

# ELECTRONIC PAYMENTS IN ALGERIA: BETWEEN PRACTICE AND CONFRONTATIONAL APPROACHES

Mohamed Lemaini<sup>1</sup>, Djamel Mecheri<sup>2</sup>

<sup>1,2</sup>University Mohamed Kheidher Biskra (Algeria).

The Author's E-mail: [mohamed.lemaini@univ-biskra.dz](mailto:mohamed.lemaini@univ-biskra.dz)<sup>1</sup>, [djamel.mecheri@univ-biskra.dz](mailto:djamel.mecheri@univ-biskra.dz)<sup>2</sup>

Received: 01/2023      Published: 05/2024

## Abstract:

Given the importance of electronic payment methods in the promotion and development of electronic banking, many countries have paid attention to this aspect by preparing all the necessary conditions and providing all the necessary material and human resources. This is in order to address the issue of information security and the increasing risks associated with electronic payments, which can be classified into organisational, security or operational risks, as well as risks caused by third parties or consumers themselves. There are also legal risks associated with electronic payments, and efforts have been made to protect against them.

In this context, various legislations, including the Algerian legislation, have issued a number of laws related to electronic signatures and certification, despite the existence of some shortcomings and difficulties that need to be overcome as soon as possible to reach the level of developed countries.

**Keywords:** Electronic payment; Electronic payment risks; E-commerce; Cybercrime; Security protection.

## Introduction:

The recent technological and digital revolution has been one of the main driving forces behind the significant developments in the economic and financial fields, particularly in the area of global financial and banking transactions. Consequently, the issue of electronic payment systems has emerged as a prominent outcome of these technological advances.

In this context, the issue of security and protection has become one of the main guarantees and challenges of electronic payment methods. This is due to the lack of information security, which is considered one of the main obstacles to the adoption of e-commerce and keeping pace with global developments in the digital realm.

Electronic payment is a form of payment that has evolved on the Internet, which represents the traditional electronic payment methods we use in our daily lives. The fundamental difference between the two is that electronic payment processes are entirely electronic and do not involve the physical transfer of funds or currency. Electronic payment is essentially “the process of digitally transferring funds, essentially the price of a good or service, using computer equipment and transmitting data over a telephone line, network or other data transmission method<sup>1</sup>.

The expansion of e-commerce has led to a decline in the role of paper money and traditional payment methods in favour of electronic payments. Cash has been the main means of settling financial transactions, and payments have been made in cash or by alternative means such as cheques and other traditional payment methods. However, these methods are not suitable for facilitating remote transactions in a non-physical environment, such as electronic contracts concluded over the Internet, where paper transactions disappear.

It is therefore important to innovate payment methods that are compatible with the nature of e-commerce, where payment is made electronically. If the customer can pay for the good or service using the same traditional methods used in contracts between absent parties, such as sending a cheque by post or fax or sending data from their bank account, these methods are not suited to the privacy and speed requirements of e-commerce. Therefore, the importance of relying on electronic payment through a unified wireless communication network via the computer became evident.

In order to keep pace with this development, Algeria had to develop its communication system through the electronic payment system and modernise its banking infrastructure. This was done by enacting Law 90/10, Article 112 of which stipulates that a means of payment can be considered to be a payment instrument that allows anyone to transfer funds, regardless of the technical basis or procedure used.

Based on the above, the research problem can be formulated as follows:

What are the risks associated with the use of electronic payments and how can they be addressed in accordance with Algerian legislation?

In order to answer this question, the research was divided into two sections. The first section deals with the risks associated with the use of modern electronic payment methods, while the second section deals with the protection against the risks associated with the use of electronic payment methods under Algerian legislation.

### **The first section: the risks associated with the use of electronic payment methods.**

The most important aspect highlighting the importance of electronic payment methods is their distinct characteristics that distinguish them from traditional payment methods. These include their international nature, as they are an accepted means of payment in all countries and allow transactions between users worldwide. They are also characterised by the use of electronic money and remote electronic transaction settlement.

With the development of the banking industry and the increased reliance on financial services technology, electronic payment methods have become associated with risks. These risks can be divided into two main categories: regulatory risks and legal risks. The first sub-section deals with regulatory risks, while the second sub-section deals with legal risks.

#### **Subsection 1: Regulatory or safety risks**

The anticipated risks associated with the use of electronic payment methods may arise from deficiencies in the operation of the payment instrument, such as accidental malfunctions or situations involving the loss of the payment instrument or the misuse of these methods.

#### **First: Risks arising from frequent malfunctions of the payment instrument during use:**

The consumer suffers losses as a result of the malfunctioning of the payment instrument. Examples of such losses include the loss of electronic funds. Another common malfunction is the lack of proper maintenance, which leads to the disruption of these systems<sup>2</sup>.

#### **Secondly, electronic piracy:**

Electronic payment piracy is counterfeiting, as the perception of its occurrence in this type of card involves the use of one of the counterfeiting methods, such as adding, deleting, forging words, numbers, signatures, seals or fingerprints<sup>3</sup>. Forgery can be either total, by completely forging the electronic payment card, or partial, by forging parts of it. The counterfeiting can take place in the messages, documents or by issuing genuine payment instruments with

counterfeit documents. In general, electronic piracy is one of the most dangerous problems of technological and scientific development, which is a double-edged sword.

**Third: Loss of the electronic payment instrument**

In many cases, a person's card may be stolen, or the data or PIN code may be compromised, or even fraudulently manipulated by electronic means, resulting in the card being used for various transactions, such as online shopping<sup>4</sup>. In the case of a cancelled credit card, the loss may occur through no fault of the cardholder. Each cardholder must use the card personally and individually and keep the PIN code strictly confidential.

**The second issue: The legal risks of electronic payments**

Having dealt with the various regulatory and security risks of payment methods, such as electronic piracy, loss of the payment instrument or malfunctions in its operation, we now come to a second type of risk, namely the legal risks, which mainly concern the violation of privacy and money laundering through electronic payment methods.

**First: Violation of privacy:**

The protection of individuals' personal data is linked to the privacy of their lives and daily transactions. The personal or individual data related to electronic contracts are the data of the contracting parties, including consumers or even their transacting partners, such as merchants and industrialists, among others<sup>5</sup>. With regard to the respect of the privacy of the consumer in electronic payment, it is necessary to respect the confidentiality of the data of the customers as consumers and to respect their right to privacy after the publication or disclosure of any data related to their personality and their private banking data. They also have the right to conceal all their banking and financial transactions by hiding any information relating to the value of their balance or financial transfers. Accordingly, any misuse of this information and its diversion or monitoring without their knowledge is prohibited, as the privacy of individuals and their secrets are exposed to aggression and fraud in the Internet world, and these attacks may increase with the increase in the use of electronic payment, especially with the technological development in the fields of piracy and theft of other people's accounts without their knowledge.

**Second: The use of electronic payment methods in money laundering:**

The development of financial transfer systems and the use of computer networks to connect all markets, as well as the ease of transferring large sums of money, especially with technological development, digitalisation and the use of the Internet and computers, has both positive and negative aspects. This is particularly true when it comes to transferring funds within a country or even across borders, which has led to an increase in e-commerce and, consequently, money laundering<sup>6</sup>.

Money laundering enables the investment or further transfer of funds from illegal sources into legitimate channels where the original source cannot be identified as legal or not, as in the case of drug trafficking, hostage-taking, gambling, human trafficking, tobacco, weapons, tax evasion and other illegal activities<sup>7</sup>.

Money laundering or whitewashing is a crime committed by organised groups involving a number of individuals, each with a role in the process. They operate in an organised manner according to a highly precise, complex and secretive system and structure<sup>8</sup>. Money laundering activities corrupt banks due to the illegal transactions that take place within them,

leading to a sharp fall in the share prices of the stock exchanges that receive these funds, all of which is done in secret.

**The second issue: Protection against the risks created by the use of electronic payment methods under Algerian legislation**

Information systems have contributed positively to the development of the banking sector and payment methods, but they have also created various negative risks. It is therefore necessary to limit these risks by means of specific measures and procedures.

**The first requirement: Proof through electronic payment methods:**

With the emergence of transactions carried out using modern technologies and at a distance, there are electronic documents that can vary from fax messages, computer output, e-mail messages, Internet messages and other modern documents.

**First: Electronic writing**

Writing is one of the most important means and methods of evidence in modern times, as it provides the parties with guarantees that other forms of evidence do not. Electronic writing has a place in the rules of evidence as long as it is signed. Many countries have recognised electronic evidence.

The Algerian legislator has included the issue of electronic evidence in the Algerian Civil Code<sup>9</sup>, as stipulated in Article 323bis1 and Article 327, paragraph 2. In this field, electronic certification also contributes to ensuring the integrity and security of the electronic exchange of data in electronic payment, whether in terms of parties, organisers, subject matter or date, in order to create a secure electronic environment for transactions over the Internet.

**Second, the electronic signature:**

The electronic signature is a digital certificate used to send any document, commercial contract, pledge or confirmation. It consists of characters, numbers, images, sound or an electronic processing system. The use of the electronic signature aims to increase the level of security and privacy for parties transacting over the Internet<sup>10</sup>.

The Algerian legislator has defined the electronic signature as “data in electronic form attached to or logically associated with other electronic data and used as a means of authentication”. However, while the Algerian legislator has recognised the electronic signature as a means of authentication, it has not specified the method by which it is to be used<sup>11</sup>.

The electronic signature is not considered part of the document or written instrument. Rather, by performing a storage function and giving credibility to the electronic document or instrument through this storage, this document may acquire credibility with third party recipients<sup>12</sup>.

The electronic signature can take different forms. It may take the form of a biometric signature based on the physical, physiological or behavioural characteristics of the signer. It can also take the form of a secret digital code or set of characters. It may also take the form of, among others, the use of an electronic pen. These forms vary in their degree of reliability and the level of guarantee they provide, depending on the procedures used to issue them, the security measures and the underlying technologies. The legal validity of the electronic signature is of great importance for electronic evidence and thus for the protection of the rights of parties transacting electronically<sup>13</sup>.

In addition, the Algerian legislator has adopted the electronic signature in accordance with Articles 323a and 327 of the Algerian Civil Code. The Algerian legislator introduced the electronic signature for the first time in 2005 by law 05-10 of 20 June 2005. However, the Algerian legislator distinguished between two types of electronic signatures by Executive Decree 07-162 of 30 May 2007. The Algerian legislator is considered to have been significantly delayed in adopting a specific law regulating the provisions of electronic signature and certification, namely Law No. 15-04<sup>14</sup>.

The role of the electronic signature is manifested in all types of electronic payment methods through its use in electronic banking transactions on smart cards and cash withdrawals, for example. It is also used in electronic messages exchanged between the bank and the customer and in establishing the digital identity of the holder of the electronic payment instrument. It also helps to express the will of the signatory<sup>15</sup>.

### **The Second Requirement: Special procedures to address the risks of electronic payments:**

Electronic payment methods have emerged and spread thanks to the information revolution. However, in order to address the risks they face, a number of procedures have been established to preserve and protect them, mainly consisting of special procedures to combat security risks and legal risks.

#### **First: Combating security risks:**

Faced with the illegal growth of electronic payment methods, which has a profound impact on user confidence, it is necessary to adopt specific procedures to combat these risks, including

#### **Encryption:**

Encryption can be defined as a complex computational process that converts readable text into unreadable symbols and signals in such a way as to achieve information security and confidentiality. The aim of encryption is to achieve the principles of reliability, credibility, data integrity, authentication of the data source and non-repudiation of actions taken.

The main objective of message encryption and electronic signatures is to achieve trust, security and confidentiality in electronic transactions. To achieve this trust and confidentiality, there must be a neutral third party that authenticates the identity of the parties and establishes the relativity of the electronic signature to its issuer by linking individuals to their public keys<sup>16</sup>.

Encryption plays a role as a measure to secure electronic transactions in general, as it provides confidentiality and privacy for data. Encryption is a mechanism by which understandable information is transformed into unintelligible information through the use of reversible secret protocols, i.e. it can be restored to its original state<sup>17</sup>.

Electronic authentication involves the provision of electronic certification by a recognised authority. Electronic authentication is a process that incorporates security aspects for exchanging information over the Internet and helps to identify key holders by issuing digital certificates from a certification authority. The purpose of electronic certification is to confirm that the electronic signature was issued by the party to whom it was assigned and that the signature is valid. As such, electronic authentication plays an important role in validating payment orders resulting from the use of electronic payment cards by encrypting the payer's information to ensure the integrity of its contents. The number entered by the cardholder is

sent to the certification authority, which then sends it to the other party, who holds the public key, for decryption, thus avoiding message repudiation. Certification proves the link between the parties<sup>18</sup>.

The Algerian legislator has defined the source of the electronic signature as “any natural or legal person who issues qualified electronic certification certificates and may provide other services in the field of electronic certification”. However, this definition has been criticised as natural persons cannot provide certification services as they require complex techniques and equipment<sup>19</sup>.

### **Administrative Oversight to Prevent Electronic Risks:**

Administrative oversight is seen as a protective barrier against any intrusion into electronic payment systems, through the adoption of special measures that primarily involve restrictions on the values stored on payment instruments.

Second: Combating legal risks: In order to ensure that privacy is not violated and to combat money laundering through the use of electronic payment methods, the following measures have been taken to address these legal risks:

#### **1- Combating the risk of invasion of privacy**

Several legal texts have been found in various legislations addressing these risks. However, while the Algerian legislator has referred to guaranteeing the rights inherent to personality and has enshrined in the Constitution the State’s guarantee of non-violation of human dignity, and has criminalised the violation of privacy, these various texts are criticised for failing to define and specify these rights relating to privacy, particularly with regard to electronic privacy<sup>20</sup>.

#### **2- Fighting money laundering through electronic means of payment:**

Given the seriousness of this crime, international efforts to combat the phenomenon of money laundering have been unified and several countries have adopted specific measures to limit the spread of this phenomenon, such as restricting the areas most active in money laundering and strengthening cooperation between international and national supervisory authorities<sup>21</sup>.

At the national level, the Algerian legislator, like other countries, has adopted specific legislation to combat the crime of money laundering, such as Law No. 06-01 on the prevention and fight against corruption and Law No. 12-02 on money laundering and terrorist financing, which introduced additional preventive and procedural measures<sup>22</sup>. The legislator also provided for the establishment of the High Authority for Transparency, Prevention and Fight against Corruption in the fourth section of the fourth chapter of the Constitutional Amendment 2020.

#### **The conclusion:**

The electronic means of payment in the Algerian banking system are mostly traditional and do not correspond to the realities of the new world. However, in line with Algeria’s efforts to keep pace with events and technological developments in the banking sector, especially in the banking sector, and in the pursuit of electronic banking, Algeria has begun to introduce and adopt some modern payment methods, the most important of which are bank cards.

Although electronic payment in Algeria is progressing at a steady but slow pace, it is also fraught with risks because it relies on the Internet, and this has created new challenges in controlling the risks associated with electronic payment methods. For this reason, a number of specific measures and legal procedures have been identified to address the risks of

electronic payment methods, as the development and progress of institutions in terms of banking intermediation is linked to the development of electronic payment methods.

Finally, we propose a series of **recommendations** that can be summarised as follows:

- Simplify procedures by reducing risks and errors, i.e. eliminate procedures in the implementation of all accounting operations for the collection of funds.
- Provide a legal framework for all forms and types of electronic payments and cover all specific procedures and legal processes to address the risks of electronic payment methods.
- Improve the cash flow of banks and institutions, including individual accounts, by making payments to their accounts in a short time, thus encouraging them to work with electronic payment cards.
- The delay in updating payment systems is one of the main obstacles to attracting investment, so it is necessary to update information and payment systems, modernise financial and banking transactions and update methods of information processing.
- The Algerian banking system is still far from the reality of electronic payment methods in developed countries, which discourages investors from coming to Algeria.
- The Algerian legislator must oblige public entities to use electronic payment methods in their financial transactions with citizens, such as paying taxes and settling bills, so that citizens can trust them and this will help in the fight against tax evasion.
- Legislation must be enacted to address the risks of electronic payments by adopting special procedures to limit the spread of money laundering, such as restricting the most active areas of money laundering and strengthening cooperation between various international and national regulatory authorities.
- The need to create a specialised department for cybercrime and electronic investigations, in order to be able to legally and technically access electronic evidence and use specialised software for the maintenance of equipment or information protection software itself.
- Work to ensure the security of the electronic exchange of data in electronic payments, whether in terms of parties, content or subject, in order to create a secure electronic environment for transactions over the Internet.
- To improve the quality and increase the flow of the Internet in order to facilitate the work of banks and financial institutions and to save time and speed in financial and banking transactions.
- The Algerian legislator must take into account the specific nature of electronic payments and the role that the electronic certification authority will play, and must therefore take care when drafting the regulatory texts that will govern these bodies.
- Algerian banks should encourage the use of electronic payment cards with certified electronic signatures and require customers to do so when opening bank accounts.

**Footnotes:**

---

<sup>1</sup> - Ben Rjidal Jaouheur, "The Internet and e-commerce", Master's thesis, Department of Management Sciences, Faculty of Economics and Management Sciences, University of Algiers, 2002, p. 83.

<sup>2</sup> - Karima Chaïb Baacha, "Mechanisms for Protection Against the Risks of Electronic Payment in Algerian Legislation", Algerian Journal of Public Policies, Volume 07, Issue 02, December 2018, p. 39.

<sup>3</sup> - Suleiman Ahmed Nadal, "Crimes Related to the Use of Credit Cards Over the Internet", article in the Journal of the Security Media Center, no date, p. 04.

<sup>4</sup> - Karima Chaïb Baacha, op. cit., p. 39

- <sup>5</sup> - Riad Fath Allah Basala, "Credit Card Crimes", Dar Al-Shorouk, Cairo, first edition, Egypt 1995, p. 85.
- <sup>6</sup> - Hawalaf Abdessamed, "The Legal System of Electronic Payment Means", Doctoral Thesis, Faculty of Law and Political Science, University of Abou Bakr Belkaïd Tlemcen, 2015, p. 354.
- <sup>7</sup> - Sayed Ahmed Al-Zamli, "The Role of Electronic Money in the Money Laundering Process", Damascus Magazine, Issue 01, Syria 2010, p. 588.
- <sup>8</sup> - Hawalaf Abdessamed, previous reference, p. 369.
- <sup>9</sup> - Roya Fayez Al-Faoury, Enas Mohammad Qutaishat, "The Crime of Public Money Laundering and Its Legal Aspects", Dar Wael Publishing, First Edition, 2002, p. 70.
- <sup>10</sup> - Decree No. 75-58 of 26 September 1975 establishing the Civil Code, as amended and supplemented by Law No. 05-10 of 20 June 2005, Official Journal No. 44.
- <sup>11</sup> - See Article 2 of Law No. 04-15 on electronic signatures and certification, Official Journal No. 16 of 2015.
- <sup>12</sup> - Mohamed Zidan Mohamed Hamou, "Requirements for Banking Information Security in the Internet Environment", Sixth Conference on the Secure Information Environment, Riyadh, 2010.
- <sup>13</sup> - Omar Mohamed Abu Bakr bin Younis, "Crimes Arising from the Use of the Internet", Doctoral Thesis, Faculty of Law, Ain Shams University, Egypt, 2004, p. 14.
- <sup>14</sup> - Decree No. 07-162 of 30 May 2007 regulating the activity of electronic certification, Official Gazette No. 37 of 2007.
- <sup>15</sup> - Ghezali Nazihah, "The Legal Mechanisms for Protecting Electronic Payment Means in Algerian Legislation", Journal of Political and Administrative Research, University of Mohamed Lamine Debaghine Sétif 2, issue 10, p. 290.
- <sup>16</sup> - Alaa Faraj Al-Tahir, "E-Government Between Theory and Practice", Dar Al-Raya for Publishing and Distribution, first edition 2010, p. 80.
- <sup>17</sup> - See Article 2 of Law No. 15-04 on the Electronic Signature.
- <sup>18</sup> - Ghezali Nazihah, "The Legal Protection of the Effectiveness of the Card Payment Order in Algerian Law", Journal of Thought, Faculty of Law and Political Science, University of Mohamed Lamine Debaghine, Sétif 2, Issue Seventeen, May 2018.
- <sup>19</sup> - Saadi Youcef, "The Evidential Value of the Electronic Signature in Algerian Legislation (A Study in the Light of the Provisions of Law 15-04)", Journal of Ijtihad for Legal and Economic Studies, University Centre of Tamanrasset, Institute of Law, Issue 11, January 2017, p. 84.
- <sup>20</sup> - Karima Chaïb Baacha, op. cit., p. 45.
- <sup>21</sup> - Rjdal Hawalafs Abdessamed, op. cit., p. 443.
- <sup>22</sup> - Sameh Abdel Wahid Al-Nehamy, "Contracting over the Internet: A Comparative Study", Dar Al-Kutub Al-Qanuniyyah, Cairo, Egypt 2008, p. 412.

## **The reference list:**

### **I. Legislative texts**

#### **Laws and decrees:**

- Law No. 15-04 on electronic signatures and certification, Official Journal No. 16 of 2015.
- Order No. 75-85 of 26.09.1975 establishing the Civil Code, amended and supplemented by Law No. 05-10 of 20.06.2005, Official Journal No. 44.

#### **Decrees:**

- Decree No. 07-162 of 30 May 2007 regulating the activity of electronic certification, Official Journal No. 37 of 2007.

### **III. Books:**

- Sameh Abdel Wahid Al-Nehami, *Online Contracting: A Comparative Study*, Dar Al-Kutub Al-Qanooneyah, Cairo, Egypt, 2008.
- Riad Fathallah Bassaleh, *Credit Card Crimes*, Dar Al-Shorouk, Cairo, first edition, Egypt, 1995.
- Rua Fayez Al-Faouri, Inas Muhammad Qatishat, *The Crime of Money Laundering and the Legal Edition*, Dar Wael for Publishing, first edition, 2002.
- Alaa Faraj Al-Taher, *E-Government Between Theory and Practice*, Dar Al-Raya for Publishing and Distribution, first edition, 2010.
- Sameh Abdel Wahid Al-Nehami, *Online Contracting: A Comparative Study*, Dar Al-Kutub Al-Qanooneyah, Cairo, Egypt, 2008.

### **IV. Journal articles:**

- Karima Chaibi Basha, *Mechanisms for protection against the risks of electronic payment in Algerian legislation*, Algerian Journal of Public Policy, Volume 07, Issue 02, December 2018.
- Suleiman Ahmed Nadal, *Crimes related to the use of credit cards on the Internet*, article in the magazine of the Security Media Center, no date.
- Sayed Ahmed Al-Zamili, *The Role of Electronic Money in the Money Laundering Process*, Damascus Journal, Issue 01, Syria 2010.
- Mohammed Zaidan, Mohammed Hamou, *Requirements for the Security of Banking Information in the Internet Environment*, The Sixth Conference on the Information Security Environment, Riyadh, 2010.
- Ghazali Nazeeha, *The Legal Mechanisms for Protecting Electronic Payment Methods in Algerian Legislation*, Journal of Political and Administrative Research, University of Mohamed Lamine Debaghine, Setif 2, Issue 10.
- Ghazali Nazeeha, *The Legal Protection for the Effectiveness of the Card Payment Order in Algerian Law*, Al-Fikr Journal, Faculty of Law and Political Science, University of Mohamed Lamine Debaghine, Setif 2, Issue 17, May 2018.
- Saoudia Youcef, *The Extent of the Probative Force of the Electronic Signature in Algerian Legislation (A Study in Light of the Provisions of Law 15-04)*,

Journal of Ijtihad for Legal and Economic Studies, University Center of Tamanghasset, Institute of Law, Issue 11, January 2017.

## **V. Theses and Dissertations:**

### **Doctoral theses:**

- Houalouf Abdessamed, The Legal System of Electronic Payment Methods, Doctoral Thesis, Faculty of Law and Political Science, Abou Bakr Belkaïd University, Tlemcen, 2015.

- Omar Mohamed Abou Bakr Bin Younes, Crimes Arising from the Use of the Internet, Doctoral Thesis, Faculty of Law, Ain Shams University, Egypt, 2004.

### **Master's thesis:**

- Ben Rjedal Jouheur, "The Internet and E-Commerce", Master's Thesis, Department of Management Sciences, Faculty of Economics and Management Sciences, University of Algiers, 2002.