RESEARCH ARTICLE

Criminal liability of third parties for illegal use of digital banking operations

Salih Bounefla

University of 8May 1945, Guelma

Algeria

Email: bounefla.salih@univ-guelma.dz

Doi Serial https://doi.org/10.56334/sei/8.6.60

Keywords Criminal liability; digital banks; digital currency; electronic banking operations.

Abstract

This study examines the criminal liability of third parties for the illegal use of digital banking and electronic payment methods. The study examines the regulation of digital banks in Algeria under Monetary and Banking Law 23-09. Despite ratifying the Arab Convention on Combating Cybercrime in 2010, Algeria has yet to issue legal texts that criminalise these acts. This has prompted judges to adapt these newly introduced crimes according to the current Penal Code. In contrast, European law has criminalised illegal acts in the digital environment affecting both traditional and digital banks, as well as physical and non-physical payment methods. This has urged EU member states to align their domestic laws with European regulations.

Citation

Bounefla S. (2025). Criminal liability of third parties for illegal use of digital banking operations. *Science, Education and Innovations in the Context of Modern Problems*, 8(6), 560-569; doi:10.56352/sei/8.6.60. https://imcra-az.org/archive/364-science-education-and-innovations-in-the-context-of-modern-problems-issue-6-volviii-2025.html

Received: 18.12.2024	Accepted: 10.04.2025	Published: 11.05.2025 (available online)

Introduction:

The significant and widespread proliferation of digital banking operations and electronic payment methods has led to numerous fraudulent methods being used illegally in the digital business environment. Digital platforms have become targets for criminal groups and hackers seeking financial gain. This has resulted in an increase in financial and banking crimes in the digital space, causing severe damage to individuals, companies, financial institutions and national economies.

In Algeria, digital banks were recently recognised through the issuance of Monetary and Banking Law 23-09[1], which is regulated by the Bank of Algeria under System 24-04[2]. This law concerns the specific conditions for establishing, licensing and operating digital banking activities. Therefore, exploring the rules of criminal liability is essential to provide greater protection for these important financial operations in the virtual business environment, thereby fostering greater public trust and encouraging adherence to state policies aimed at digitising the financial and banking sector.

By 'third parties', we refer to individuals who can unlawfully access a customer's account at a traditional or digital bank without being a party to the contract — i.e. neither the customer nor the bank — and commit crimes such as theft,

embezzlement, or fraud remotely via the internet or any other electronic network.

Third parties are criminally liable for unlawful acts relating to digital banking operations or the unlawful use of electronic payment methods, such as accessing the client's account via the bank's automated data processing system or the unlawful use of electronic payment methods. From this perspective, this study aims to address the following issue:

Can criminal liability be established for third parties due to unlawful acts affecting digital banking operations under the current Penal Code?

To answer this question, we have divided the study into two sections. The first section addresses the liability of third parties for the unlawful use of a digital bank's electronic system. The second section discusses the liability of third parties for the unlawful use of electronic payment methods.

Section One: Liability of Third Parties for the Illegal Use of the Digital Bank's Data Processing System

In the absence of legal texts that explicitly criminalise unauthorised access to the electronic systems of traditional or digital banks under Algerian law, we will examine the liability of third parties for illegally using the bank's data processing system. This includes their responsibility for conducting electronic banking operations unlawfully under Law 04-15, which amended the Penal Code and introduced a new section titled 'Interference with Data Processing Systems', as set out in Articles 394 bis to 394 bis 7.

Subsection One: The Crime of Unauthorised Access to or Presence in the Bank's Data Processing System

This crime is described by various terms, including unauthorised access, hacking, intrusion, or fraudulent entry and retention in information systems. Thus, the crime of unauthorised access to and retention within the bank's data processing system refers to entering or remaining within the information system without permission from the responsible party, thereby harming the confidentiality, integrity or availability of the system and its contents[3].

The 2001 European Convention on Cybercrime, signed in Budapest, addresses the crime of accessing data processing systems in order to ensure the confidentiality and integrity of information and data used in electronic systems, particularly banking systems[4]. Article 2 of the Convention requires member states to enact legislative and regulatory measures that criminalise unauthorised access to data processing systems if the act is committed intentionally and without justification, with the intent to obtain computer data or for any other dishonest purpose[5].

For banks and digital banks, unauthorised access may result in the illegal transfer of funds from customer accounts or from the bank to other accounts. It may also lead to the theft of customers' personal data, such as passwords and card details, or the destruction of the database relating to customers' accounts, should the perpetrator be unable to transfer funds to their own or other accounts.

Firstly: The legal element

The legal element of the crime is set out in Article 394 bis, which states: 'Anyone who fraudulently accesses or remains in all or part of a data processing system shall be punished by imprisonment for a term of three months to one year, and a fine of between 50,000 and 100,000 DZD.' This penalty is doubled if the crime results in the deletion or alteration of data in the system. If the aforementioned acts lead to the disruption of the system's operation, the penalty shall be imprisonment for six months to two years and a fine of 50,000 to 150,000 DZD.'

It is noteworthy that this article corresponds with Article 323-1 of the French Penal Code, which illustrates the influence of French legislation on Algerian law.

Secondly, the material element consists of the criminal act, which can manifest in two forms: a simple form and an aggravated form.

The material element consists of the criminal act, which can manifest in two forms: a simple form and an aggravated form. The simple form is represented by the mere act of unauthorised access to and remaining in the bank's data processing system. The aggravated form occurs when access is accompanied by the deletion or alteration of data, or the disruption of the information system's operation[6].

The simple form involves two acts: access (l'accès) and remaining (le maintien). 'Access' refers to the fraudulent entry into an information system using the necessary technical means. According to the explanatory memorandum of the European Convention on Cybercrime, access is defined as full or partial entry into a computer system and its various components, including hardware, software, stored data, directories, transaction data and content-related data.

'Remaining' refers to an unauthorised presence within the bank's information system, such as connecting to and viewing bank data and customer accounts, or conducting various operations. This presence within the information system occurs without the consent of the bank or the individual authorised to control the system. The act of remaining can extend beyond the designated time for legitimate access. Therefore, remaining is criminalised even if the access was legitimate or occurred accidentally, for example due to an error or oversight. In such cases, the perpetrator must disconnect and withdraw immediately.

The aggravated form of the crime of accessing and remaining within the bank's data processing system is outlined in paragraphs two and three of Article 394 bis.

The aggravated form of the crime of accessing and remaining within a bank's data processing system is outlined in paragraphs two and three of Article 394 bis. This occurs when access or presence results in the deletion or alteration of data within the system, or renders the system incapable of performing its functions. 'Deletion' refers to the removal of data within the bank's system and constitutes the most severe form of harm, warranting a heavier penalty. Alteration involves modifying bank data, for example by transferring funds from a customer's account to another account, or paying for goods or services from the customer's account. Disruption of the system refers to any act that causes it to become incapacitated, preventing various banking operations from being performed.

Hackers typically resort to disrupting the system when they fail to achieve their specific goals, such as stealing money or confidential card information. This allows them to eliminate any traces within the system that could enable law enforcement to identify the perpetrator. Consequently, Article 11 of Law 09-04 on the prevention of crimes related to information and communication technology obliges service providers to retain data enabling the identification of service users, along with data pertaining to devices, connection dates and times, and the addresses of websites accessed.

Third: The Mental Element

The mental element of the crime of accessing or remaining within a bank's data processing system consists of criminal intent, encompassing knowledge and will. Criminal intent is established in the accused whenever fraud is present and they intentionally commit the act without authorisation from the bank that owns the information system. Therefore, the mental element is satisfied if the perpetrator is aware of all the elements that constitute the crime. This means that they are intentionally targeting the data processing system, do not have the right to access or remain in it, and are violating the system's confidentiality and privacy.

As is evident from the text of Article 394 bis, the legislator does not require specific criminal intent for the crime to be established. It is sufficient for the criminal judge to conclude that the perpetrator intentionally committed the crime based on various circumstantial evidence, such as hacking programmes and the offender's possession of data related to the system.

In a ruling dated 1 June 2010, the Batna Court held that 'the court established from the case documents, particularly the technical report analysing the defendant's email, that he was accessing the system through hacking (fraud), using various programmes to collect sensitive information and use it to threaten the American company in exchange for financial compensation...'[7].

If the aforementioned elements of the crime of unauthorised access to and remaining within the bank's data processing system are established, and if the perpetrator had the legal capacity to commit the crime at the time[8], criminal liability arises and the judge must impose the penalties prescribed in Article 394 bis. Finally, it is worth noting that this crime is the first unlawful act that the Arab Convention on Combating Cybercrime requested member states to criminalise, as stated in Article 6.

Subsection Two: Tampering with Data in the Bank's Data Processing System

In addition to the relevant Algerian legal provisions, this crime is addressed in the European Convention on Cybercrime under the heading "Attacks on the Integrity of Information". It is also mentioned in Article 8 of the Arab Convention on Combating Cybercrime.

First: The Legal Element

This crime is defined in Article 394 bis 1 as follows: 'Anyone who fraudulently inputs data into the data processing system, or who fraudulently removes or alters data, shall be punished by imprisonment for a term of six months to three years, and a fine ranging from 500,000 to 2,000,000 DZD.' This corresponds to Article 8 of the Arab Convention on Cybercrime and Article 4 of the European Convention on Cybercrime.

The purpose of this provision is to protect the data processing systems of banks and other public and private entities, ensuring that they are protected from intentional harm in the same way as physical objects.

The purpose of this provision is to protect the data processing systems of banks and other public or private entities, ensuring this protection is comparable to that enjoyed by physical objects against intentional harm. The legal interest protected here is the integrity of stored data and computer programs, and improving their operation and use[9].

Secondly, the material element

The material element of this electronic banking crime consists of the acts of inputting, deleting and modifying data. Inputting refers to adding new data to the designated medium and occurs whenever foreign programs, such as viruses, are introduced or new data is added. Inputting unauthorised data into the information system is one of the most common methods of attacking information systems and represents half of all cases of information fraud[10].

Deletion involves removing part of the data recorded on the system's medium, destroying that medium or transferring or storing part of the data on another memory device. The deletion or erasure of data is akin to the destruction of a physical object, rendering it unrecognisable.

Modification involves changing existing data, such as introducing malicious or virus-laden programs with the intent of

manipulating the software. The aim is to make the data unavailable or inaccessible to the person entitled to access it — typically the account holder — thus preventing them from conducting various banking operations. This crime is considered a crime of harm, focusing on achieving a definite result rather than being a crime of risk. Additionally, this crime only pertains to information within the bank's system, not information external to it.

Third: The Mental Element

The mental element of the crime of tampering with data in the bank's data processing system involves an intentional attack on the system, which requires general criminal intent based on the offender's knowledge. These actions constitute an assault on the integrity of the data within the bank's information system. The will of the offender must be directed towards committing these acts intentionally; the crime can only be established if these acts are committed fraudulently, meaning with intent. Notably, the term "fraud" appears twice in this brief article: once in the context of inputting data and once in the context of removing or modifying data.

The difference between the results in this crime and those in the previous crime is that the result in this case—namely, the crime of data tampering—is intentional, as desired by the perpetrator, whereas in the crime of unauthorized access and remaining, such results are not intended by the offender[11].

Subsection Three: The Crime of Assaulting Data Outside the Bank's Data Processing System

Algerian legislators did not limit protection to data within the information system but extended it to data outside it by criminalizing the handling of data resulting from any of the crimes specified in the section on interference with data processing systems. The goal is to prevent these crimes and mitigate their effects due to the significant danger they pose to legally protected interests.

Firstly: The legal element

This crime is defined in Article 394 bis 2 of the Penal Code, as amended by Law 04-15. 'Anyone who deliberately and fraudulently engages in any of the following shall be punished by imprisonment for a term of two months to three years and a fine of between 1,000,000 and 5,000,000 DZD:

Designing, researching, compiling, providing, publishing or trading in data stored, processed or transmitted by an information system which may be used to commit the crimes specified in this section;

- possessing, disclosing, publishing or using any data obtained from any of the crimes specified in this section for any purpose.'

This article corresponds to Article 9 of the Arab Convention on Cybercrime, Article 6 of the European Convention on Cybercrime and Article L323-3-1 of the French Penal Code.

It criminalises handling proceeds from crime and money laundering with knowledge of their illegality[12]. The aim is to hold accountable those who engage in these actions, thereby mitigating their effects and providing protection for all electronic operators in the banking[13], financial or other sectors. Trading in such data is one of the most serious offences mentioned in this article, as it involves profiting from selling this critical information to other criminals, which can lead to its marketing and subsequent dissemination among interested hackers.

Second: the material element

The material element of this crime manifests in two forms. The first encompasses all actions related to the design, research, compilation, provision, publication or trading of data, regardless of its source or whether it is stored, processed or transmitted by others. These actions must lead to the commission of the crimes specified in this section using the data.

The second form of the material element relates to all actions involving information obtained from any of the crimes specified in Section 7 bis of the Penal Code, which deals with interference with data processing systems. This includes possessing data obtained from the specified crimes and disclosing, publishing or using it for any purpose.

While Article 9 of the Arab Convention provides a simpler and broader definition of various crimes, it criminalises the use of tools and programmes intended for committing different cybercrimes. It also criminalises handling passwords or access codes for information systems, as well as possessing these tools and passwords with intent to commit the previously defined crimes.

Article 394 bis 2 makes it clear that the Algerian legislator has expanded the criminalisation of dealing with data that can be used to commit crimes against data processing systems. This is not limited to data stored within the system, but also includes data transmitted through other information systems. Therefore, any dealings with unlawfully obtained data that could lead to the commission of a crime are considered criminal. This includes possessing bank card numbers, PINs or passwords; accessing customer bank accounts; or using, disclosing or publishing these numbers. All of these actions are deemed criminal.

Third: the mental element

In terms of the mental element of this crime, dealing with unlawful information constitutes an intentional crime, as indicated by the phrase 'Anyone who deliberately and

fraudulently...'. Therefore, this crime requires both general and specific criminal intent.

Despite repeated amendments to the Penal Code by the Algerian legislator, these modifications remain limited. Even though a vast number of cybercrimes are committed daily against banking and other information systems, the Algerian legislator has specified only three types of crime, as noted earlier. These provisions are insufficient to provide adequate legal protection for information within data processing systems[14].

One widely prevalent cybercrime that has been overlooked by the Algerian legislator, but mentioned in some comparative legislation, is the crime of disrupting system operations or unlawful interception. The Arab Convention defines this as 'the intentional unauthorised interception of data flows by any technical means and the disruption or cessation of technical data transmission'[15]. Unlike the previous crimes, the perpetrator does not access the data processing system or alter the data within it; rather, they interfere from outside, hindering the system's operations and leading to a slowdown in data flow.

During this slowdown, the execution of electronic banking operations is delayed or disrupted, causing the system to malfunction. This is precisely when criminals intervene. The French Penal Code addressed this crime in its 2015 amendment.

In a French judicial ruling, it was determined that the crime occurred when the defendants repeatedly sent numerous fraudulent messages through the computer system, causing confusion in the receiving system — for example, subscription requests for contests that could result in prizes[16].

Section Two: Liability of Third Parties for the Illegal Use of Electronic Payment Methods

Both modern and traditional electronic payment methods are considered personal[17], as they are issued in the name of the holder for their personal use, or for the use of a legal entity through its legal representative. Therefore, using these methods for transactions by anyone other than the intended user is deemed unlawful, regardless of how the third party obtained the payment method. In this context, a 'third party' is anyone to whom the electronic payment method was not issued, whether an individual or a legal entity. If a third party uses the payment method without the owner's knowledge, this is unlawful and establishes their criminal liability.

Unlike traditional payment methods such as cheques, which enjoy significant criminal protection under Algerian law[18] — where crimes related to cheques are articulated in the Penal Code[19], the Commercial Code[20], and the law governing general rules for postal and electronic communications — there are currently no legal provisions addressing crimes related to electronic payment methods[21]. Therefore, we will first explore the possibility of establishing criminal liability for third parties based on various property crimes defined in the Algerian Penal Code. Subsequently, we will discuss third-party liability for the unlawful use of electronic payment methods according to European law, which includes specific provisions criminalising such use.

Subsection One: Third-Party Liability for the Illegal Use of Electronic Payment Methods under Algerian Law

In the absence of legal texts that criminalise unlawful acts involving electronic payment methods, some scholars have attempted to apply certain crimes from the Penal Code to these acts, framing them as theft, embezzlement, fraud, forgery or breach of trust. We will also attempt to establish the criminal liability of third parties for the unlawful use of electronic payment methods through property crimes outlined in the Penal Code, as well as forgery.

Firstly: The crime of theft and use of stolen electronic payment methods.

As outlined in Section One of Chapter Three of the Algerian Penal Code, concerning felonies and misdemeanours against property, the crime of theft is one of the most significant and serious crimes against property.

1. The Legal Element

Article 350, paragraph one, serves as the legal basis for stealing electronic payment methods, stating: 'Anyone who embezzles something owned by another is considered a thief and shall be punished by imprisonment for a term of one to five years and a fine of 100,000 to 500,000 DZD.'

2. The material element

Stealing an electronic payment method involves removing the payment method from the possession of its rightful owner. This can be a physical payment method, such as electronic bank cards, or an intangible payment method, such as digital wallets or electronic currency. It must be done against the will of the holder and without their consent. The material element of theft is based on the act of taking, which is a criminal offence involving the thief taking possession of the stolen item without the consent or knowledge of the owner, or with their knowledge but without consent if they have been threatened or coerced by the thief.

The theft of electronic payment tools raises the issue of their physical or non-physical nature. If bank cards are considered physical items, their theft is straightforward, as they can be stolen. Seizing such cards does not raise any issues regarding their classification as property or their suitability for embezzlement, as they are indeed assets, albeit of minor value, and not insignificant.

However, the theft of electronic wallets raises the question: can the theft of electronic money, due to its non-physical nature, be classified as theft in the absence of legal texts?

However, the theft of electronic wallets raises the question of whether the theft of electronic money can be classified as theft in the absence of legal texts, given that electronic wallets are inherently intangible as they represent a data file.

In practice, stealing a bank card alone is not beneficial for the thief as they cannot use it without the PIN[22]. This prevents them from conducting electronic payments with merchants or online. A stolen card can only be used without a PIN if it is forged, for example by transferring one of its components to another card. Nevertheless, stealing a card without its PIN does not exempt this act from being classified as theft. While this theft may not benefit the thief, it certainly harms the cardholder.

If the theft involves the card and its PIN, it is undoubtedly a criminal offence, as the card itself is considered the property of another. Knowing the PIN increases the card's financial value due to its potential use in stealing funds by the thief or others.

3. The Mental Element

The mental element must include criminal intent, encompassing both knowledge and will. This is established when the offender steals an electronic payment method intending to possess, benefit from or use it. It also applies if the intention is to destroy the electronic payment method as long as the result is the owner's permanent loss of it.

The offender cannot claim ignorance of the card's PIN because theft is one thing and benefiting from the stolen item is another. This is similar to stealing unsigned cheques, which, although they may have low value, are not worthless and can be cashed with a forged signature, just like an electronic bank card.

Theft is punishable under Articles 250 and following of the Penal Code, depending on the circumstances.

Additionally, the thief becomes criminally liable when they use the electronic payment method to conduct various banking operations. This constitutes a separate crime from the initial theft, as it involves fraud through the use of a stolen payment method and deceptive tactics to convince the victim — the source of the payment method — of the existence of fictitious credit.

Fraud is defined as any act performed by the offender, whether directly or indirectly, through which they obtain movable property from another person without justification by means of deception specified by law, thereby misleading the victim into delivering the property[23]. However, some argue that this crime is not fraud because the victim is the ATM or internet network, which are not conscious entities.

When purchasing goods or services with the card, the offender may forge a signature on the receipt, which constitutes a separate crime of forgery. However, others suggest that characterising the act as fraud using a false identity is more accurate[24], as the unauthorised cardholder uses deceptive methods by presenting false credentials to others or to the machine, ultimately resulting in the theft of funds from the rightful owner.

Secondly, the crime of forgery and use of forged electronic payment methods.

Forgery and imitation of electronic payment methods, particularly electronic bank cards, are among the most serious crimes affecting payment systems. This is because, aside from losing the payment method itself, the owner does not anticipate any criminal activity until they suffer a loss of funds from their bank account. In the absence of specific provisions in the Algerian Penal Code regarding the forgery and use of electronic payment methods, we will apply the crime of cheque forgery, which is addressed in the Penal Code and concerns a traditional payment method, to electronic payment cards. This application is somewhat contentious as we consider electronic bank cards to be commercial documents, albeit used in various civil and commercial contexts.

1. The legal element

Article 375 of the Penal Code states: 'Anyone who forges or counterfeits a cheque shall be punished by imprisonment for a term of one to ten years and a fine not less than the value of the cheque or the amount of the shortfall in the balance; anyone who accepts a forged or counterfeited cheque knowing it to be forged shall be punished accordingly.' This article falls under Section Two, titled 'Fraud and Issuing Checks Without Funds'.

However, various types of forgery are addressed in Chapter Seven, starting from Article 197. This includes the forgery of ordinary, commercial or banking documents in Articles 219 to 221.

Checks and electronic payment cards are both financial payment methods, and forging either undermines public trust in them as secure payment options. Therefore, it is essential to protect individuals' trust in these tools and documents, which the legislator has accorded special legal and financial significance as they have become indispensable in society.

Forgery is defined as the alteration of a document's truth by one of the legally prescribed methods, resulting in damage if done with fraudulent intent. Thus, it involves making a change to something that is fundamentally correct. Conversely, counterfeiting or imitation involves creating a false item that resembles something genuine; for example, producing a cheque that closely resembles a real cheque[25].

2. The material element

In the crime of forgery, the material element involves altering the truth of one or more statements in a document,

where such an alteration may cause or potentially cause harm. Changing the truth on a cheque constitutes criminal behaviour that forms the material element of the crime. The essence of this alteration is deception or falsification. Therefore, adding or omitting even a minor detail from a cheque constitutes an alteration to the cheque, qualifying it as forgery, even if it is no longer accepted by the bank.

The alteration must occur in a written document, regardless of the writing method or language used. Whether the forgery is executed in the forger's handwriting or someone else's does not affect the nature of the forgery, nor does the type of document influence the process of forgery. The crime is established once the other elements are satisfied, regardless of whether the perpetrator has used the forged item, since using the forged item constitutes a separate crime from the act of forgery itself.

Some argue[26] that card forgery can be compared to money forgery rather than document forgery, given that electronic bank cards can carry significant financial value. Therefore, the provisions for the forgery of money should apply, resulting in harsher penalties than those for the forgery of ordinary documents. However, this comparison is not entirely valid in reality.

Another issue arises when attempting to apply the provisions for cheque forgery to electronic bank cards, particularly if we accept that a cheque is a commercial documen[27]. The question is whether the characteristics of a document apply to electronic payment methods, especially intangible ones like electronic money, which certainly do not have the characteristics of a document. Furthermore, some argue that electronic bank cards do not possess the attributes of documents to which the provisions of cheque forgery apply. This is because a bank card consists of both physical elements, such as its shape and visible components, and intangible elements, such as the data recorded on the magnetic strip or microchip.

3. The Mental Element

As it is classified as an intentional crime, the mental element in the crime of forgery includes both general and specific criminal intent. General criminal intent refers to the offender's awareness that they are committing a crime involving all the elements defined by law. This means they recognise that they are altering the truth of the document in a way that is legally defined as criminal, and that this alteration could cause harm to others.

Specific criminal intent, which the legislator requires for certain crimes such as forgery, involves the offender intending to use the forged card or cheque, either immediately or eventually, whether by themselves or by others. Using this method constitutes another crime if it meets the necessary criteria, akin to the crime of cheque forgery. Therefore, using the forged item is a separate crime from forgery.

This is reflected in the second paragraph of Article 375, which states: 'Anyone who accepts a forged cheque knowing it is forged...' Acceptance of the forged cheque implies acceptance of its use.

The material element of this crime involves the act of receiving and using the forged cheque. There must be a connection between acceptance and use, with use being defined as utilising the cheque for its intended purpose. Mere possession does not constitute use: the forged cheque must be presented and its value asserted as if it were valid. The crime is ongoing, beginning when the document is presented and continuing as long as the presenter maintains it.

As for the mental element, it is sufficient for the recipient of the cheque to be aware that it is forged in order to incur criminal liability for its use, thus subjecting them to the penalties outlined in Article 375.

In terms of criminal liability for the use of the forgery, it is sufficient for the recipient of the cheque to be aware that it is forged. This makes them subject to the penalties outlined in Article 375. This knowledge must precede the use; subsequent awareness has no bearing on the crime. Notably, a forged cheque can usually only be used once, whereas a forged card can be used multiple times. This is another reason why the provisions for cheque forgery should not be applied to electronic bank card forgery.

It is evident from the above that Algerian law has not criminalised harmful acts resulting from electronic payment methods. We have concluded that it is difficult to characterise these harmful acts within the established crimes in the law and that interpretations in the absence of specific provisions have varied significantly. Furthermore, establishing liability without clear criminalisation legislation or determining the crime without explicit legal provisions is not straightforward.

Subsection Two: Third-Party Liability for the Illegal Use of Electronic Payment Methods under European Law

Criminal liability arising from the illegal use of electronic payment methods has evolved alongside changes in the concept of these methods. The definition of electronic payment methods has shifted from physical means to encompass both tangible and intangible forms.

European Directive (EU) 2019/713 of 17 April 2019[28], concerning the fight against fraud and forgery in non-cash payment methods and replacing Framework Decision No. 2001/413/JAI of 28 May 2001, defines non-cash[29] payment methods as follows: 'Any device, tool or protected record, whether intangible or tangible, that enables its holder or user to transfer money or monetary values, including electronic money.[30]'

The same article specifies that a 'protected device, tool or record' is any device or tool that is protected against counterfeiting or unlawful use, for example through its design, or via encryption or electronic signatures[31].

This directive broadens the scope of payment methods to include electronic payment tools such as credit and debit cards, online money transfers, virtual currencies and electronic wallets. Therefore, it encompasses intangible payment tools in the form of data or electronic files, such as virtual money.

The recent European directive calls on member states to criminalise the intentional and unlawful use of stolen, misappropriated or otherwise illicitly obtained electronic payment methods. It also calls for the criminalisation of the unlawful use of all forged and counterfeit electronic payment methods[32].

In order to detail the crimes related to the unlawful use of electronic payment methods as outlined in the latest European Directive (2019/713), we can classify them as either tangible or intangible.

First: Crimes Related to the Illegal Use of Tangible Electronic Payment Methods

Although the unlawful use of tangible payment methods, including electronic ones, is criminalised under the domestic laws of most EU member states, the recent European directive reaffirms this in Article 4. This article urges Member States to criminalise these acts by enacting appropriate criminal penalties.

Article 04 of the recent European directive criminalises all acts of theft and robbery involving tangible payment methods, including electronic ones. It also criminalises the forgery and counterfeiting of these methods through fraudulent means. Additionally, it criminalises the possession of stolen, misappropriated or otherwise illicitly obtained tangible payment methods. The same article prohibits any dealings with stolen or forged payment methods as these involve fraudulent use. Any act related to obtaining, receiving, possessing, purchasing, transferring, importing, exporting or distributing these payment methods is also criminalised.

The directive refers to the definitions of crimes relating to fraud, forgery, theft or unlawful possession concerning tangible payment methods, as specified in the domestic laws of Member States — these concepts existed prior to the digital era[33].

Prior to the issuance of this directive, the French legislator had already criminalised all unlawful acts concerning tangible payment methods, including electronic payment methods, by explicitly outlining related crimes in monetary and financial law and specifying applicable penalties for these offences and crimes related to cheques. This includes the forgery and counterfeiting of electronic payment methods, as well as their use or attempted use when the user is aware that they are forged. It also criminalises accepting or receiving payment through forged means while being aware of this fact[34].

Second: crimes related to the illegal use of intangible electronic payment methods.

The most significant addition brought by European Directive 2019/713 is the expansion of its application to intangible payment methods, thereby criminalising their unlawful use. This directive addresses the fight against fraud and forgery in non-cash payment methods. This directive urges European countries to align their legislation with technological developments in the banking and financial transactions sector, driven by massive changes in communication methods.

While many countries, including Algeria, have yet to regulate standard electronic payment methods such as bank cards, or define crimes associated with their unlawful use, European nations have made significant progress. Not only have they organised tangible electronic payment methods, they have also amended their laws to keep pace with advancements in electronic payment systems, particularly concerning virtual currencies and electronic wallets.

In this context, the European Directive calls on Member States to take the necessary measures to criminalise intentional unlawful acts relating to intangible electronic payment methods and to impose appropriate penalties for these crimes. The directive also mandates the criminalisation of unlawfully acquiring or embezzling any intangible payment method, especially when such acts lead to crimes involving unauthorised access to information systems, harm to the integrity of these systems, damage to data within these systems or the unlawful interception of data flows[35].

For the first time, Article 5 of European Directive 2019/713 criminalises the forgery and counterfeiting of intangible payment methods[36]. The possession of intangible payment methods obtained unlawfully or that are forged or counterfeited is also criminalised, especially if they are used fraudulently and the counterfeit nature was known at the time of possession. The article also prohibits any dealings in stolen or forged intangible payment methods due to their fraudulent use, as well as any acts relating to the acquisition of these methods by the individual or others, or their sale, transfer, distribution or provision to others.

The Directive outlines criminal penalties for offences relating to both tangible and intangible payment methods, distinguishing between penalties imposed on individuals and those imposed on legal entities[37]. Penalties for individuals can range from one to five years' imprisonment, depending on the nature of the crime.

Furthermore, the Directive stipulates the criminal liability of legal entities for offences covered by the Directive that

occur for their benefit, whether by individuals acting independently or as members of the legal entity. This includes decisions made on behalf of the legal entity or oversight of its operations. The directive encourages European countries to impose appropriate[38], deterrent penalties on legal entities found responsible for crimes relating to tangible and intangible electronic payment methods. These penalties may include financial or non-financial fines, along with additional sanctions.

Proposed penalties for offences committed by legal entities include temporary or permanent bans on engaging in commercial activities, judicial supervision, procedures for dissolving the legal entity and the temporary or permanent closure of the establishment involved in the crime.

Among the penalties proposed by Directive 2019/2366 for crimes against legal entities are:[39] temporary or permanent prohibition from engaging in commercial activity, placement under judicial supervision, taking measures pending the dissolution of the legal entity, and temporary or permanent closure of the establishment that committed the crime.

Conclusion:

In conclusion, we can affirm the following:

Algerian legislation does not include specific provisions that explicitly criminalise unlawful acts relating to digital banking operations or electronic payment methods. As there can be no crime without a legal text to define it, the crimes relating to property outlined in the Algerian Penal Code cannot be applied to electronic payment methods. Furthermore, third-party criminal liability cannot be established under these provisions due to the clear differences between the property subject to criminalisation and electronic payment methods.

Despite Algeria's ratification of the Arab Convention on Combating Information Technology Crimes in 2010, it has not issued legal texts to criminalise these acts, whether committed by customers or third parties. This situation means that judges must adapt to these emerging crimes according to current Penal Code provisions.

In the absence of explicit legal provisions, those related to violations of automated data processing systems, as outlined in the 2004 Penal Code amendment, can be applied to crimes affecting electronic banking systems and the various electronic systems through which electronic payment methods operate. This is due to the shared virtual electronic environment in both cases.

European countries have amended their laws to keep pace with developments in electronic payment methods, particularly intangible payment methods relating to digital currencies and electronic wallets. EU legislation has called for the criminalization of the forgery and counterfeiting of both tangible and intangible payment methods, as well as the possession of such methods through unlawful, forged or counterfeit means, or their fraudulent use.

Footnotes and references:

1. Law No. 29-09, dated June 21, 2023, concerning the monetary and banking law, Official Gazette No. 43, dated June 27, 2023.
2. Regulation No. 24-04, dated October 13, 2024, regarding the specific conditions for licensing, authorization, and operation of digital banking activities. Available on the Bank of Algeria website.
3. Yassine Bouhlit, Cyber Crimes and Their Prevention in Algerian Law, Dar Al-Jami'a Al-Jadida, Alexandria, 2019, p. 178.
4. Hossam Abdul Rahman Farag Ahmed Al-Khouli, Previous Reference. p. 101.
5. Article 1 of the Budapest Convention, 2001.
6. Yassine Bouhlit, Previous Reference, p. 180.
7. Judgment No. 05272/10 issued by the Batna Court on 01/06/2010, cited in Yassine Bouhlit, Previous Reference, p. 186.
8. Ahmed Bousqiqia, Previous Reference. p. 163.
9. Interpretative Report on the European Convention on Cybercrime, Previous Reference, para. 60.
10. Yassine Bouhlit, Previous Reference, p. [missing information].
11. Mohammed Khalifa, Criminal Protection of Computer Data in Algerian and Comparative Law, Dar Al-Jami'a Al-Jadida, Alexandria, 2007, p. 161.
12. Article 2, paragraph 3 of Law No. 05-01 concerning the prevention of money laundering and the financing of terrorism. Previous Reference.
13. Sabah Abdul Rahim and Wahiba Abdul Rahim, "Cyber Commerce Crimes,"International Journal of Legal and Political Research, Vol. 1, No. 1, p. 38.
14. Brahim Yamina, "The Applicability of Traditional Penal Code Rules to Computer Crimes (Theft Crime as a Model)," Journal of Law, Vol. 4, No. 5, December 2015, p. 124.
15. Article 07 of the Arab Convention on Combating Information Technology Crimes, Previous Reference.
16. Alaa Al-Tamimi, Previous Reference, p. 574.
17. Article 2-2 of the International Visa Card Contract states: "The card is strictly personal and may only be used by its holder personally, and must be signed upon receipt."
18. Amal Bouhentala, Criminal Protection of Cheques in Algerian Law, PhD Thesis, Batna University, 2015, p. 88.

19. Articles 37 bis 2, 347, 375 of the Criminal Procedure Code, amended by Ordinance No. 15-02, dated July 23, 2015, Official Gazette No. 40, dated July 23, 2015.
20. Articles 526 bis 5, 526 bis 6, 526 bis 13, 537 of the Commercial Code.
21. Article 53 of Law No. 18-04, Previous Reference.
22. Article 03 of the CIB Card Contract, and Article 08 of the Golden Electronic Payment Card Contract.
23. Mansour Rahmani, Criminal Law of Property and Business. Part One, Dar Al-Uloom, Annaba, 2012, p. 9.
24. Noura Ben Bouzid, Previous Reference, p. 132.
25. Amal Bouhentala, Previous Reference, p. 144.
26. Noura Ben Bouzid, Previous Reference, p. 126.
27. Hawaf Abdul Samad, Previous Reference. p. 689.
28. Directive (EU) 2019/713, op. cit.
29. Framework Decision No. 2001/413/JAI of the Council, dated May 28, 2001, concerning the fight against counterfeiting of means of payment other than cash, OJ L149/1, June 2, 2001.
30. Article 2-a: Payment instrument other than cash: a device, object, or protected record, material or immaterial, or a combination of these elements, other than legal tender, which, alone or in conjunction with a procedure or a set of procedures, allows its holder or user to make a transfer of money or monetary value, including through digital exchange means.
31. Device, object, or protected record: a device, object, or record protected against imitation and fraudulent use, for example, in its design or through coding or signatures.
32. Article 3: Fraudulent use of payment instruments other than cash: Member States shall take necessary measures to establish as a criminal offense the following intentional acts: a) fraudulent use of a payment instrument other than cash that is stolen, usurped, or obtained by other illegal means; b) fraudulent use of a payment instrument other than cash that is false or forged.
33. Recital 15 of Directive 2019/713, op. cit.
34. Article L 163- of the Monetary and Financial Code, amended on March 23, 2019.
35. Articles 03 to 06 of Directive 2013/40/EU of the European Parliament and Council, dated August 12, 2013, concerning attacks against information systems and replacing Framework Decision 2005/222/JAI of the Council, OJ No. L218/8, August 14, 2013.
36. Article 5 of Directive 2019/713.
37. Article 9 of Directive (EU) 2019/2366, op. cit.
38. Article 10 of Directive (EU) 2019/2366, op. cit.
39. Ibid, Article 11