journal of legal and economic research | Volume:03/ N°:01 (2020), p634-650

Protecting electronic money from money laundering in Algeria

حماية النقود الالكترونية من تبييض الأموال في الجزائر

* **Salima BOUAKAZ, Doctorate Student**
University of Larbi Tebessi- Tebessa, Algeria
salima.bouakaz@univ-tebessa.dz

Send Article Date: 27/02/2020 Date of acceptance of the article: 09/05/2020

****

Abstract:

Electronic money plays an important role in e-commerce, facilitating e-marketing operations without the need for mobility, thanks to the tremendous development of information and communication technology. However, despite these advantages, new challenges have emerged. Money laundering, which turned it from a tool to activate e-commerce into a tool to commit crime, all of which led to the need to devote the principle of protection of this method both in public texts or private as well as technical protection of financial systems.

Key words: Electronic Money - Electronic Commerce Law - Money Laundering - Protection.

ملخص:

تقوم النقود الالكترونية بدور مهم في مجال التجارة الالكترونية، حيث تسهل عمليات الوفاء لعمليات التسويق الالكتروني دون الحاجة للتنقل، وهذا بفضل التطور الهائل لتكنولوجيا المعلومات والاتصال، إلا انه وبالرغم من هذه المزايا التي توفرها، فقد أفرزت تحديات جديدة تتمثل في استخدامها بشكل غير مشروع لارتكاب جرائم تبييض الأموال، ما جعلها تتحول من وسلة لتفعيل التجارة الالكترونية إلى أداة لارتكاب الجريمة، كل ذلك دفع

* D/S.Salima bouakaz: salima.bouakaz@univ-tebessa.dz

إلى ضرورة تكريس مبدأ الحماية لهذه الوسيلة سواء في النصوص العامة أو الخاصة إلى جانب الحماية التقنية للأنظمة المالية.

الكلمات المفتاحية: النقود الالكترونية- قانون التجارة الالكترونية- تبييض الأموال- حماية.

Introduction :

The tremendous development of information and communication technology has produced several changes and new developments in all sectors, including the financial and banking sector, which in turn has produced new financial services, keeping pace with the nature of electronic commercial transactions that saved a lot of effort and time for those who are involved in such kind of activities, but this development was accompanied by new challenges consisting in the emergence of computer crimes as a new type of economic and financial crimes, such as money laundering, by exploiting these modern means to enter their suspicious money into the legitimate economy cycle, especially in the light of the characteristics that characterize this type of crimes, as it is difficult to prove given that they take place in a virtual environment and quickly without leaving traces behind them along with professional bands, performing them, what is imposed on the legislator is a new challenge consisting in the necessity of adopting mechanisms to protect electronic money and arranging the criminal penalty for what is contrary to it, which makes us present the following problem:

Is the protection established for electronic money within the framework of electronic commercial transactions sufficient to prevent its use in money laundering operations?

This is what will be shown in this research paper through the following tracks:

First: The relationship of electronic money to money laundering

Second: Electronic money protection against its use in money laundering.

SECTION I: The Relationship of Electronic Money to Money Laundering

In the light of the global changes that have taken place today and with the development of modern technological methods used in all areas of our life, the scope of electronic commerce has expanded and its methods have been developed, as money has evolved and has emerged in a new form that is completely appropriate for electronic commerce transactions and the traditional methods of payment are declining in front of the growth and spread of the electronic payment system[1], through which the value of goods and services provided by electronic commerce can be paid by transferring the money from the consumer to the provider or supplier.

However, despite the great advantages provided by electronic money and the increasing volume of dealing with it via the Internet, this has been accompanied by a steady growth in the accompanying crimes for its use, such as the crime of money laundering electronically.

Therefore, the concept of electronic money will be tackled, then how to use it in money laundering.

First Requirement: The Concept of Electronic Money:

The use of electronic cash began in 1994 through the efforts of the company E- cash in its successful pilot project in cooperation with banks, and then it was granted the right to issue electronic cash in addition to one hundred commercial companies[2].

Money has spread more recently in the payment of fixed-value and dues payment compared to previous years in which liquid money was the only acceptable method[3].

Paragraph 1: Definition of Electronic Money:

The term electronic money takes many forms and as this expression

applies to debit card as well as credit card and stored-value cards and smart cards[4] are used.

The European Central Bank defined electronic money as: "an electronic stock of cash value on a technical method commonly used to make payments to contractors other than its issuance, without the need for a bank account when the transaction is made and used as a prepaid portable tool."[5]

Electronic money or digital money is intangible money that takes the form of electronic units or electromagnetic pulses bits and is stored in a safe location on the customer's computer hard disk known as the electronic wallet.[6]

And the person who wants to use electronic money has only to open an account at the banks that provide the service of exchanging ordinary money for electronic money, then the account holder withdraws the money from his bank account to put it in his account for electronic money, which is found on the hard disk of his private computer by a special program cyber wallet[7].

Paragraph 2: Characteristics of Electronic Money

The essence of the relationship between electronic money and money laundering operations lies in the set of characteristics that this money has, and distinguishes it from traditional money, which enabled money-launderers to use it as a tool to commit the crime of money laundering. The most important of these characteristics are[8]:

• Electronic money is a cash value stored electronically: it is a coded data that is placed on electronic messages in the form of plastic cards or on a computer's memory.

• It is two-dimensional as it is transferred from the consumer to the merchant without the need for a third party between them.

• It is not homogeneous, as each source issues different electronic money in terms of value or the number of goods and services that can be purchased with it.

• It is easy to use due to its small size and light weight.

• It is considered private money as it is issued by private credit companies or institutions.

• The presence of risks of human and technological errors, as this method remains vulnerable to the occurrence of many problems, especially in the absence of trained staff, having sufficient experience to be able to manage the risks resulting from such modern technologies[9].

Second Requirement: - Electronic money facilitates the commission of money laundering offences

Despite the advantages of electronic money to facilitate economic life, it is not immune to criminals who launder the money and use it in a wrong way, whether in terms of relying on it to facilitate money laundering crimes, or even expanding the crime of money laundering

Paragraph 1 : Electronic Money Facilitates Committing Money Laundering Crimes

Electronic money is an ideal way to store a monetary value for money obtained from an unlawful source in order to launder it, and here the negative side of this advanced means of payment is highlighted, so that it becomes a means of committing the crime given that its control is extremely difficult, as it is not a physical material that can monitor its movement, and the true identity of the dealers may not be recognized, and in this way the criminal can perform whatever he wants in relation to the financial operations to reach his real purpose in hiding the reality of his illicit funds[10], as there is a great possibility for money laundering, using digital cash through the deposit and merger stages, In the first stage, the holder of the money

to be laundered begins to circulate this money by depositing it in the financial institution, whether in the physical or virtual world by means of digital deposit, and thus avoids paper accounting restrictions, and in the merger stage, the holder conducts digital transfers to countries without money laundering operations, and then transfers it to other places and insert it into the global economic movement without the risk of revealing its true source[11].

Thus, we find that electronic money is one of the means produced by modern technology in order to settle commercial and financial transactions without the need for traditional liquid money. This money has a number of advantages that enable the owners of illicit money to use it as a means of committing a crime of money laundering, and here the danger of using this money illegally with the intent to commit this crime in contrary to the real purpose for it was found[12].

Paragraph 2: Electronic Money Expands the Crime of Money Laundering

The object of the crime of money laundering consists in the unlawful money, resulting from the committing crimes, and electronic money may help secure these illicit funds that need to be cleaned. For example, the use of this money leads to increased cases of tax evasion, as it is difficult for the agencies responsible for collecting taxes to monitor transactions that take place online using this money, and it is difficult to impose taxes on them. There is no doubt that the money that results from tax evasion is unlawful money that needs to be cleaned. On the other hand, private electronic money makes it difficult to verify its authenticity when concluding transactions, it may be discovered after completing the transaction that the electronic money with which this transaction was settled is fake. Consequently, the money, resulting from it is illegal money that needs to be cleaned, and in addition to that there is a real possibility to extract fake copies of electronic money by knowing the details of the original electronic money, and if this is achieved then this money is illegal money[13].

Also, this money is vulnerable to theft through unlawful access to personal account devices and systems saved on computers through what is known as unlawful decryption, and this theft is not different from the theft of traditional money and the result of the two thefts is considered illegal money[14].

SECTION II: Electronic Money Protection against its use in Money laundering

In order to protect this method against its use other than for the purpose for which it existed, it was necessary to think of resorting to a technique capable of securing electronic payment methods in general and making them more confidential and effective, as the Algerian legislator stipulated to protect them through special texts consisting mainly in Law N°. 18-05 dated on 05/10/2018, comprising the electronic commerce law[15], as well as the law 09-04 dated on 16/08/2009, comprising special rules for the prevention and fight against crimes related to information and communication technologies[16].

First Requirement: Aspects of Technical Protection:

The use of electronic money has been accompanied by the emergence and growth of attacks on it, as it has become a target of electronic criminal gangs which led the international financial institutions, banks and owners of electronic commercial sites to develop technical security means and systems to provide protection and create confidence in the consumer and the merchant to exchange goods and online services, and the Algerian legislator has stipulated within the electronic commerce law N°18-05 mentioned in article 11 thereof that it falls on the electronic supplier when submitting his electronic commercial offer to include sufficient information to ensure the proper functioning of electronic commercial transactions like the provisions related to the protection of personal data, where the same law stipulated that not including this term is considered a offence in pursuance of the article 39, and singled out for it a financial penalty ranging from 50,000 DZD to 500,000 DZD.

Among these means and technical systems to secure buying and selling we mention:

Paragraph 1: Safe Electronic Transactions System[17]

It is a protocol that uses software called electronic wallet software, in which the number of the electronic card holder and the digital certificate issued by an approved bank, whether conventional or electronic.

This protection is carried out by issuing digital certificates to the consumer and the merchant certifying their identity during the conduct of electronic commercial transactions, by a high trust body called the accreditation body, where it extracts these identities, after confirming the identity of the consumer and the true identity of the merchant, where they are stored in the electronic portfolio of each of them. Thus, the use of a secure electronic transaction system would provide technical protection for electronic payment methods in general and payment cards in particular, which are electronic money[18].

Paragraph 2: SSL System

This system is an electronic program that contains a protocol for exchanging data and information in an encrypted way between two computers over the internet, so that data and information are only read and accessed by the sender or the receiver, then it was developed in order to transfer Securely exchange data and information over the internet[19].

Paragraph 3: 3D Secure System

It is a technical protection system that was invented by Visa Card company in 2001, in order to secure electronic payments via the Internet when using electronic cards in this, as this system allows verification of the user's identity for electronic cards through the SSL encryption system[20].

Second Requirement: Legal Aspects of Protection

The use of electronic payment methods in general to meet the value of goods and services via the Internet has accompanied a steady growth in the attacks accompanying their use, which compelled various countries to issue penal legislation in order to provide them with legal protection.

Paragraph 1 : Through the Penal Code

The Algerian legislator has stipulated, within article 394 repeated of the Penal Code[21], that it punishes anyone who attempts to have access via cheating to every part of the automated data-processing system or attempts to do so. Through the text of the article, we note that every entry into the information system of a website or a part of it is considered a crime punishable by law.

Accordingly, unauthorized entry is achieved by simply initiating it or actually entering the information system regardless of the method used in that, whether entry into the whole system or part of it, and the result is not required to be achieved, as it is considered a crime of behavior[22], and this case represents an unlicensed crime of entry in its simple form, but if the act of entering or remaining leads to the deletion or alteration of data or sabotage of the information system of the website, this is considered data tampering which is stipulated by the Algerian legislator within the article 394 repeated 1 of the Algerian Penal Code which is considered a material crime that is not enough for its occurrence that it threatens the integrity of the data only, but there must be an actual damage concerning data consisting in the change of their state[23].

Punishments for the Crime of Tampering Data: article 394 repeated 1 of the Penal Code stipulated an original penalty for the offender, which is the imprisonment from 6 months to 3 years and a fine from 500,000 DZD to 2,000,000 DZD.

In addition, article 394 repeated 6 stipulates complementary penalties, which are the sources of hardware, software and means used with the closure of sites that are objects to the crime, as well as the closure of the shop or place of exploitation if the crime is committed with the knowledge of the owner.

The Algerian legislator also criminalized dealing in the data obtained from the crime [24], and this would protect the electronic consumer whose data were illegally obtained from disclosure or publication.

The Penalties Prescribed for the Crime of Dealing in the Data Obtained from the Crime: Article 394 repeated 2 of the Penal Code stipulates that the perpetrator of the crime shall be punished by imprisonment from two months to 3 years and a fine from 1,000,000 DZD to 5,000,000 DZD, in addition to that Article 394 repeated 6 stipulated complementary penalties represented by the sources of the hardware, software and means used with the closure of sites that are object of the crime, as well as the closure of the shop or place of exploitation if the crime was committed with the knowledge of the owner.

Paragraph 2: Through the Law 4/9, Comprising the Special Rules for Preventing and Combating Crimes Related to Information and Communication Technologies.

The worsening of information crimes, especially with weak technical protection, required explicit legislative intervention. The Algerian legislator has redeemed the legal void through Law 09-04, comprising special rules for the prevention and control of crimes related to information and communication technologies[25], through the establishment of a national body to prevent and combat crimes related information and communication technologies in pursuance of article 13 thereof, which assigned it tasks within the article 14 of the same law. They consist in the following:

- Activating and coordinating crime prevention and control operations related to information and communication technologies.)

- Assisting the judicial authorities in their investigations regarding crimes related to information and communication technologies, including gathering information and completing judicial expertise's.

- Exchanging information with their counterparts abroad in order to collect all data useful in identifying the perpetrators of crimes related to information and communication technologies and determining the place of their existence.

The legislator also entrusted the body with other tasks that came in the text of article 4 of the presidential decree N °15-261.

In light of respecting the legislative provisions set out above, the authority is charged of the following:

- Proposing elements of a national strategies to prevent and combat crime related to information and communication technologies.

- Activating and coordinating crime prevention and control operations related to information and communication technologies.

- Assisting the judicial authorities and judicial police interests in combating crimes related to information and communication technologies, including through the collection and provision of information and through judicial expertise.

- Ensuring the preventive monitoring of electronic communications in order to detect crimes related to terrorist and subversive acts and prejudice to the security of the state, under the authority of the competent judge and excluding any other national bodies.

- Collecting, recording and archiving digital data and defining their source and path for use in judicial procedures.

- Ensuring the implementation of requests for assistance issued by foreign countries and the development of information exchange and cooperation at the international level in its field of their competence.

- Developing cooperation with national institutions and bodies involved in crime related to information and communication technologies.

- Contributing to training specialized investigators in the field of technical investigations related to information and communication technologies.

- Contributing to updating legal standards in their field of competence.

The body therefore, the authority has a preventive role to play, preceding the consumers' exposure to any electronic crime, such as piracy of payment cards or bank financial balances and the monitoring of electronic financial transfers around which there is a suspicion of money laundering[26].

In fact, the confidentiality of transactions concluded by electronic money must be preserved from the infringing of others, whether they are ordinary individuals or government agencies. In this case, a serious problem will arise, which is the contradiction between the necessity of maintaining the confidentiality of transactions on the one hand as a human right, and the right of the state to use all available means to eliminate crime. For example, the state may have to monitor various communication networks with the aim to prevent the occurrence of the crime of money laundering or tax evasion by using electronic money. In such cases, it will be difficult to reconcile maintaining the confidentiality and privacy of transactions of individuals on the one hand, and the need to tackle crime on the other hand.

Also, commercial transactions by electronic money, which may be the object of bleaching, are usually trans-boundaries, which

necessitated the creation of articles related to international cooperation and judicial assistance that will have a major role in detecting the perpetrators of these crimes, provided that the requests of states are not contrary to public order, or from this would affect national sovereignty, in addition to the requirement of maintaining the confidentiality of the information reported, and not to use it in anything other than what is indicated in the request, as stipulated in the relevant international agreements and bilateral agreements, and the principle of reciprocity[27].

Paragraph 3: Through Law 18-05 Related to Electronic Commerce

The Algerian legislator, within Law N °18-05 of 10/05/2018 related to electronic commerce, stipulates in article 11 of it that it is the responsibility of the electronic supplier when submitting his electronic commercial offer to include sufficient information to ensure the proper functioning of electronic commercial transactions along the lines of the provisions related to data protection of a personal nature where the same law stipulated that not including this item is considered an offence according to article 39 thereof and singled out for it a financial penalty ranging from 50,000 to 500,000 DZD, in addition to granting the possibility to the competent judicial authority to consider the case to suspend its access to all electronic payment platforms for a period of not less than six month.

Indeed, providing capabilities and methods to protect the personal data of the electronic consumer is in fact a protection for the electronic money that it contains from misuse by the hackers, whether by stealing it or using it in money laundering operations in the name of its owner and without his knowledge, which makes them immune from every judicial follow-up in case they are identified.

As for electronic payment, Law 18-05 stipulated that it should be done through the designated payment platforms that are created and operated exclusively by accredited banks by the Bank of Algeria, or

Algeria Post and connected to various types of electronic payment terminals.

It is worth noting that the Bank of Algeria plays an important role in protecting financial transactions in general, as it is a control body over banks, and it has the jurisdiction to set the system for internal control of banks and financial institutions, as we find it stipulated in System N ° 11-08 in its article 29 on the need to place banks and financial institutions are organized, procedures and means that allow them to respect the applicable legal and regulatory provisions within the framework of the control of money laundering and terrorism and combating them, including ensuring the precise identification of the person in charge of the operation and the recipient of electronic transfers in addition to their addresses, whatever the method used, with the need to comply with the legal obligation to notify the suspicion within the framework of the legal forms stipulated.

Conclusion:

Through this research paper, we find that contemporary life imposed on man modern means to complete his financial transactions easily through electronic money in particular, and despite the importance of this modern technology and its advantages, it has not escaped from exploiting it for purposes other than those for which it was found, such as money laundering operations, despite the prescribed protection for electronic money that indicates that the Algerian legislator has made a significant effort, especially in the light of the modernity of the law regulating electronic commercial transactions and related laws, but it remains insufficient and requires the extra care required by information technology.

The most important findings are:

- Electronic money is electronic numbers stored to facilitate electronic payments without the need to move around and physical payment.

- Electronic money is a private money as it is issued by private credit companies or institutions.

- Electronic money is one of the most important modern technologies used in electronic commercial transactions, which was used as a tool to commit money laundering crime.

- The legislator has devoted electronic money to technical and legal protection from money laundering operations, however, with Algeria's formal adoption of a law regulating the conduct of electronic commercial transactions, it has become necessary for this virtual world to remain more careful and cautious to prevent this method of payment from being deviated from the field for which it was found.

Accordingly, the following recommendations were proposed:

- The need to frame electronic money transactions, especially with openness to electronic commercial transactions.

- Engaging high-level staff of banks and them cooperate with banking program designers to reduce money laundering.

- There should be an exchange of experiences, legal and financial information between banks.

- Requiring all authorities that issue electronic money to submit periodic reports and on their responsibility for the money they issue to the competent regulatory authorities, such as the central bank and the financial inquiry processing cell.

Marginalization:

[1] Soumia DIMECHE, **E-commerce is inevitable and its reality in Algeria**, Master's Thesis, Faculty of Economics and Management Sciences, University of Constantine, 2010/2011, p. 70.

[2] Saleh Mohamed Hosni Mohamed EL HAMLAWI, **an analytical study of the role of electronic money**, e-banking conference between sharia and law, Volume

1. Faculty of Charia and Law and Dubai Chamber of Commerce and Industry, May 10-12, 2003, p. 221.

[3] Gania BATLI, **Electronic payment methods**, Edition 1, Homa, Algeria, 2018, p. 254.

[4] Saleh Mohamed Hosni Mohamed EL HAMLAWI, ibid, p 245.

[5] Gania BATLI, ibid, p 255.

[6] Nabil Salah Mahmood EL ARABI, **Electronic check and digital money,** comparative study**,** e-banking conference between sharia and law, Volume 1. Faculty of Chariaa and Law and Dubai Chamber of Commerce and Industry, May 10-12, 2003, p.70-71.

[7] Adnan Sarhan Ibrahim, **E-payment,** e-banking conference between sharia and law, Volume 1. Faculty of Chariaa and Law and Dubai Chamber of Commerce and Industry, May 10-12, 2003, p 285.

[8] Bassem Ahmed ZALAMI, **The Role of Electronic Money in Money Laundering**, Damascus University, Journal of Economic and Legal Sciences, Volume 26, First Issue, 2010, p. 547.

[9] Gania BATLI, ibid, p 259.

[10] Nader Abdelaziz Chafi, **Banks and Electronic Money**, Modern Book Foundation, Tripoli, Lebanon, 2007, p 83.

[11] Gania BATLI, ibid, p 260.

[12] Bassem Ahmed ZALAMI, ibid, p 552.

[13] Ibid, p 559.

[14] Nader Abdelaziz Chafi, ibid, p 89.

[15] Law No. 18-05 of 10/05/2018 relating to e-commerce, O.J 28 of May 16, 2018.

[16] Law 09-04 of 05 August 2009, which contains special rules for the prevention and control of crimes related to information and communication technologies, O.J 47 of August 16, 2009.

[17] Mohamed KHMIKHEM, **Consumer Criminal Protection in E-Commerce Contracts**, Ph.D. in Public Law, Aboubakar Belkaid University, Algeria, 2016/2017, p. 187

[18] Ibid, Sama page.

[19] Soumia DIMECHE, ibid, p 93.

[20] For more information see, Aude Plateaux and Other, Privacy in the 3 D Secure payment system, p: 03; The website, https://hal.archives-ouvertes.fr/hal-00958445/document, 19/02/2019 at 05:12.

[21] Order No. 66/156 of 08/06/1966, contained in the Penal Code, O.J. 49 of 11 June 1966.

[22] Saleh SHENINE, Criminal Protection of E-Commerce, PhD thesis in Private Law, Aboubakar Belkaid University, Algeria, 2012/2013, p. 75.

[23] Mohamed, KHALIFA, Criminal Protection of Computer Data, New University Pubishing house, Alexandria, 2007, p. 179...

[24] Ibid, p 195.

[25] Offences related to information and communication technologies in accordance with article 2, paragraph A, means offences of violating the automated processing systems of data specified in the Penal Code, any other crime is committed or facilitated through an information system or electronic communications system.
[26] Osama Ahmed Badr, **Consumer Protection in Electronic Contracting (Comparative Study)**, New University Publishing House, Egypt, 2005, p. 25.
[27] See Article 17 and 18 of Act 09-04, which contains special rules for the prevention and control of crimes related to information and communication technologies.