SOME COMMENTS ON THE OFFENCE OF CARRYING OUT OF FINANCIAL OPERATIONS FRAUDULENTLY IN ROMANIAN LEGISLATION

Adrian-Cristian MOISE*

Abstract

The study performs an analysis of the offence of carrying out of financial operations fraudulently, provided by the Article 250 of the Romanian Criminal Code. When performing the analysis of the offence of carrying out of financial operations fraudulently, it were taken into account the text in force of the offence of carrying out of financial operations fraudulently, provided by the Article 250 of the Romanian Criminal Code, the provisions of the Article 2 and of the Article 4 from the Council Framework Decision 2001/413/JAI of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment, the provisions of the Article 3 of the the Directive 2014/62/EU of the European Parliament and of the Council of 15 May 2014 on the protection of the euro and other currencies against counterfeiting by criminal law and replacing Council Framework Decision 2000/383/JHA and the provisions from the Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA.

The analysis aims to determine whether the texts of the Council Framework Decision 2001/413/JAI on combating fraud and counterfeiting of non-cash means of payment and of the Directive 2014/62/EU on the protection of the euro and other currencies against counterfeiting by criminal law were transposed in the Article 250 of the Romanian Criminal Code.

Keywords: *offence of carrying out of financial operations fraudulently; electronic payment instrument; instrument of digital currency; identification data; fictional identification data; transfer of funds.*

JEL Classification: [K14]

1. Introduction

The offence of carrying out of financial operations fraudulently is provided by the article 250 from Chapter IV, entitled *Frauds committed*

* Associate Professor, PhD., Spiru Haret University of Bucharest, Faculty of Juridical, Economic and Administrative Sciences, Craiova, Romania; Attorney-at-law, Dolj Bar Association, Romania.

through computer systems and electronic payment means from the Romanian Criminal Code. The legal text states:

"(1) Carrying out of an operation of cash withdrawal, uploading and downloading of an instrument of digital currency or transfer of funds, by use, without the consent of the holder, of an electronic payment instrument or the identification data which allows its use, shall be punishable by imprisonment from 2 to 7 years.

(2) With the same punishment is sanctioned the carrying out of one of the operations stipulated at paragraph (1), by unauthorized use of any of the identification data or by use of fictional identification data.

(3) Unauthorized transmission to other person of any identification data, with a view to carrying out one of the operations stipulated at paragraph (1), shall be punishable by imprisonment from one to 5 years".

The offence of carrying out of financial operations fraudulently is part of the category of offences against patrimony which is based on fraud. This type of offence consists in the use of an electronic payment instrument, including also the identification data which allows its use with a view to carrying out the transfer of funds, other than those ordered and executed by financial institutions, cash withdrawals, as well as uploading and downloading of a digital currency instrument (Sauca, 2005: 48). This act creates a state of danger for the trust which has to be given for the possession and use of electronic payment instruments.

At the European Union level, the legal framework that governs the carrying out of financial operations fraudulently consists of the following legal acts: the Council Framework Decision 2001/413/JAI of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment and the Directive 2014/62/EU of the European Parliament and of the Council of 15 May 2014 on the protection of the euro and other currencies against counterfeiting by criminal law and replacing Council Framework Decision 2000/383/JHA.

The Article 2 of the Council Framework Decision 2001/413/JAI on combating fraud and counterfeiting of non-cash means of payment stipulates the offences related to the following payment instruments: credit cards, eurocheque cards, other cards issued by financial institutions, travellers cheques, eurocheques, other cheques and bills of exchange.

The same Article 2 includes the offence of carrying out of financial operations fraudulently, namely in the Article 2 (b), which refers to counterfeiting or falsification of a payment instrument in order for it to be used fraudulently and in the paragraph (d) of the Article 2, which refers to fraudulent use of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified payment instrument.

The Article 4 of the Council Framework Decision 2001/413/JAI provides the offences related to specifically adapted devices.

The offence of carrying out of financial operations fraudulently also appears in the wording of Article 4, this fact may fall under the following paragraph of the Article 4: "the following conduct is established as a criminal offence when committed intentionally, the fraudulent making, receiving, obtaining, sale or transfer to another person or possession of instruments, articles, computer programmes and any other means peculiarly adapted for the commission of any of the offences described under Article 2(b)".

The Article 3 (1)(d)(i) of the Directive 2014/62/EU on the protection of the euro and other currencies against counterfeiting by criminal law includes provisions that also cover the offence of carrying out of financial operations fraudulently: "the fraudulent making, receiving, obtaining or possession of instruments, articles, computer programs and data, and any other means peculiarly adapted for the counterfeiting or altering of currency is punishable as a criminal offence, when committed intentionally".

We also mention the Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA adopted in Brussels on the 13th of September 2017 is due to come into force in the near future.

This new directive aims to cover not only traditional non-cash means of payment, such as bank cards or checks, but also new payment methods that have emerged in recent years: digital wallets, payments made on mobile phones and virtual coins.

We noticed that, unlike the Council Framework Decision 2001/413/JHA, the new Directive on combating fraud and counterfeiting of non-cash means of payment brings to the forefront the following news (Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, 2017: 18): defines the payment instruments in a more encompassing and robust way which also includes non-corporeal payment instruments, as well as digital mediums of exchange; makes it a self-standing offence, aside from using such instruments, to possess, sell, procure for use, import, distribute or otherwise make available a stolen or otherwise unlawfully appropriated counterfeited or falsified payment instrument; expands the scope of the offences related to information systems to include all payment transactions, including transactions through digital exchange mediums; introduces rules on the level of penalties, in particular setting a minimum level for maximum penalties.

We noticed that the act of carrying out of financial operations fraudulently is covered by the new Directive on combating fraud and counterfeiting of non-cash means of payment in the Articles 3, 4 and 6. Therefore, the Article 3 (b) contains provisions on the fraudulent use of counterfeited or falsified payment instruments.

The Article 4 (b) and (c) refers to the offences preparatory to the fraudulent use of payment instruments, which include the theft or counterfeiting of a payment instrument and various acts involved in trafficking of those stolen or counterfeited instruments. Moreover, these provisions criminalise possession, procurement for use, import, export, sale, transport, distribution or otherwise making available of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified payment instrument in order for it to be used fraudulently.

Like the Article 3, the article 4 covers all offences involving payment instruments and therefore also applies to acts such as the sale of stolen authentication data, such as for exemple, carding and phishing.

The Article 6 form the new Directive refers to tools used for committing offences and sets out offences relating to tools used for committing offences referred to in the Article 4(a) and 4(b) and the Article 5, to be criminalised by the Member States of the European Union.

It aims at criminalising the intentional production, sale, procurement for use, import, export, transport, distribution or otherwise making available of a device or an instrument, computer data or any other means specifically designed or adapted for the purpose of committing any of the offences referred to in the Article 4(a) and (b) or the Article 5, for example, skimming devices used for stealing credentials, as well as malware and forged websites used for phishing.

2. The pre-existing conditions

2.1. *The object of the crime*

The special legal object of the offence is represented by the social relationships relating to public confidence in the safety of the use of electronic payment instruments, to the integrity and authenticity of the computer data contained therein, to public trust in e-commerce and to public trust on the identity of individuals, that is the correspondence between the identity of the person under whom the offence is committed and its real identity (Dobrinoiu, Pascu, Hotca, Chiş, Gorunescu, Neagu, Dobrinoiu, Sinescu, 2014: 319).

The material object of the offence of carrying out of financial operations fraudulently consists of the material supports called electronic payment instruments, such as bank cards, but also in computer data which are targeted by the offender. The electronic payment instrument is at the same time the means of committing the offence.

2.2. *The subjects of the crime*

The active subject of the offence can be any person who fulfils the general conditions provided by the law for criminal liability. The active subject of the offence of carrying out of financial operations fraudulently may also be the

person who has falsified the electronic payment instrument, in which case we will have a criminal contest.

Criminal participation is possible in all its forms: co-author, incitement and complicity.

Passive subject of the offence is the owner of the electronic payment instrument used unlawfully or the person to whom the identification data used belongs. The secondary passive subject is the legal holder of the electronic payment instrument, for example, the issuing financial institution.

3. The constitutive content

3.1. The objective side

The material element of the objective side is made by any of the three alternative actions provided by the Romanian legislator. The material element in the case of the offence of carrying out of financial operations fraudulently is carried out in all three variants by an action to perform a cash withdrawal, uploading or unloading operation of an instrument of digital currency or a transfer of funds.

Regarding the first normative variant, which is the standard version, the material element consists in the use of an electronic payment instrumen[1] and the associated identification data (PIN-Personal Identification Number- code or an identity card) at one of the POS-Point of Sale- terminals provided by Romanian National Bank Regulation no.6 from the 11th of October 2006[2] on the issuance and use of electronic payment instruments and the relations between the participants in transactions with these instruments, without the consent of the right holder. A person's bank account is accessed by the offender by simultaneously using both the electronic payment instrument and its PIN code in the stages of identifying the electronic payment instrument and validating the PIN code.

In the second normative variant, which is an assimilated variant, the material element consists of withdrawing cash, uploading or downloading of an instrument of digital currency or transferring funds by unauthorized use of any of the identification data or by use of fictional identification data.

In the case of this variant, we note that the offender uses both fictitious identification data and actual identification data.

Therefore, in both normative versions, both the identification data and the electronic payment instrument must not belong to the offender. Concerning the fictional identification data, it was considered in the specialty literature that these

[1] According to the provisions of Article 180 of the Romanian Criminal Code, the electronic payment instrument is "an instrument which allows the holder to carry out cash withdrawals, uploading and downloading of a digital currency instrument, as well as transfers of funds, other than those ordered and executed by financial institutions".

[2] Published in the Romanian Official Gazzette, Part I, no. 927 from the 15th of November 2006.

data refer to the identification data of the holder of the electronic payment instrument and not to the data of the electronic payment instrument, because an electronic payment instrument can not operate with a fictional PIN code (Dobrinoiu, Pascu, Hotca, Chiş, Gorunescu, Neagu, Dobrinoiu, Sinescu, 2014: 320).

The third regulatory variant, being a mitigated variant, also sanctions the unauthorized transmission to another person of any identification data for the purpose of performing the following operations: withdrawal of cash, uploading or downloading of an instrument of digital currency or transfer of funds.

We note that the Romanian Criminal Code does not expressly specify by what means unauthorized transmission of identification data to other persons can be made, including any means of transmission, even means of remote transmission (Sauca, Mădălina, 2005: 50).

The offence of carrying out of financial operations fraudulently presents many operating modes frequently used by offenders, especially cybercriminals.

According to the latest statistics, the most fraudulent financial operations are done through the Internet network. An example of a fraudulent operation with electronic payment instruments is phishing. Phishing is the creation of messages sent by electronic mail or web pages which are exact reproductions of some existent sites, in order to mislead the users to disclose personal, financial data or data related to the passwords (Moise, 2011: 292).

E-mails of phishing type appear to be sent from a bank, an insurance company, a trader or an electronic payment instruments processor (Stancu, Dragomir, 2009: 164).

Another example of a fraudulent operation with electronic payment instruments is skimming, which is the activity of copying valid data from the magnetic stripe of an authentic card through a card reading device, without the knowledge of the legitimate holder, with the intention to use it for fraudulent purposes (Stancu, Dragomir, 2009: 183).

In the main, skimming is based on the fact that the data on the magnetic stripe can be registered and then rewritten on a card, which can be a new card or a counterfeited one with the help of an information system and a device for rewriting the magnetic stripes of the cards.

Cards counterfeited through this mode of operation contain valid registrations, not intervening difficulties in the electronic recognition and containing the same electronic features as those of the original card (Moise, 2011: 291). Skimming devices have a slot through which passes the bank card to copy the information contained on the magnetic stripe and can be classified in: hand skimmers and ATM/Automatted Teller Machine/POS skimmers, which are mounted on the ATM and at the points of sale (Blanda, 2007: 41-44).

Another example of a fraudulent operation with electronic payment instruments is carding. Through this method the offenders intend to steal and

use the data of account holders on commercial sites (Moise, 2011: 293). This method is carried out by the change of the source code of the original page, the information entered by the legitimate holder of the account data being directed to an e-mail address indicated by the offenders, without being aware of it (Kövesi, Finta, 2006:191).

Once the data has been obtained, they are used in e-commerce and in the card forgery processes.

With regard to the data being transmitted, they may be identification data associated with the electronic payment instrument or they may be financial-banking data. Some of these data refer to identification elements, being arranged on the front of the electronic payment instrument, in this case the bank card, such as the following (Moise, 2011: 289): the company's logo; the hologram; the latent UV image; the issuer's identification number; the embossed account number; the card's expiration date.

Other data refer to identification items that are placed on the back of the bank card (Moise, 2011: 289-290): the magnetic stripe; the signature panel; the Card Verification Value -CVV- which is a number formed of three digits, established by the issuer, which is encoded on the magnetic stripe of valid cards; the CVV2 Code for Visa Card and the CVC2 Code for MasterCard card is a number formed of three digits imprinted on the signature panel, inversely inclined towards left, without these codes no online transactions can be performed; the duplicate account number is imprinted inversely inclined, towards left, on the signature panel, ensuring that it corresponds to the number on the front of the card; permanent impression**,** the bank cards are printed with permanent ink.

Immediate consequence

The immediate consequence consists of a state of danger for the legally deployment of the e-commerce activity, confidence in the financial-banking circuit, the security of the financial and banking system, and the confidence of the public in the security of transactions through electronic payment instruments.

The offence of carrying out of financial operations fraudulently affects the interests of the holder of the electronic payment instrument or of another person whose identification data are used without right, and that person may even be a commercial company having commercial relations with the holder of the electronic payment instrument (Dobrinoiu, Pascu, Hotca, Chiş, Gorunescu, Neagu, Dobrinoiu, Sinescu, 2014: 323).

Causality link

There must be a *causality link* between the activity of the offender and the consequence that results from the materiality of the crime.

3.2. The subjective side

The offence of carrying out of financial operations fraudulently is committed only with direct intention. We believe that direct intention is obviously in the Article 250 of the Romanian Criminal Code, in the sense that the offender uses the electronic payment instrument or the identification data that allow it to be used without the consent of the holder of the respective instrument, or uses fictional identification data, or disperses any unauthorized identification data to others.

Considering the aspects presented, we believe that the offender acted premeditated, committing the offence with the form of guilt of direct intention.

Regarding the third normative version, we emphasize that the form of guilt required by the rule of criminalisation is the direct intention qualified by purpose.

4. The forms of the offence

The preparatory acts are possible, but they are not criminalised and thus they are not punishable.

The attempt is possible and is punished according to the article 252 of the Romanian Criminal Code.

The consumption of the offence of carrying out of financial operations fraudulently takes place when any of the fraudulent financial operations (cash withdrawals, uploading or downloading of an instrument of digital currency or transfer of funds other than those ordered and executed by financial institutions) referred to in Article 250 of the Romanian Criminal Code was committed. Therefore, the offence is consumed when the material element is carried out and the socially dangerous result is produced.

The exhaustion of the offence occurs at the time of committing the last act criminalised by law. The offence can be committed in continuous or continued form.

5. Modalities

The offence of carrying out of financial operations fraudulently presents the following normative modalities, according to the provisions of the article 250 of the Romanian Criminal Code: the use of an electronic payment instrument or identification data allowing its use, without the consent of the holder of that instrument, the unauthorized use of any identification data or the use of fictional identification data, the unauthorized transmission to any other person of any identification data.

To these normative modalities may correspond various fact modalities.

6. Sanctions

The punishment provided for the offence of carrying out of financial operations fraudulently in the case of paragraph 1 and paragraph 2 of the Article 250 is imprisonment from 2 to 7 years. For the paragraph 3 of the article 250, the prescribed penalty is imprisonment from one to 5 years.

7. Procedural Aspects

The criminal prosecution initiates *ex officio*.

Conclusions

Taking into consideration the definition of the electronic payment instrument, stipulated in the Article 180 of the Romanian Criminal Code, we noticed that the notion of *digital currency instrument* is not defined anymore in the current criminal legislation, and the new definition of the *electronic payment instrument* is more comprehensive, covering also the notions of *payment instrument with access at distance,* as well as *instrument of digital currency* which were comprised in the old criminal legislation, specifically in the old Law no. 365/2002 on electronic commerce.

We emphasize that the offence of carrying out of financial operations fraudulently, referred to in the Article 250 of the Romanian Criminal Code transposed the provisions of the Article 2 (b) and (d) (offences related to payment instruments) of the Council Framework Decision 2001/413/JAI on combating fraud and counterfeiting of non-cash means of payment. Moreover, we noticed that the text of the Article 4 (offences related to specifically adapted devices) of the Council Framework Decision 2001/413/JAI of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment was transposed too into the text of the Article 250 of the Romanian Criminal Code.

We remark that the provisions of the Article 3 (1)(d)(i) of the Directive 2014/62/EU on the protection of the euro and other currencies against counterfeiting were transposed into the Article 250 of the Romanian Criminal Code, which refers to the offence of carrying out of financial operations fraudulently.

We express our wish that in the near future Romanian legislators should start adapting the Romanian Criminal Code to the provisions of the new Directive on combating fraud and counterfeiting of non-cash means of payment, which it will come into force soon.

Bibliography

1. Blanda, Petru, (2007), *Preventing and combating credit card frauds*, Târgovişte: Pildner&Pildner.
2. Dobrinoiu, Vasile; Pascu, Ilie; Hotca, Mihai Adrian; Chiş, Ioan; Gorunescu, Mirela; Neagu, Norel; Dobrinoiu, Maxim; Sinescu, Mircea Constantin, (2014), *The new Criminal Code commented. The special part*, Second Edition, Bucharest: Universul Juridic Publishing House.
3. Kövesi, Laura Codruţa; Finta, Sorin, (2006), *Legal framing of computer fraud*, Law Review, no.12.
4. Moise, Adrian Cristian, (2011), *The forensic investigation methodology of cybercrimes*, Bucharest: Universul Juridic Publishing House.
5. Sauca, Mădălina, (2005), *E-commerce offences*. Timişoara: Mirton Publishing House.
6. Stancu, Emilian; Dragomir, Corina, (2009), *Aspects related to computer attacks directed against credit institutions*, Law Review, no.10.
7. Stancu, Emilian; Dragomir, Corina, (2009), *Technical and Legislative Aspects of Cards Related Frauds*, Law Review, no.7.
8. Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA adopted in Brussels on the 13th of September 2017, the European Commission.
9. The Directive 2014/62/EU of the European Parliament and of the Council of 15 May 2014 on the protection of the euro and other currencies against counterfeiting by criminal law and replacing Council Framework Decision 2000/383/JHA, Official Journal of the European Union, 21.05.2014, L151/1.
10. The Council Framework Decision 2001/413/JAI of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment, Official Journal of the European Union, 02.06.2001, L149/1.
11. The Romanian Criminal Code.
12. The Romanian National Bank Regulation no. 6 from the 11th of October 2006 on the issuance and use of electronic payment instruments and the relations between the participants in transactions with these instruments.