

THE NEW ISSUES RAISED BY THE DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES AND THEIR IMPACT ON ALGERIA (NEW CYBER THREATS TO ALGERIA)

SOULEYMAN KANKARA¹, HASSEN BEN ABDELKABIR².

¹University of Bechar-Tahri Mohamed, Business Law (Algeria).

²University of Ahmed DRAIA Adrar, Business Law (Algeria).

Received: 16/09/2023

Published: 10/11/2023

Abstract:

This research paper sheds light on the issue of cybersecurity in Algeria and the legal challenges posed by this modern concept. Undoubtedly, the tremendous advances in technology and electronic communications have led to the continuous development of methods of fraud and attacks on various technological infrastructures of different countries. Algeria is one of the countries facing such threats. Therefore, this research paper aims to highlight the conceptual framework of cybersecurity and to elucidate the attitude of Algerian legislation towards it.

The issue of cybersecurity is of great importance, whether it is related to the economic, social, cultural, political or security spheres. It is therefore of the highest priority to delve into a detailed explanation of this concept, which has become the talk of the town, especially in the light of significant changes in the technological field. This underlines the importance of studying this topic in order to enlighten the readers and the different segments of society about the meaning of this term.

Keywords: *cybersecurity, cybercrime, technological advances, credit cards.*

Introduction:

Cybersecurity is one of the issues that raises numerous legal challenges, especially with the significant growth in the technological field. This immense development in the field of the information revolution has contributed to the evolution of crimes committed in this field. Today, it is undeniable that cybercrime has become one of the most threatening crimes for societies that do not have the necessary infrastructure to combat such offences. Digital criminals exploit vulnerabilities to commit various crimes. One area that is subject to various types of attack is the credit card system. The most common crimes in this area include credit card forgery and money laundering via the Internet using credit cards.

It is therefore necessary to provide the necessary legal protection to defend against or mitigate these attacks. This will help to protect the rights of users of these modern electronic payment instruments and encourage people to engage in such transactions. This can only be achieved by ensuring cybersecurity.

Consequently, our research paper focuses on the problem statement: To what extent has the Algerian legislator addressed the issue of cybersecurity and its challenges in different dimensions in Algeria? In other words, how has the Algerian legislator addressed the issue of cybersecurity?

Section One: The conceptual framework of credit cards

In this section we highlight some issues related to the conceptual framework of credit cards, focusing in particular on their definition (subsection 1). We also address the distinction between credit cards and other electronic payment instruments (subsection 2). We also discuss the components of a credit card (subsection 3). Finally, we examine the main organisations responsible for issuing credit cards (subsection 4).

First section: Definition of credit cards

Subsection 1: Linguistic definition of credit cards

The term card refers linguistically to a small piece of paper. Ibn Al-A'rabī and others have described it as a small card on which the quantity of a particular item, whether a physical object or a value, is

recorded. In a narration from Ibn Abbas (may Allah be pleased with him), he advised a woman who asked him a question to write it on a (small piece of paper). In another narration of Abdullah, it is mentioned: "On the Day of Resurrection, a person will be brought out and ninety-nine registers will be presented containing his sins, but he will also be given a card bearing witness to the statement, 'There is no god but Allah,' which will outweigh the registers."¹

Second section: The legal definition of credit cards

They can be defined as a contract in which the bank undertakes to cover a certain credit limit for the customer. The customer is then obliged to use the credit card for the purpose for which it was issued, presenting it to merchants who accept transactions with it in order to pay for various goods and services. This is done by means of special devices used by the merchant to obtain the necessary information, and then the bank that issued the card settles the payment².

Third section: The legal definition of credit cards

Credit cards are defined as a contractual agreement between two parties: the financial institution (the card issuer) and the customer (the cardholder). In this agreement, the financial institution undertakes to pay the financial amounts owed by the customer to commercial entities. The customer, in turn, is obliged to reimburse the financial institution for the amounts paid on his behalf³.

Fourth section: Definition of credit cards from an economic perspective

Credit cards are cards issued by banks to their customers on the basis of information relating to the customer's name and card number. These cards allow customers to use them in various commercial establishments, including service providers and others. After using these services, a list of items purchased and their prices is sent to the bank for payment settlement⁴.

Section Two: How credit cards differ from other electronic payment instruments

This section highlights some of the differences between credit cards and other electronic payment instruments:

Subsection 1: The difference between credit cards and electronic cheques

Credit cards are susceptible to various forms of manipulation due to their reusable nature. This differs from electronic cheques, where each cheque is independent and has a unique number. In addition, electronic cheques are typically used only once in a commercial transaction. These factors help to prevent fraud and manipulation of electronic cheques⁵.

From the information provided, it is clear that payment by electronic cheque is considered to be the safest and most secure for the cardholder. This is because it is not susceptible to manipulation or fraud, since the electronic cheque is used only once in the transaction. However, the situation is different with credit cards, which are more vulnerable to manipulation and misuse of their numbers by cybercriminals. It is undeniable that the most common crimes involving credit cards are counterfeiting and money laundering.

Second: The difference between credit and debit cards

The fundamental difference between debit and credit cards is that a debit card does not provide the cardholder with any credit from the issuing bank. In addition, the cardholder does not have a grace period for payment, unless it is an indirect payment situation. In such cases, the debit cardholder

¹- Abi Al-Fadl Jamal al-Din Muhammad ibn Mukram Ibn Mundhur, the African Egyptian: "Lisan al-Arab," Volume 1, Fourth Edition, published by Dar Sader, Beirut in 2005, page 103.

²- Jalal Ayed al-Shawra: "Electronic Payment Methods," First Edition, First Release, published by Culture Publishing and Distribution House, Amman, Jordan in 2008, page 24.

³- Omar Yusuf Abdullah Ababneh: "Payment by Installment Using Credit Cards," First Edition, published by Dar al-Nafa'is for Publishing and Distribution, Amman, Jordan, in 2008, page 41.

⁴- Fahmi Mahmoud Shukri: "Commercial and Economic Dictionary," First Edition, published by Dar Osama for Publishing and Distribution, Amman, Jordan, in 2009, pages 335-336.

⁵- Musa Isa Al-Aamiri: "The Smart Check," a research paper presented at the Banking and Law Business Conference, Volume 1, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, May 10-12, 2003, page 94.

benefits from the extended period between the date of purchase and the date on which the invoices are sent to the bank⁶.

Building on this, the primary role of a debit card is to serve as a payment instrument for the purchase of goods and services by the customer, without providing credit to the legitimate cardholder.

Third section: Parties involved in credit cards

Subsection 1: The International Card Association

The International Card Association is a global organisation responsible for establishing and overseeing the card system. It grants membership to banks interested in issuing credit cards and facilitates financial settlements between them through a designated global bank chosen by the organisation. In addition, the International Card Association acts as an arbitrator to resolve any disputes that may arise between the parties involved⁷.

Second: Issuing bank

The issuing bank is the entity responsible for issuing the credit card to the cardholder based on an authorised licence from the International Card Association, of which it is a member. The issuing bank facilitates the payment of the value of goods to merchants who accept transactions with the card⁸. In this sense, it can be said that the bank is the authorised institution to issue the credit card to the cardholder (i.e. the legitimate holder of the card) after the necessary procedures to obtain the card have been completed. The bank then pays for the goods and services purchased by the customer in exchange for a specified fee.

Third: Merchants

Merchants are the businesses that accept credit card payments. They provide goods and services to customers and then settle their debts with the bank.

Fourth: Legitimate cardholder

The legitimate cardholder is the person in whose name the credit card is issued. They obtain the card by following certain procedures that allow them to acquire the card. The cardholder is responsible for paying the annual fee. It's important to note that the cardholder's obligations vary depending on the type of credit card and the terms and conditions attached to it⁹.

Fourth section: Major organisations involved in the issuance of credit cards

Subsection 1: The Visa organisation

Visa is a non-profit organisation responsible for issuing Visa cards. Its headquarters are in San Francisco. Visa allows any bank worldwide to become a member, subject to certain membership criteria. The Visa organisation coordinates and facilitates the relationship between its member banks¹⁰.

⁶- Nazih Mohammad Al-Sadiq Al-Mahdi: "Towards a General Theory of Credit Card Systems from a Legal Perspective," a research paper presented at the Banking and Law Business Conference, Volume 2, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, May 10-12, 2003, page 758.

⁷- Mohamed Abdul Halim Omar: "Credit Cards and the Relationships Arising from Their Use between Sharia and Law," a research paper presented at the Banking and Law Business Conference, Volume 2, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, May 10-12, 2003, page 672.

⁸- Al-Sadiq Mohamed Al-Amin Al-Darir: "Credit Cards," a research paper presented at the Banking and Law Business Conference, Volume 2, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, May 10-12, 2003, page 640.

⁹- Abdul Hamid Al-Ba'li: "Banking Credit Cards - Artistic Depiction and Jurisprudential Graduation (A Comparative Analytical Study)," a research paper presented at the Banking and Law Business Conference, Volume 2, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, May 10-12, 2003, page 702.

¹⁰- Hussein Mohammed Al-Shibli and Mohannad Fayez Al-Dweikat: "Forgery and Fraud with Credit Cards," First Edition, Majdalawi Publishing and Distribution House, Jordan 2009, page 49.



The Visa network includes more than one million ATMs worldwide. It supports the use of Visa and Visa Electron cards, and these machines are distributed in around 160 countries. As a result, Visa cards are widely accepted throughout the world because of the privileges they offer cardholders¹¹.

Second: Mastercard organisation

The Mastercard organisation is Visa's second largest competitor and offers various categories of cards such as Mastercard Silver, Business Mastercard and Cirrus cards, which are linked to cash withdrawals from ATMs worldwide. In 1990, the Mastercard organisation had 163 million member institutions and its cards were accepted by over 9.4 million merchants. Mastercard also owns the Banknet network of payment systems¹².

In this context, it is worth noting that the Mastercard organisation achieved significant results in various spending sectors in 2004. The number of Mastercard cards used by legitimate cardholders worldwide reached 679.5 million, with 16.7 billion financial transactions. The volume of purchases made with Mastercard reached a growth rate of 12.4% in 2005¹³.

Third: The American Express organisation

The American Express organisation is a financial institution that issues American Express cards and oversees their issuance. It does not grant issuing licences to other banks or financial institutions, nor does it allow the name of another bank to appear on its cards, except for one type of card, the American Express Gold card. The organisation is responsible for issuing the following cards: American Express Green Card, American Express Gold Card and American Express Platinum Card¹⁴.

It is worth noting that by the end of 2005, American Express' revenues had exceeded USD 29.1 billion. This increase can be attributed to the changing spending behaviour of cardholders. As a result, the company issued 9.4 million new cards¹⁵.

Fourth: Diners Club International Organisation

The Diners Club International organisation is a global programme that pioneered the credit card industry in 1950. Its headquarters are in Chicago, USA. It offers extensive expertise in the field of credit cards. The organisation provides strategic guidance to its global network, which spans more than 200 countries. Diners Club International uses advanced technological resources to adapt to the changing business environment. Diners Club International has more than eight million cardholders¹⁶.

The second topic: Credit card fraud methods and techniques

Cybercrime against credit card systems uses various methods and techniques. Before we look at these crimes, let's first discuss the concept of cybercrime in section 1. Then, in section 2, we'll define cybersecurity. In section 3, we'll look at credit card fraud as a crime. Section 4 focuses on the definition of money laundering through the Internet. Finally, in section 5, we'll look at money laundering via the Internet using credit cards.

The first branch: Content of cybercrime

First: Definition of cybercrime

Cybercrime is defined as "any crime that can be committed through a computer system or network, and in principle includes all crimes that can be committed in an electronic environment¹⁷".

¹¹- Nasreen Abdul Hamid Nabi: "The Electronic Aspect of Commercial Law," First Edition, Ma'arif Establishment, Alexandria, 2008, page 59.

¹²- Mansour Ahmed Haji Al-Azahari: "Cash Withdrawal Card (ATM Card)," a research paper presented at the Banking and Law Business Conference, Volume 1, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, May 10-12, 2003, page 365.

¹³- Nasreen Abdul Hamid Nabi: "The previous reference," pages 58 and 59.

¹⁴- Issam Hanafi Mahmoud Mousa: "The Legal Nature of Credit Cards," a research paper presented at the Banking and Law Business Conference, Volume 2, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, May 10-12, 2003, page 855.

¹⁵- Nasreen Abdul Hamid Nabi: "The previous reference," page 58.

¹⁶- Radwan Ghoneim: "Credit Cards between Banking Legal Status and Jurisprudential Grounding," First Edition, Dar Al-Fikr Al-Jamei, Alexandria 2014, pages 94 and 95.

¹⁷- Nahla Abdel Qader Al-Mumani: "Cyber Crimes," Second Edition, Culture Publishing and Distribution House, Amman, 2010, page 50.



It is further defined as all crimes committed through the virtual domain using electronic means.

Second: Cyber threat methods

Cyber threats are defined as "any action aimed at disrupting the security of an information system by compromising its availability, integrity or confidentiality¹⁸".

Cyber threats can use the following methods: "service disruption, information destruction or modification, network espionage, and destruction of assets and information."¹⁹

The second branch: Cybersecurity content

First: Definition in Algerian law

Algerian legislation defines cybersecurity in Article 10, paragraph 3 of Law No. 18/04. It states that cybersecurity is "the set of tools, policies, security concepts, security mechanisms, risk management guidelines, practices, guarantees and technologies that can be used to protect electronic communications against any event that could compromise the availability, integrity and confidentiality of stored, processed or transmitted data²⁰".

Second: Definition in Moroccan law

Moroccan legislation defines cybersecurity in Article 2(1) of Law No. 20/05 on Cybersecurity. It states: "In the context of this law, the following meanings shall apply: Cybersecurity refers to a set of measures, procedures, security concepts, risk management approaches, practices, training, best practices and technologies that enable an information system to resist events related to the cyber domain that could compromise the availability, integrity and confidentiality of stored, processed or transmitted data, as well as related services provided by that system or allowing access to it²¹".

The third branch: Credit card fraud

Credit cards, in their various forms, are susceptible to forgery, which is a widespread crime, especially in credit card transactions. Based on this, we will look at the definition of credit card forgery (first), the elements of the crime of credit card forgery (second), the types of forgery that credit cards can be subjected to (third), and finally the penalties for credit card forgery in some laws (fourth).

First: Definition of credit card forgery

Before discussing the definition of the crime of credit card forgery, it is necessary to distinguish between two things:

1- The extent to which the visually displayed data on the credit card is considered part of the forged document.

Based on the prevailing opinions of Islamic jurisprudence, it is believed that the data appearing on the front and back of the credit card fall within the category of documents and therefore the crime of forgery can be committed on them²².

2- Non-visible data and the applicability of the concept of forgery to them

There is a difference of opinion in Islamic jurisprudence regarding the consideration of non-visible data recorded on the credit card as part of the document to be forged. The prevailing opinion in Egyptian jurisprudence is to exclude the application of the concept of forgery to electronically recorded data on the card²³.

Second: Elements of the crime of credit card forgery

1. Material element (act of use):

¹⁸- Law No. 20/05, dated July 30, 2020, regarding Cybersecurity, Official Gazette of the Kingdom of Morocco, Issue 6904, page 4160.

¹⁹- Bara Samir: "Cybersecurity," Algerian Journal of Human Security, Issue 04, University of Kasdi Merbah Ouargla, July 2017, page 260.

²⁰- Article 10 of Law 18/04, dated 24 Sha'ban 1439 (corresponding to May 10, 2018), specifying general rules related to postal and electronic communications, Official Gazette of the People's Democratic Republic of Algeria, Issue 27, issued on May 13, 2018, page 07.

²¹- Law No. 20/05, referred to earlier, page 4160.

²²- Muhammad Nour al-Din Sayyid Abdel-Majeed: "Criminal Liability for Altering the Truth in Payment and Credit Cards," First Edition, Dar al-Nahda al-Arabiya, Cairo, page 91, 92.

²³- The same reference, page 99.

The act of use, in the context of credit cards, refers to the legitimate holder of the card presenting it to merchants who accept it as a means of payment for goods and services. This act of use is intended to settle payment for those goods and services. The act of use also occurs when a counterfeit card is inserted into an ATM in order to withdraw cash from the cardholder's account²⁴.

2. Moral element:

The use or attempted use of a counterfeit card is an intentional offence. To establish this element, it is sufficient to prove general criminal intent, which includes both the offender's knowledge (awareness) that the card is a forgery and the deliberate intention to present the card and falsely claim its authenticity²⁵.

3. Damage caused by credit card fraud

In cases of credit card fraud, the damage caused is considered potential. This damage affects both the legitimate cardholder and the issuing authorities of the credit card. Altering the truth in relation to these cards results in potential material, social and moral damage. This damage includes the loss of confidence in economic and banking transactions carried out by means of credit cards²⁶.

Third: Types of credit card fraud

1- Total forgery:

Total forgery is generally defined as the creation of a document that did not previously exist. This means creating a document and falsely attributing its issuance to a person or authority that has no connection with it, or to an authority that did not issue it²⁷.

In the context of credit cards, it can be defined as: the creation of an entire credit card that did not exist before and attributing it to a person who has no connection with it or to an authority that did not issue it.

2-Partial forgery:

Partial forgery refers to forgery that affects one of the components of the credit card. This may include forging the signature strip on the back of the card, altering the name or image of the legitimate cardholder, and other forms of partial forgery that may occur on specific components of the credit card.

Fourth: Penalties for credit card forgery in some laws

1: In UAE law:

Article 13/01 of Federal Decree Law No. (5) of 2012 on Combating Information Technology Crimes states: "Whoever forges, imitates or copies a credit card, debit card or any other electronic means of payment using information technology or software shall be punished by imprisonment and a fine of not less than five hundred thousand dirhams and not more than two million dirhams, or both²⁸."

2: In Saudi Arabian law:

Article 383 of Law No. 11 of 2004 on Computer Crimes of the Penal Code states: "Whoever:

- a) Forges an electronic payment card.
- b) Using a forged or stolen electronic payment card with knowledge of its forgery or theft.
- c) Accepts an invalid, counterfeit or stolen electronic payment card knowing it to be invalid, counterfeit or stolen.

²⁴- Ihab Fawzi al-Saqa: "Criminal Liability for Unauthorized Use of Payment and Credit Cards (A Comparative Study)," First Edition, Dar al-Nahda al-Arabiya, Cairo, 2008, page 353.

²⁵- Jameel Abdul Baqi Al-Saghir: "Criminal and Civil Protection of Magnetic Credit Cards (An Applied Study in French and Egyptian Jurisprudence)," Dar al-Nahda al-Arabiya, Cairo, 2003, page 149.

²⁶- Samah Mohamed Abdul Hakam: "Criminal Protection of Credit Cards (Electronic Payment Crimes)," Dar al-Nahda al-Arabiya, Cairo, 2003, page 55.

²⁷- Fotouh Abdullah Al-Shadhli: "Explanation of the Penal Code (Special Part), Book One: Crimes Harmful to Public Interest," Dar al-Matbou'at al-Jami'a, Alexandria, 1999, page 377.

²⁸- Article 13/01 of Federal Decree-Law No. 5 of 2012, dated 25 Ramadan 1433 (corresponding to August 13, 2012), concerning the prevention of information technology crimes, United Arab Emirates, page 27.

d) Manufactures, without a licence, devices or machines for the production of electronic payment cards²⁹.

3-In Moroccan law:

In accordance with Article 331 of the Commercial Code, the penalties provided for in Article 316 are applicable to the payment instruments in this section. The following acts are punishable:

1. Forgery or alteration of a payment instrument.
2. Knowingly using or attempting to use a forged or falsified payment instrument.
3. Knowingly accepting payment by means of a false or falsified payment instrument.

Therefore, anyone who commits any of these acts - offences - is subject to the provisions of Article 316, which relates to criminal penalties for forgery of cheques. The article states that the offender shall be punished with imprisonment for a term ranging from one to five years and a fine ranging from 2,000 to 10,000 dirhams³⁰.

Section Four: Definition of the Crime of Internet Money Laundering

This is the act of money laundering through the Internet, which is defined as the process of disguising the proceeds of illegal activities, such as drug trafficking, terrorism and others, by removing their illicit nature and using the Internet as a means of concealing their illegal source. These operations are carried out by organised crime syndicates that have significant sums of money derived from prohibited activities such as drug trafficking and corrupt practices. These groups deliberately introduce these illicit funds into the financial system using the Internet³¹.

Based on the provisions of Article 02 of Decree No. 12/02, as amended and supplemented by Law No. 05/01 on the Prevention of Money Laundering and the Financing of Terrorism and their Suppression, the Algerian legislator has defined the cases that constitute the crime of money laundering. The article states that

Money laundering is considered to be the act of transferring or transporting funds, knowing that they are the direct or indirect proceeds of crime, in order to conceal or disguise the illicit origin of these funds or to help a person involved in the commission of the original crime from which these funds were derived to escape the legal consequences of his actions. It also includes concealing or disguising the true nature of the funds, their source, location, disposition, movement or rights associated with them, knowing that they are proceeds of crime. Acquiring, possessing or using the funds knowing that they are criminal proceeds is also considered money laundering³².

Second: Elements of the crime of money laundering via the Internet

1- Material element: The material element of this crime consists of three components: the existence of a previous or original underlying crime that serves as a source of illicit funds, the generation of tainted funds as a result of that crime, and the perpetrator or perpetrators, depending on the circumstances, engaging in criminal activity to launder those illicit funds. This activity takes the form of a series of simple or complex economic and financial transactions designed to purify the illicit funds and integrate them into the financial system so that they appear legitimate³³.

2- Moral element: The moral element of this crime consists of two components: the knowledge element, where the perpetrator is aware of the material elements of the crime, and the intent element, which is the intention to achieve the criminal result of legitimising the illicit funds³⁴.

²⁹ - Maawan Mustafa: "E-commerce and Combating Cybercrime (Civil and Commercial Evidence)," Dar al-Kitab al-Hadith, Algeria, 2010, pages 528-529.

³⁰- Radwan Ghoneim, the same reference, pages 126-127.

³¹- Abdullah Abdul Karim Abdullah: "Money Laundering Crimes on the Internet (A Comparative Study)," Dar al-Jami'a al-Jadida, Alexandria, 2008, page 21.

³²- Article 02 of Decree No. 12/02, dated 20 Rabi' al-Awwal 1433 (corresponding to February 13, 2012), amending and completing Law No. 05/01, dated 27 Dhul-Hijjah 1425 (corresponding to February 6, 2005), related to the prevention of money laundering and terrorism financing, Official Gazette of the People's Democratic Republic of Algeria, dated February 15, 2012, Issue 08, page 08.

³³- Muhammad Abdullah Abu Bakr Salama: "Encyclopedia of Cybercrimes (Computer and Internet Crimes)," Modern Arab Bureau, Alexandria, 2007, pages 208-209.

³⁴- Muhammad Abdullah Abu Bakr Salama, the same reference, page 209.



Third: Characteristics of money laundering via the Internet

This crime is committed using computers as a means of gaining access to the Internet. It is committed via the Internet because it acts as a link between all the potential targets of such crimes, such as banks, financial institutions and stock exchanges. The perpetrator is a highly skilled individual. Money laundering via the Internet has no geographical boundaries as it is an open international network³⁵.

Fifth: Internet money laundering crimes involving credit cards

Attacks on credit cards via the Internet take various forms. One of these forms is the use of a credit card to buy jewellery and later pay the bill with cash derived from drug trafficking. It is worth noting that the link between the Internet and money laundering is characterised by its speed, as it is not constrained by geographical boundaries. The Internet, together with smart cards, is widely accepted by the public. On the other hand, it attracts cybercriminals who seek to exploit the weaknesses to carry out various attacks on these cards, including using them to launder their illicit funds³⁶.

This crime can also be committed using smart cards. This is done by transferring money electronically over the international network. These cards are similar to bank cards but contain a microprocessor. The use of these cards has become widespread in Europe, the United States and Canada. Cardholders can load them with electronic money using devices equipped with this system, such as mobile phones. They can then use these cards to pay for goods and services or to make transfers to bank accounts³⁷. It is well known that technological advances have contributed to the growth of illicit money laundering and its integration into the financial system, particularly with the adoption of cash transactions via the Internet by some institutions and companies worldwide. This has led to the emergence of what is known as digital laundering, in which cash transfers are made via the Internet. One of the features of this method is that it facilitates payment transactions for businesses and e-commerce. On the other hand, it has increased the risk of hacking and made it more difficult to monitor the parties involved to ensure the confidentiality of banking information³⁸.

Conclusion:

Based on the above discussion, we can conclude that cybersecurity is a contemporary issue that has emerged as a result of technological advances. Consequently, this development has been accompanied by an increase in cybercrime, which remains a significant threat to transactions conducted in the virtual world. There is no doubt that the provision of the necessary infrastructure is essential to mitigate the risks associated with these crimes and to minimise their negative impact on various sectors.

Through our research we have come to the following set of findings and recommendations:

- Credit cards are common tools in all forms of electronic payments. We recognise the benefits and advantages that these tools bring to all parties involved. However, the issue of legal protection remains crucial and should be taken into account, especially as the number of users continues to grow. The Algerian legislator should therefore address the existing gaps in the Penal Code and the Code of Criminal Procedure by devoting a section or chapter to electronic payments in general and credit card payments in particular.
- Establish specialised judicial bodies and appoint judges with expertise in cybercrime to deal with such cases.
- Organise study days, national and international conferences and seminars to shed light on the main crimes committed in this area and methods of combating them.

³⁵- Abdullah Abdul Karim Abdullah: "Money Laundering Crimes on the Internet (A Comparative Study)," Dar al-Jami'a al-Jadida, Alexandria, 2008, pages 23-24.

³⁶- Abdelfattah Byoumi Hegazy: "Money Laundering Crime (Between Electronic Media and Legislative Texts)," First Edition, Dar al-Fikr al-Jamei, Alexandria, 2006, pages 22-23.

³⁷- The same reference, page 23.

³⁸- Ahmed Safar: "Combating Money Laundering in Arab Countries," Arab Banks Union, Beirut, 2003, pages 52-53.



List of sources:

- [1] Law 18/04, dated 24 Shaban 1439, corresponding to 10 May 2018, which establishes the general rules relating to postal services and electronic communications. Official Gazette of the People's Democratic Republic of Algeria, issue 27, dated 13 May 2018.
- [2] Decree No. 12/02 of 20 Rabi Al-Awwal 1433 corresponding to 13 February 2012 amending and supplementing Law No. 05/01 of 27 Dhu Al-Hijjah 1425 corresponding to 6 February 2005 on the prevention of money laundering and terrorist financing. Official Journal of the People's Democratic Republic of Algeria of 15 February 2012, issue 08.
- [3] Law No 20/05 of 30 July 2005 on cybersecurity. Official Journal of the Kingdom of Morocco [No information on the number of the issue].
- [4] Federal Decree-Law No. (5) of 2012, dated 25 Ramadan 1433, corresponding to 13 August 2012, on combating crimes related to information technology. United Arab Emirates.
- [5] Ibn Manzur Al-Afriqi, Abu Al-Fadl Jamal Al-Din Muhammad Ibn Mukarram: "Lisan Al-Arab" (Encyclopaedia of the Arabic Language), Volume 1, 4th edition, Dar Sader, Beirut, 2005.
- [6] Fahmi Mahmoud Shakri: "Al-Mu'jam Al-Tijari Wal-Iqtisadi" (Commercial and Economic Dictionary), 1st edition, Dar Osama for Publishing and Distribution, Amman, Jordan, 2009.

Book list:

- [1] Ahmed Saffar: Combating Money Laundering in Arab Countries, Arab Banking Union, Beirut, 2003.
- [2] Ihab Fawzi El-Sakka: Criminal Liability for Unauthorised Use of Debit and Credit Cards (A Comparative Study), 1st edition, Dar Al-Nahda Al-Arabiya, Cairo, 2008.
- [3] Jalal Aayed Al-Shawara: Electronic Payment Methods, 1st edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2008.
- [4] Jamil Abdel Baqi Al-Saghier: Criminal and Civil Protection of Magnetic Credit Cards (An Applied Study in the French and Egyptian Judiciaries), Dar Al-Nahda Al-Arabiya, Cairo, 2003.
- [5] Hussein Mohammed Al-Shibli and Muhanad Fayez Al-Dweikat: Forgery and Fraud with Credit Cards, 1st edition, Dar Majdalawi for Publishing and Distribution, Jordan, 2009.
- [6] Radwan Ghoneimy: Credit Card between Banking Legal Status and Jurisprudential Grounding, 1st edition, Dar Al-Fikr Al-Jamei, Alexandria, 2014.
- [7] Sameh Mohamed Abdel Hakam: Criminal Protection of Credit Cards (Electronic Payment Crimes), Dar Al-Nahda Al-Arabiya, Cairo, 2003.
- [8] Abdullah Abdel Karim Abdullah: Money Laundering Crimes on the Internet (A Comparative Study), Dar Al-Jami'a Al-Jadeeda, Alexandria, 2008.
- [9] Omar Youssef Abdullah Ababneh: Instalment Payment through Credit Cards, 1st edition, Dar Al-Nafa'is for Publishing and Distribution, Amman, Jordan, 2008.
- [10] Fotouh Abdullah Al-Shadhli: Explanation of the Penal Code (Special Section), Volume 1: Crimes Harmful to the Public Interest, Dar Al-Matabi'at Al-Jameia, Alexandria, 1999.
- [11] Mohammed Abdullah Abu Bakr Salama: Encyclopaedia of Cyber Crimes (Computer and Internet Crimes), Al-Maktab Al-Arabi Al-Hadith, Alexandria, 2007.
- [12] Mohammed Nour El-Din Sayed Abdel Majeed: Criminal Liability for Altering the Truth in Debit and Credit Cards, 1st edition, Dar Al-Nahda Al-Arabiya, Cairo.
- [13] Moawen Mustafa: E-commerce and Combating Cybercrime (Civil and Commercial Evidence), Dar Al-Kitab Al-Hadith, Algeria, 2010.
- [14] Nisreen Abdel Hamid Nabih: The Electronic Aspect of Commercial Law, 1st edition, Manshe'at Al-Ma'arif, Alexandria, 2008.
- [15] Nahla Abdul Qader Al-Moumani: Cyber Crimes, 2nd edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2010.

Articles and research papers:

- [1] Bara Samir: Cyber Security, Algerian Journal of Human Security, Issue 04, Kasdi Merbah University (Ouargla), July 2017.

- 
- [2] Saddiq Mohammed Al-Amin Al-Dharyr: Credit Cards, a paper presented at the Banking Conference between Sharia and Law, Volume 2, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, 10-12 May 2003.
- [3] Abdulhamid Al-Ba'ali: Banking Credit Cards: Artistic Imaging and Jurisprudential Graduation (A Comparative Analytical Study), a paper presented at the Banking Conference between Sharia and Law, Volume 2, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, 10-12 May 2003.
- [4] Abdel Fattah Bayoumi Hegazy: Money Laundering Crime (Between Electronic Media and Legislative Texts), 1st edition, Dar Al-Fikr Al-Jamei, Alexandria, 2006.
- [5] Abdullah Abdel Karim Abdullah: Money Laundering Crimes on the Internet (A Comparative Study), Dar Al-Jami'a Al-Jadeeda, Alexandria, 2008.
- [6] Essam Hanafi Mahmoud Musa: Legal Nature of Credit Cards, a paper presented at the Banking Conference between Sharia and Law, Volume 2, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, 10-12 May 2003.
- [7] Mohamed Abdel Halim Omar: Credit Cards and the Emerging Relationships Resulting from Their Use between Sharia and Law, a paper presented at the Banking Conference between Sharia and Law, Volume 2, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, 10-12 May 2003.
- [8] Munathara Ahmad Haji Al-Azhari: Cash Withdrawal Card (ATM Card), a paper presented at the Banking Conference between Sharia and Law, Volume 1, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, 10-12 May 2003.
- [9] Musa Isa Al-Amri: The Smart Check, a paper presented at the Banking Conference between Sharia and Law, Volume 1, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, 10-12 May 2003.
- [10] Nazih Mohammed Al-Sadiq Al-Mahdi: Towards a General Theory of the Credit Card System from a Legal Perspective, a paper presented at the Banking Conference between Sharia and Law, Volume 2, College of Sharia and Law, Dubai Chamber of Commerce and Industry, United Arab Emirates University, 10-12 May 2003.