to know how these deals are completed.¹

2-2 Internet Gambling Crime:

This crime falls within the process of money laundering with gambling clubs spread around the world, which has made virtual casino sites on the Internet subject to suspicion and monitoring by American authorities. The legal problems facing owners of virtual gambling sites on the Internet are unauthorized, unlike real clubs, and all this is for exorbitant amounts of money resulting from gambling over the network. There are more than 100 gambling sites on the Internet where all types of gambling provided by real sites are practiced. The gambling market in America is considered the fastest growing ever, where site owners resort to establishing and managing them from places adjacent to America. These clubs announce their physical presence in the Caribbean region via the Internet. The FBI has followed Internet sites that carry out money laundering activities and focused its work and investigations on gambling operations and the people who carry out these activities. It was found that these sites are located in "Curaçao, Antilles, Antigua Island, and the Dominican Republic."²

II. Crimes that occur on intangible assets through digital data

The development witnessed by the world in the recent period of the last century in various fields was accompanied by an important development, especially in the field of communications regarding information technologies, which increased dealings with them due to their speed and the time they save. The information generated from human interactions was largely limited and its volume did not represent any problem for its collection and storage. However, with the advancement of humanity and the increase in the amount of information, traditional methods of collecting information became incapable of meeting needs efficiently and effectively. It became necessary to have

¹-Munir Muhammad Al-Junbihi, Mamdouh Muhammad Al-Junbihi, Previous Reference, p.80.

²Mamdouh Abdel Hamid Abdel Muttalib, Computer and World Information Network Crimes, Law Library, Sharjah (United Arab Emirates), First Edition, 2001, p. 70.

more advanced means to protect and collect this information. With the emergence of this information, legal problems arose about the extent to which this information can be considered intangible assets

Therefore, we will address the definition of money in general: Money is what is suitable to be the subject of a right with financial value, and the thing is the subject of the right. Things are divided into material things and immaterial or intangible things, knowing that from the traditional point of view, money does not apply to material things. For this reason, the definition of money in the context of financial crimes was "any material thing that is suitable to be the subject of a financial right".¹

Intangible assets have been defined as: assets that cannot be identified by touch but by other senses, and the rights that are determined on them are recognized. The rights that apply to them are intangible rights or powers granted by law to a person over an intangible thing, including the author's right to their literary or musical work, the inventor's right to their invention, and the designer's right to their design.²

We will address the following regarding the infringement on tangible and intangible assets.

It is clear to us that information is one of the fruits of human beings that transforms into a knowledge balance from which humanity draws everything it needs to facilitate its way of life. This service that humans provide to each other necessitated the recognition of the rights of the owners of these works to have their works attributed to them. It seems that this recognition is not sufficient to fulfill their right, but rather the rights must be protected. The image of intangible assets appears in informational assets; therefore we will address:

¹ Ahmed Abdel Razzaq Al-Sanhouri, Al-Wasit in Explaining Civil Law, Property Right, Part Two, Arab Heritage Revival House, Beirut, 1952, p.09.

² Ahmed Abdel Karim Salama, Private International Law, Arab Renaissance House, Cairo, 2008, p. 1010.

1- Theft of information assets

In the midst of technological development, the importance of information has increased, especially that stored within automated processing systems. With the massive spread of computer communication networks - the Internet - forms of attacks on information have increased, the value of which depends on the considerations of privacy and security available to it. One form of attack on information is the theft of information assets. This raises a problem, especially when this information is inside the device without right or copying this information. Some have defined it as the theft of information from programs and data stored in the computer circuit illegally, or copying information programs illegally, or copying programs illegally after the perpetrator of this operation was able to obtain the password or by picking up electromagnetic waves emitted by the computer during its operation and using antennas connected to a special computer [1].

The process of stealing information assets takes different forms. It may be done through mental capture of data, by looking and listening, and it may be done by copying electronically stored data inside the computer, whether stored within the computer system or on conventional storage media. It may be committed after installation by hacking the computer system, and finally, information asset theft operations may be committed by intercepting computer data during its transfer process.

2- Intellectualproperty

- Meaning of intellectual property: It is the fruit of human creativity and invention, and some laws have called it mental property [2] because it is based on mental output, such as copyright, the inventor's right to his invention, the merchant's right to his trademark, and so on.

3- Digital drug trade crime:

These crimes are carried out especially through those sites spread across the network that are related to promoting drugs and bad marketing for their use, and even go beyond that to teaching how to grow and

manufacture drugs of all kinds and sell them.¹ It is not limited to these sites only, but even forums and chat rooms contribute to that. Drug consumption is no longer limited to what was previously done by injecting it into the vein or chewing or smelling it... Rather, human thought has developed to transform the abuse system into electronic abuse or digital abuse that has the same effect as natural drugs. Drug abuse via the Internet is represented by the drug dealer sitting in front of his computer to receive purchase orders for drugs through his website. Here, he does not send one of his followers to deliver the purchased drug, but rather the buyer performs a download process for the drug he wants in the form of files, which is known as digital drugs.

Digital drugs are audio files containing mono or dual tones that the user listens to, making the brain reach a state of numbness similar to the effect of real drugs, or at least this is what some claim. These audio files - or digital drugs - were designed to simulate hallucinations and the euphoria associated with drug use by influencing the mind unconsciously. This effect occurs through inaudible sound waves called white noise covered with some simple rhythms to cover the disturbance of those waves. Digital drugs have found tremendous popularity among Internet users, especially among young people.²

Mental property refers to those rights that apply to something intangible, i.e., intangible, and scholars call this type of rights the name of innovation and creativity rights, and the law calls them moral rights, which are those that pertain to mental rights, because they relate to mental or intellectual activity.

III. The Algerian legislature's position on digital fraud offenses

The Algerian legislature has tried to combat the crime of digital fraud by enacting a strong legal arsenal in which it has developed procedural

¹ Muhammad Saleh Al-Alfi, scientific research entitled: Patterns of Internet Crimes, p. 11 published on the following website <http://www.eastlaws.com> and this site was viewed on 28.06.2017

² Abu Sari' Ahmed Abdel Rahman, scientific research entitled The Use of the Internet in Drug Abuse - Digital Drugs - in December 2010, p. 05, 06 on the website www.child-trafficking.org and the site was viewed on 15,06,2017.

and punitive provisions for the acts constituting cybercrime in general, and has ratified some conventions that deal with this criminal behavior:

1- Internal laws

Among the most important legislations issued by the Algerian legislator in this field, we mention the following:

- Law 04/15 of November 10, 2004, amending and supplementing Order 66/156 containing the Penal Code, where it added a seventh section under the title of infringement of automated data processing systems in articles 394 bis to 394 bis 7

- Law 06/22 of December 20, 2006 amending and supplementing the Code of Criminal Procedure through the articles regulating local and specific jurisdiction and inspection procedures

- Law 09/04 of August 5, 2009, containing special rules for the prevention of crimes related to information and communication technologies. This law aims to establish procedural provisions commensurate with cybercrime, where the National Authority for the Prevention of Crimes Related to Information and Communication Technologies was created in Article 13 and entered into force in 2015 by Presidential Decree 15/268.

- Law 16/02 of June 19, supplementing Decree 66/156 containing the Penal Code, this law came to supplement Articles 87 bis11 and 87 bis12, in addition to Article 394 bis8.

It is also worth noting that recently, during a meeting of the Supreme Council of Security, a new criminal pole was created to follow up and combat cybercrimes.¹

However, it is noticeable that the Algerian legislator did not take the initiative to develop a specific and precise text for the concepts and forms of digital fraud offenses, but only referred to them in Article 394 bis2 of Law 04/05 of the Algerian Penal Code with the concept of trafficking in information data through information systems with the aim of making profits.

2- Conventions signed by Algeria

The most important convention signed by Algeria in the field of information technology is the Arab Convention on Combating Information Technology Crimes, which was ratified by Presidential Decree 14/252 dated September 8, 2014 and signed in Cairo on September 21, 2010. Thus, Algeria has adopted the provisions of the convention as legal rules and is bound by them

¹ - Abdelkafi Mariam, Bourbaba Souria, Previous Reference, p 420

in the face of other countries acceding to the convention on the one hand, and on the other hand, its judiciary is obliged to apply its content ¹

Conclusion:

At the conclusion of this research paper, we conclude that the crime of information fraud as a type of electronic corruption is one of the most serious new crimes that affect public and private interests, and therefore we propose to confront this crime through the following:

- Saving effort and money to strengthen electronic surveillance to minimize the crime of electronic fraud.
- The need for the Algerian legislator to intervene in order to create legal texts specific to digital fraud crimes and limit their forms.
- The need for local and foreign cooperation in order to benefit from expertise in the field of e-commerce and recognize the mechanisms for combating digital fraud crimes.

¹ - Nani Lahcen, Investigation of IT-related crimes between legislative texts and technical privacy, New University Publishing, 2018, p. 43