THE 16TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

The Youth of Today - The
Generation of the Global Development

Counterfeiting and Fraud of Credit and Debit Cards. National and European Legislative Affairs

Alexandru-Adrian Eni[1]

Abstract: As the world becomes more and more interconnected, technology has begun to be seen as a convenient and useful tool for communication between individuals, a situation that has facilitated participation in some of the commitments that were considered challenges in the past. In fact, technology has provided, among other issues, the kind of social interaction that has indeed bridged the gap between different cultures and ideologies. Today's world is an age of technology, and that technology is constantly changing. More than one hundred and fifty years ago, the conduct of commercial operations was quite different from today. Currently, much less time is spent on data processing, information retrieval, cataloging and evaluation of business statistics. In addition, surveys of catalog items and the processing of purchasing transactions have been automated, reducing or eliminating human intervention. This has contributed to saving resources for strategic use. Technology is, in fact, transforming every aspect of our lives, including medicine, art and education, but also organized crime.

1. Introduction

We live in a time when technology is evolving from day to day and the way we understand it is becoming more important. At the same time, with the development of technology, cybercrime is a new challenge for criminal law systems around the world.

The improvement of technology led in the first phase to the increase of the simplification of life and related financial operations, but also represented a niche supported by weak legislation that led to the creation of a vacuum of organized crime that grew in the early 2000s.

Cybercrime is the social phenomenon characterized by committing crimes in the field of information technology (Gheorghe & Barbăneagră, 2006, p. 12).

The progress of techniques and technology has materialized, among other items, in the emergence of high-performance computers and programs that, mainly, have been a huge leap for humanity (Gheorghe & Barbăneagră, 2006, p. 12).

In addition to the widespread concern to use the computer in the interest of society and in compliance with the law, this technology has offered the opportunity to individuals eager for the benefits of new

[1] Danubius University of Galati, Romania, Address: 3 Galati Blvd., 800654 Galati, Romania, Corresponding author: alexandru_eni@yahoo.com.

inventions to take advantage of new technologies, bypassing the law, giving rise to cybercrime (Gheorghe & Barbăneagră, 2006).

Cybercrime is the totality of acts committed in the area of new technologies, in a certain period of time and on a certain well-defined territory (Amza, 2008, p. 32).

The generalization of credit and debit card payment transactions has led to a significant increase in fraud in their use. These frauds can be committed: in stores (by presenting a foreign card obtained illegally for the payment of a good or service), through telematic networks (by performing payment transactions on the Internet by someone who is not the owner of the card using data about it) or at ATMs (using a foreign card to withdraw money from ATMs in a non-consensual way).

Chapter 1

The legal regulation conferred by the Romanian legislation was and is given by the Framework Law no.161 / 2003 art.42, repealed by art.130 point 1 of Law no.187 / 2012, Law no.365 / 2002 as well as articles 364 and 365 Penal Code.Art.364

The structure of incrimination

The infraction of unauthorized transfer of computer data is regulated in the Criminal Code in a standard version with two hypotheses. Thus, it constitutes a crime by art.364 the act of unauthorized transfer of data from a computer system or from a means of storing computer data.

A. The object of the crime

a) The special juridical object. It represents the core of social relationships that are born around the concepts of confidentiality and availability associated with data and information stored in digital format. The individualism of the defended legal interest is that of the owner or right holder of the digital data so that he has the respective information, in the sense desired by him or according to the legal regulations.

b) Material object is conferred by the physical elements which are called computer data, defined as any device or set of devices interconnected or in a functional relationship, one or more of which ensures the automatic processing of data, by means of a computer program[1].

B. Subjects of the infraction

a) Active subject. It is defined by any natural or legal person being criminally responsible.

Participation can be achieved in all its forms: complicity, co-authorship or instigation.

b) The passive subject is established by the natural or legal person holding or rightfully owning the data that represents the material object of the criminal act. Through the analysis of European and national jurisprudence we can also notice the existence of the secondary passive subject, in the situation when the crime causes an injury against the interests of the entities that manage the computer data.

The material element is represented by the transfer that translates into the extraction and processing of a quantity of computer data from the initial storage medium (electromagnetic card / data stored on the server in mobile banking applications) in another storage medium.[2]

[1] Art.181 paragraph (1), the Criminal Code of 2009, published in the Official Gazette, Part I no. 510 of July 24, 2009, entered into force on February 1, 2014.
[2] Noul Cod Penal Comentat, Partea Specială, Ediția a-III-a/ The New Commented Criminal Code, Special Part, 3rd Edition, p. 900.

Referring technically to this procedure, regarding the cloning of computer data on a bank card, we define it as follows:

1. Copy - is given by the moment when the amount of stored information is cloned from the media on which it is found (electromagnetic tape) on a compatible blank media. The transfer of computer data arouses a special interest both in doctrine and in judicial practice, as its manifestation is a special one. On the first hand, we consider that the legality or illegality of the transfer does not reside only in the nature of the data that is the object of the transfer, but especially in the right of the perpetrator to dispose of them, duplicating them or change their storage place.

Unauthorized transfer of computer data from a computer data storage device in the case of Skimming to an ATM is done by "reading" the magnetic tape of the cards using handmade electronic devices type "kitten" camouflaged in plastic interfaces that mislead legal users (before the respective cards enter the ATM acceptance slot), the perpetrators actually make an unauthorized transfer of computer data stored on track no. 2 of the magnetized surface in the internal memory of the micro-controllers (skimmers)[1].

Due to its functionality and mode of operation, the bank card is considered to be a medium for storing digital information.

By decision no. 15/2013[2], The High Court of Cassation and Justice defined Skimming as representing "illegal operations with devices or computer programs", in the form legislated in art.365 par (2) Penal Code., Namely the illegal possession of a device, of a computer program, a password, an access code or other computer data from those provided in par. (1), for the purpose of committing one of the offenses provided in art. 360-364[3].

The immediate consequence is the existence of a copy of the targeted digital data on a storage medium other than the original one and the damage caused to the holder by taking over that data.

Causal relationship. Between the action of the offender and the consequence produced on the new location of the digital data concerned, it is necessary to have a causal link, but which must be proven by technical expertise.

Forms. Sanction

Preparatory acts, although possible, are not criminalized, so they are not punishable.

Sanction

The punishment for unauthorized transfer of computer data is imprisonment from 1 to 5 years.

Article 365 of the Criminal Code

First of all, it should be noted that, in relation to law no. 161/2003, the current criminal law does not bring changes regarding the facts described and incriminated, but only provides a sanctioning regime proportional to the degree of social danger of criminal activity with devices or computer programs, reducing the amount of imprisonment. Thus, the sanction provided in the previous criminal law, namely the phrase from 3 to 12 years is changed from 6 months to 3 years or a fine for the person who, without right, produces, imports, distributes or makes available in any form, passwords codes access or other such computer data that allows full or partial access to a computer system, for the purpose of committing one of the offenses provided in art.360-364; while for the possession, without right, of a device, a

[1] The New Commented Criminal Code, Special Part, 3rd Edition, p. 900.

[2] Decision no. 15/2013 of the HCCJ, published in the Official Gazette no. 760 of December 6, 2013.

[3] The Criminal Code of 2009, published in the Official Gazette, Part I no. 510 of July 24, 2009, entered into force on February 1, 2014

computer program, a password, an access code or other computer data from those provided in par. (1), for the purpose of committing one of the offenses provided in art. 360-364, shall be punished by imprisonment from 3 months to 2 years or by a fine. It should be noted that, except for the decrease of the amount of the punishment, the introduction of the fine for the listed deeds is observed.

The object of the infraction

The special juridical object is represented by the social relations regarding the trust in the data, devices and computer programs, in the sense of their correct and legal use, as well as in the correct and legal development of the commercial operations in connection with them.

Material object of the crime is the electronic devices or programs specially created or adapted to be used as means for committing other computer crimes, as well as computer data related to the protection of the system (passwords, access codes, etc.).

B. Subjects of the infraction

The active subject (author) can be any natural person criminally responsible.

Participation is possible in all its forms: co-authorship, instigation or complicity.

The passive subject of the crime is the natural or legal person legally entitled to the computer system, likely to be harmed by committing the incriminated acts, but also the owner or holder of copyright for hardware or software products modified or adapted for criminal purposes.

The natural or legal person holding or owning (not necessarily using) passwords, access codes or other such computer data that has been fraudulently used to allow access to a computer system will also be liable.

3. Constitutive Content

3.1. The Objective Side

Material element

The material element consists of the action of producing, selling, importing, distributing or making available one or more computer devices or programs, specially designed or adapted for the purpose of committing one of the aforementioned computer crimes.

“Manufacturing of a computer device” means the performance of technical activities by which certain electronic components are joined and interconnected in such a way that the product obtained can interact (directly or remotely) with a computer system or become an integral part of it. . The legislator also wants to incriminate the deed of the person who, although he has no contribution to the creation of the computer device or program, “imports”, “distributes” or “makes available” to the person who acts directly on the computer system.

At the same time, the production, sale, import, distribution or making available to unauthorized persons of passwords, access codes or any other computer data that allow access, in whole or in part, to a computer system will be sanctioned.

The password, like the access code, is a variable-length string of numbers, letters, and special signs that result from touching certain keyboard buttons or randomly generated, by applying a mathematical algorithm to certain electrical (or other) signals within a special device manufactured for this purpose. Figuratively, the password and access code can be compared to the “teeth” of a key. With their help, for security reasons, authorized holders or users restrict the access of aliens to the systems, devices or computer programs they run or manage.

Immediate effect and causation.

The immediate consequence is the creation of a state of danger, threat, to data, devices or software. A person who has experienced such an event will get a certain fear or reluctance to use the credit or credit card when making purchases or withdrawing money from ATMs. There must be a causal link between the perpetrator's activity and the consequence produced. This connection results ex re, in from the materiality of the deed.

By the address no. 1776 / II.6 / 2015 of July 6, 2015[1], The Prosecutor's Office attached to the Oradea Court of Appeal, based on art. 131 para. 4, art. 131 para. 1 and the following from Law no. 302/2004 sent to this court of appeal the request having as object the request of the judicial authorities of the United States of America regarding the transfer of the convicted person P_______ S _____- T____, in order to continue the execution in a Romanian penitentiary of the sentence of 87 months imprisonment applied by the judgment of the Southern District Court of New York, which became final on February 27, 2014.

It was noted in law that the convicted person P_______ S_____ T____ was convicted by the criminal judgment handed down by the Upper District Court of New York in case no. S1: 13-CR-xxxxx-02 (AJN) to a sentence of 87 months in detention for committing the offenses of bank fraud, prev. and ped. of art. 1344[2].

Thus, convicted P_______ S_____ T____ together with the named Olsen Steffen set up electronic devices at ATMs to steal ATM customers' debit account numbers, as well as PIN codes, which they use as secure access codes. Their funds. Specifically, members of the group, including convict P_______ S_____ T____, installed the cloning devices either on the ATM door or on the ATM card reader, which looks exactly like the genuine card reader. Thus, when a customer inserted the card into an ATM that has a cloning device attached, it was read twice, once by the real reader, which allows the customer to access his account a second time by the cloning device. , which gathers the information on the debit cards. In addition to the cloning devices, the members of the group also installed cameras around the ATMs, which recorded the PIN code typed by customers.

With regard to the double criminality, the court will note that, as indicated above, in fact, the convicted person was found to have formed an organized criminal group and that, together with the other members of the group, they installed electronic devices at ATMs of several banks in the United States, as well as cameras, thus gathering information from the debit cards of customers of these banks, data which with the help of a computer and a device called magnetic stripe reader (MSR) encoded blank cards (often blank magnetic stripe gift cards) with account numbers withdrawn from cloning devices. Subsequently, the convicted person and other members of the group affixed white stickers to the face of the gift cards with the PIN codes corresponding to the compromised accounts, which could thus function as forged, cloned cards. The convicted person used some of these cards to make unauthorized withdrawals from customers 'accounts or gave them to other members of the organized criminal group who also made unauthorized withdrawals from customers' accounts.

[1] Address no. 1776 / II.6 / 2015 of July 6, 2015.

[2] 18 U.S. Code § 1344 - Bank fraud, Chapter 63. Mail Fraud and other Fraud Offenses, Part I. CRIMES, 18 U.S. Code Title 18 — Crimes and Criminal Procedure.

Thus, it will be noted that, according to the Romanian legislation, the deeds of the convicted person would have constituted, prior to the entry into force of the current Criminal Code, the offenses of establishing an organized criminal group, prev. and ped. of art. 3 of Law no. 39/2003, possession of equipment in order to falsify electronic payment instruments, prev. and ped. of art. 25 of Law no. 365/2002 and the falsification of electronic payment instruments, prev. and ped. of art. 24 para. 1 of Law no. 365/2002.

According to the current Penal Code, the deeds committed by the convicted person would constitute the offenses of forming an organized criminal group, prev. of art. 367 para. 1 of the Criminal Code, possession of instruments for counterfeiting securities, fraudulent financial transactions, prev. and ped. of art. 314 para. 2 Criminal Code and prev. and ped. of art. 250 Penal Code.

For the above considerations, based on art. 135 para. 6 of Law no. 302/3004, with reference to the European Convention on the Transfer of Sentenced Persons, adopted in Strasbourg on March 21, 1983[1], to which the United States is a party, will accept the application and recognize the criminal sentence handed down by the New York South District Court in case no. S1: 13 CR-xxxxx-02 (AJN), by which the convicted person P_______ S _____- T____ was sentenced to 7 years and 3 months imprisonment (87 months imprisonment), in order to execute this punishment in Romania[2].

3.2. The subjective side

Direct intention. Illegal operations with computer devices or programs are committed with qualified direct intent for the purpose. Thus, the actions described in par. (1) and (2) shall be committed for the purpose of committing the offenses provided by art. 42-45 (illegal access to a computer system, illegal interception of a computer data transmission, alteration of computer data integrity, disruption of computer systems operation).

4. Forms. Procedure. Sanctions and procedural issues

Forms.

Preparatory acts, although possible, are not criminalized and as such are not punished.

It is noted that the facts incriminated in art. 365 lit. a) -c) of the Penal Code constitute preparatory acts of the offenses provided in art. 360-364 Penal Code, but the Romanian legislator preferred to incriminate them separately. The attempt is punishable, in accordance with the provisions of art.366. At the same time, we can consider the change of legal classification of the facts by fully recognizing by the defendants the acts committed, the guilt of the defendants in the form of direct intention.

The Constanţa Court of Appeal showed that, by decision no. 15 / 14.10.2013 of the High Court of Cassation and Justice, the appeal was admitted in the interest of the law and it was established that the installation at the ATM of the autonomous devices for reading the magnetic stripe of the authentic card and its corresponding PIN code false) constitutes the offense provided by art. 46 para. (2) of Law no. 161/2003, the current art. 365 para. (2) Criminal Code that criminalizes illegal operations with computer devices or programs.

According to the judges of the Constanţa Court of Appeal, since the passive subject of the crime is provided by art. 46 para. (2) of Law no. 161/2003, the current art. 365 para. (2) The criminal code that criminalizes illegal operations with computer devices or programs is the holder of the computer system

[1] European Convention on the Transfer of Sentenced Persons, adopted in Strasbourg on 21 March 1983, Published in the Official Gazette no. 154 of July 19, 1996

[2] www.rolii.ro, accessed on 06.04.2021

and not the natural person holding the bank card, and the two defendants in this case acted on a single criminal resolution (taking into account the time and manner in which they acted), committing several material acts against the same passive subject, in this case it is necessary to retain the provisions of art. 35 para. (1) Criminal Code: "the crime is continued when a person commits at different time intervals, but in the realization of the same resolution and against the same passive subject, actions or inactions that each present the content of the same crime".[1]

In recent years, our country has been an important provider of cybercrime, as evidenced by the police operations that took place in collaboration with European states, in order to dismantle certain criminal groups. A first example of such an action is the operation "Armageddon", so in 2006, the Romanian, Italian and Spanish police destroyed a gang of over 80 criminals, mostly Romanians, who dealt with the forgery of bank cards in Romania and other European countries. Criminals: installed fake card readers at ATMs in Romania, Italy, Germany, France, Canada or Turkey, then copied the information from the cards and access codes that they transferred (cloned) to other fake cards, with which they withdrew the amounts of money from the accounts held by bank customers. The Romanian police arrested 12 card forgers in Bucharest and Constanța, and another eight members of the network operating abroad were put under general investigation. In the same operation, code-named Armageddon, Spanish police arrested 66 people, mostly Romanians.[2]

It should be noted that this criminal development involves rapid and effective cooperation between the states involved, this being possible only through an appropriate domestic and international legislative framework that allows for a rapid response to this type of cooperation.

Most of the provisions of domestic law are found in the Framework Law no. 161/2003[3], Title III, called Prevention and fight against cybercrime, art. Art. 42, Law no. 365/2002[4], but also articles 364 and 365 of the Penal Code. These laws are harmonized with European law, namely the Council of Europe Convention of 23 November 2001 on cybercrime[5].

The Convention establishes the obligation for States Parties to cooperate to the fullest extent possible in order to investigate cybercrime and to obtain electronic evidence. Also, Article 23 stipulates that the provisions of the 2001 Convention will not apply to other provisions of an international, regional or bilateral nature or even domestic provisions relating to mutual assistance in the field.[6]

Technical procedure for cloning cards

As we presented in the previous chapter about chips or so-called "skimmers", in this chapter we will present how they work.

To commit these frauds, a common practice among criminals is "card cloning", which consists of making a copy or storing data on our card. To perform card cloning, a small device called a pocket skimmer is used, a device measuring almost 2 cm long and 0.5 mm thick, difficult to detect whose operation is very simple. It is a device that uses the technology used by ATMs to read the magnetic

[1] Constanța Court of Appeal, criminal conclusion no. 874 / P of October 7, 2015.
[2] https://business24.ro/carduri/carduri-bancare/operatiunea-armaghedon-politia-a-anihilat-o-banda-de-80-de-hoti-de-carduri-80795, accessed on 22.03.2021.
[3] LAW no. 161 of April 19, 2003 on some measures to ensure transparency in the exercise of public dignity, public office and in the business environment, prevention and sanctioning of corruption, published by the Official Gazette. no. 279/21 apr. 2003.
[4] Law no. 365/2002 on electronic commerce, published in the Official Gazette no. 959 of November 29, 2006.
[5] Ratified by Law no. 64/200. Published in the Official Gazette no. 343 of April 20, 2004
[6] Mariana Zainea, Raluca Simion- Infracțiuni în domeniul informatic, Culegere de practică judiciară, C.H.Beck Publishing House, Bucharest 2009, p.9

stripe of the cards. In this case, the reading is performed by passing it through a small slot the data being stored for later transfer to a computer.

This can happen in any business through clever hand movements and distraction games if, for example, the cashier finds that the reader is not working, so he passes it through to another who, at that moment, accepts the fee. The person in charge of the trade could hide a skimmer[1] in the first terminal and he would have made the copy in front of our eyes. You can also copy the data when passing the card through an ATM that has been tampered with to hide the Skimmer. The process[2] will be as follows: simply pass our card through the reader that collects the data and then connects to a computer. Within it, through specialized software, it will be possible to access the following data: name and surname of the cardholder, card number, expiration date and security number (CVV). Thus, this data could be used to make online purchases or to complete cloning. For this last step, it would have a card encoder that rewrites the computer information on blank cards.

Conclusion

When we refer to the word crime, we have the classic image of a criminal act physically directed against a person. The notion of cybercrime is a relatively new phrase in the legal vocabulary, cybercrime is a cross-border criminal act adapted to newer cyber trends.

Regarding the cloning of cards, this crime can be considered the easiest cybercrime, which does not require in-depth knowledge of computer science, but only an adequate infrastructure for committing the criminal act.

We use our cards to pay for dinner at a restaurant, to pay for home delivery, for online shopping or for ride-sharing services. Millions of transactions take place every day, so criminals can easily steal cards information due to vulnerability as well as victims.

Criminals can purchase the so-called “skimmers” chips from the online environment, for small sums, as well as card readers and the necessary software. Thus, the infrastructure required for card cloning is rudimentary, compared to the scale of the criminal act.

In terms of how to operate, there are many options, from installing “skimmers” on the counter to using them in a restaurant with the help of waiters, at the supermarket or even at companies that provide food delivery services.

When a note is paid through the POS terminal, it takes only a few seconds until the card is read and the copied data, and after being returned the victim has no indication that he has been robbed.

However, I consider that this crime does not constitute a criminal act of high gravity, this statement being supported by the amount of the penalty established by the Penal Code, by Article 365 on the facts provided in Articles 360-364. At the same time, that the current criminal law proposes a sanctioning regime directly proportional to the degree of social danger of the cybercrimes committed as well as by introducing the criminal fine.

Simultaneously, according to Regulation no. 6 of October 11, 2006, of the NBR, by art. 23 paragraphs (1) stipulates that *the issuer is obliged to credit the holder's account with the value of the compensations, within one banking day from the moment of recognizing the holder's right to them or from the*

[1] David A. Montague- Fraud Prevention Techniques for Credit Card Fraud, p.42

[2] National Institute of justice, Investigative Uses of Technology: Devices, Tools, and Techniques, p.37, https://www.ojp.gov/pdffiles1/nij/213030.pdf, accesat pe data de 27.03.2021

establishment of this right by a court or arbitration, while paragraph (2) of the same article mentions that *the issuer is liable to the holder of an electronic payment instrument for the lost value and improper execution of the user's transactions, if the loss or improper execution is attributed to a malfunction of the instrument, device, terminal or any other equipment authorized to be used by the holder, provided that it is proved that the malfunction was not knowingly caused by the user.*[1]

In this regard, corroborating the statements, we conclude this paper considering that cybercrime, especially card cloning, will be present in everyday life, and over time, due to the current global economic situation due to the current pandemic, will gain considerable momentum, primarily due to WHO rules recommending the use of cryptocurrencies to the detriment of Fiat currencies.

References

National and international normative acts:

*** (2014). The Penal Code of 2009, published in the *Official Gazette,* Part I no. 510 of July 24, 2009, entered into force on February 1.

*** (2006). Law no. 365/2002 on electronic commerce, published in the *Official Gazette,* no. 959 of November 29.

*** (2013). Decision no. 15/2013 of the HCCJ, published in the *Official Gazette* no. 760 of December 6.

*** (2004). Law no. 64/2004 for the ratification of the Council of Europe Convention on Cybercrime, adopted in Budapest on November 23, 2001, Published in the *Official Gazette* no. 343 of April 20.

18 U.S. Code § 1344 - Bank fraud, Chapter 63. Mail Fraud and other Fraud Offenses, Part I. CRIMES, 18 U.S. Code Title 18—*Crimes and Criminal Procedure.*

18 U.S. Code § 1349.Attempt and conspiracy, Chapter 63. Mail Fraud and other Fraud Offenses, Part I. CRIMES, 18 U.S. Code Title 18—*Crimes and Criminal Procedure.*

National Institute of justice (2007). *Investigative Uses of Technology: Devices, Tools, and Techniques*, p. 37, https://www.ojp.gov/pdffiles1/nij/213030.pdf.

Constanţa Court of Appeal (2015). *Criminal conclusion no. 874 / P of October 7.*

*** (1996). European Convention on the Transfer of Sentenced Persons, adopted in Strasbourg on 21 March 1983, Published in the *Official Gazette* no. 154 of July 19.

*** (2001). *Council of Europe Convention of 23 November 2001 on Cybercrime*.

*** (2003). Law no. 161 of April 19, 2003 on some measures to ensure transparency in the exercise of public dignity, public office and in the business environment, prevention and sanctioning of corruption, Published in the *Official Gazette,* no. 279/21.

*** (2006). Regulation no. 6 of October 11, 2006 on the issuance and use of electronic payment instruments and the relations between the participants in transactions with these instruments, published in the *Official Gazette* Part I 927.

*** (2012). Law no. 187 of October 24, 2012 for the implementation of Law no. 286/2009 on the Penal Code, Published in *the Official Gazette*, no. 757 of November 12, 2012

2. Author's works (national and international):

Amza, Tudor (2008). *Criminologie- Tratat de teorie şi politică criminological*. Bucharest: Lumina Lex Publishing House.

Dobrinoiu, Vasile; Pascu, Ilie; Hotca, Mihai Adrian; Gorunescu, Mirela; Păun, Costică; Dobrinoiu, Maxim; Neagu, Norel & Constantin Sinescu, Mircea (2016). *Noul Cod Penal Comentat, Partea Specială, Ediția a-III-a*. Bucharest: Universul Juridic Publishing House.

[1] Regulation no. 6 of October 11, 2006 on the issuance and use of electronic payment instruments and the relations between the participants in transactions with these instruments, published in the Official Gazette Part I 927 15.11.2006.

Gheorghe, Alecu & Barbăneagră, Alexei (2006). *Reglementarea penală și investigarea criminalistică a infracțiunilor din domeniul informatics*. Bucharest: Pinguin Book Publishing House.

Montague, David A. (2006). *Fraud Prevention Techniques for Credit Card Fraud*. Victoria: Trafford Publishing House.

Zainea, Mariana & Simion, Raluca (2009). *Infracțiuni în domeniul informatic, Culegere de practică judiciară*. Bucharest: C.H. Beck Publishing House.

3. Surse online:

https://business24.ro/carduri/carduri-bancare/operatiunea-armaghedon-politia-a-anihilat-o-banda-de-80-de-hoti-de-carduri-80795.

www.rolii.ro.