Legal classification of the offence of installing a card magnetic band reading device („skimmer") within the cash machine slot.

MARIAN DRILEA-MARGA
Law Faculty
Transilvania University
Brasov, 25th Eroilor Avenue
ROMANIA
drilea.marian@gmail.com

Abstract: The content of the notion of offence of informatics nature is extremely varied, being approached from different perspectives within the specialized literature and legal practice. By informatics criminal offence in the broad sense, one can understand any criminal offence in which a computer or a network of computers is the object of a criminal offence, or in which a computer or a network of computers are the instrument or means of carrying out a criminal offence [1] . By computer criminal offence in the restricted sense one can understand a criminal offence in which the perpetrator interferes, with no authorisation, with the processes of automatic data taking over.

Key-word: skimming, skimmer, informatic system, electronic payment instrument, reading device

1 Introduction

Law 161/2003 regulates the following categories of criminal offences: A. criminal offences against the confidentiality and integrity of the data and informatics systems: 1.the criminal offence of illegal access to an informatics system; 2.the criminal offence of illegal interception of informatics data transmission; 3.the criminal offence of the informatics data integrity alteration; 4.the criminal offence of the informatics systems functioning perturbation; 5. The criminal offence of performing illegal operations with devices or informatics programmes. B. Informatics criminal offences: 1. The criminal offence of informatics forgery; 2. Informatics fraud criminal offence. 3. Infantile pornography through the informatics systems.

2 The illegal access to an informatics system

The criminal offence of illegal access onto an informatics system is provided at art. 42 of Law 161/2003. The law envisages the following: (1) The illegal access to an informatics system constitutes a criminal offence and s punished with prison from 6 months to 3 years or with a fee. (2) If the offence provided at paragraph (1) is carried out bz means of breaking the security measures, the punishment is prison from 3 to 12 years. The legal regulation envisages the protection of the informatics systems and the data stored on within by the unauthorised access thereto. The informatics system is defined by the Law as being any device or ensemble of interconnected devices or which are in functional relation, from which one or more ensures the automatic data processing, with the help of an informatics program. An informatics programme is defined by the law as being an ensemble of instructions for obtaining a determined result. By security measures, the law understands the use of procedures, devices or informatics specialised programmes with the help of which the access to an informatics system is restricted or prohibited for certain users' categories. The special legal object consists of the social relationship that regards the security of the informatics system and its inviolability and that are intended to guarantee the confidentiality and integrity of the data, as well as of the informatics systems. The cybercrime was defined as "the whole number of new technology related facts, committed within a certain period of time on a precise territory" [2]. The material object consists of the components of the informatics systems over which the criminal offence activity was endorsed (like data sticks) or through which the illegal access has been initiated (i.e., the components of the informatics networks). The active subject can be any person, and the passive

subject is the owner of the informatics system or of any data contained within. The objective side. The material element of the criminal offence is carried out through an activity of illegal access onto an informatics system. The illegal access onto an informatics system means, in the sense of the law, that this particular person is in one of the following situations: a) it is not authorised, according to the law, or of a contract; the persons that operate in the data base concerning the staff of an institution do so on the basis of the authorisation received from the management of the institution, because it observes the work legislation and the one concerning the personal data; b) exceeds the limits of the authorisation; exceeding the limits of the authorisation can mean the access to resources from inside the company/institution that is at levels of access superior to the ones allowed to the user; c) it is not allowed, from the competent natural or legal person to give it, to use it, to administrate or to control an informatics system, or to develop scientific researches or to make any other operation is an informatics system [3]. The subjective side is determined by the direct or indirect intention. The perpetration has been performed in the moment of actually obtaining the access to the attacked informatics system, regardless of the consequences of that action over the informatics system and the data contained within. The moment of the access can be determined through specific technical means (journal files etc.). The attempt is punished, according to the provisions of art. 47. Sanction. The criminal offence of illegal access to an informatics system is punished with prison from 3 to 6 months, or with a fine. The aggravated situation is punished with prison from 3 to 12 years.

1.1 Legislative and technical aspects concerning the credit card fraud

The credit card, the main instrument of electronic payment used in the transactions without cash, is defined by the Romanian National Bank Regulation no. 6 from October 11th 2006[2] as being: „an information support that is standardized, secured and individualized, that allows to its holder to use the money from an account opened on their name at the issuant of the card and/or to use a credit line, within the limit of a previously established maximum amount, opened by the issuant in favour of the credit card holder, in the view of making some operations"[4].

1.1.1 The operation modalities

The personal identification code related to a card (Personal Identification Number - PIN) is the personal code given in good faith by the issuer to a credit card holder, code that allows the identification of the credit card holder when it is used at a terminal; when the payment can be done through data electronic transfer, the PIN can be considered the electronic equivalent of the credit card holder's signature.

1.1.2 Credit card modalities of use.

There are, mainly, three types of transactions, which can be made with the credit cards: payments with present credit card transactions without present credit card and cash withdrawing. Concerning the cash withdrawing, the operation entails the following procedure: the card holders can withdraw cash from the cash machines (the data stored in electronic format on a magnetic band or on chip shall be read by ATM *(Automatic Teller Machine)* and must correspond to the PIN code introduced by the card's holder); from the affiliated banks and from the foreign exchange office that accepts cards, also from other institutions.

1.1.3 Skimming

Skimming entails the copying of the whole content of one or more recordings on the magnetic band of an authentic card, without the knowledge of the legitimate holder, with the intention of using the data obtained in criminal purposes. Being in possession of the card, the perpetrator (skimmer) shall use a small device of keypad type (keypad) in order to transcribe the Card Security Code, consisting of 3 or 4 digits and that isn't usually present on the magnetic band. In other cases, the skimmer manufactures special devices that imitate the interface of the ATM and that attaches them to the latter, with the purpose to uptake (register, obtain, copy) the identification data of the cards introduced by the confused users. These devices come together with mini video cameras that register the moments of introducing the PIN codes afferent to the cards.

3 The forgery of the electronic payment instruments. Issuing or holding with the intention of their issuance.

ISBN: 978-960-474-291-2

Î.CC.J Penal Section, decision no. 5288 from September 15th 2006 „ The offence of assembling, at a cash machine, a device for reading the magnetic band of the cards, gathers the constitutive elements of the criminal offence of illegal access to an informatics system by breaking the security measures, provided by art. 42(1) and (3) of Law no.161/2003, as the cash machine constitutes an informatics system in the sense of art. 35(1) letter a) of this Law, and by assembling the device for reading the magnetic band, the security measures of the cash machine are broken, with the purpose of assuring that the account's number and the operations carried out are confidential as well as the prevention of the false pretences use of the cards.

The offence of forging electronic payment instruments as the cards, to hold such forged instruments and to withdraw cash amounts of money with their help, gather up the constitutive elements provided by art.24 paragraph (2) of the same law concerning the issuance of the forged electronic payment instruments or their holding with the intention of their issuance, as the issuance of the electronic forged payment instruments can be obtained by the withdrawing of the amounts of money in cash, the transfer of the forged electronic payment instrument's possession by other persons not being necessary."

By the judgment in the criminal case no. 21/2006 of the Hunedoara Court, the following defendants were convicted: C.C., G.M., T.I. and I.F. for criminal offence against the confidentiality and integrity of the data and the informatics systems provided by art. 42 paragraph (1) and (3) of Law no. 161/2003, of the criminal offence of forging of electronic payment instruments provided by art. 24 paragraph (1) of Law no. 365/2002, of the criminal offence of forging of electronic payment instruments provided by art. 24 paragraph (2) of Lawn no. 365/2002, of the criminal offence of false pretences making of financial operation provided by art. 27 paragraph (1) of Law no. 365/2002 and the criminal offence of aggravated theft provided by art. 208 paragraph (1), art. 209 paragraph (1) letter a) and e) Penal Code, all with the application of art. 41 paragraph (2), of art. 33 letter a) and b) and of art. 34 paragraph (1) letter b) Penal Code. The Court withholds that in May 2005, the defendants C.C., G.M., T.I. and I.F. agreed to use the reading devices of the card's magnetic band and a mini video camera which they previously procured, for obtaining the necessary data in order to clone several cards for cash withdrawal purposes. Therefore, in many occasions, the defendants went in different localities, installed the reading devices of the card's magnetic bands and the mini video camera on several cash machines obtaining thereby the data from the cards used on this cash machines, which they downloaded and stored in a computer from the defendant I.F's domicile. After all the obtained data are stored in the computer, the defendants purchased blank cards and glued on each one an adhesive label on which they have written the PIN code or the codes read previously with the mini video camera, at the defendant I.F.'s computer being attached also an electronic inscription device, with the help of which the defendant G.M. made the magnetic band's inscription of each blank, with the account previously copied, corresponding to the PIN code written on the label. In June 28th, July 7 th, July 8 th, July 11th and July 21st 2005, the defendants withdraw cash with the help of the cloned cards from the cash machines of several banks. Through the decision no. 197/A from June 22nd 2006, The Alba Iulia Court of Appeal, penal section, approved the appeals declared by the defendants, changed the legal classification from the criminal offences provided by the art. 27 paragraph (1) of Law no. 365/2002 and art. 208 paragraph (1), art. 209 paragraph (1) letter a) and e) Penal Code, with the application of art. 41 paragraph (2) from the same Code, in a single criminal offence provided by art. 27 paragraph (1) of Law no. 365/2002, with the application of art. 41 paragraph (2) Penal Code, convicted the defendants on the basis of the latter laws and reduced the punishments applied to the defendants.

The declared appeal, between others, by the defendant C.C., through which invoked the cassation case provided by art. 385^9 paragraph (1) pct. 12 Criminal Procedure Code., is alleged. Concerning the defendant's C.C. request through which he wants his exoneration according to art. 11 point 2 letter a) pertaining to art. 10 paragraph (1) letter d) Criminal Procedure Code for the criminal offences provided by art. 42 paragraph (1) and (3) of Law no. 161/2003 with the application of art. 41 paragraph (2) Penal Code and art. 24 paragraph (2) of Law no. 365/2002, in the variant of the issuance of forged electronic payment instruments, with the application of art. 41 paragraph (2) Penal Code it is noticed that it has no legal basis. The dispositions of art. 24 paragraph (1) form the Law no. 365/2002 provide that the forgery of an electronic payment instrument is punished with prison from 3 to 12 years and the prohibition of some rights, and art. 24 paragraph (2) from the same law incriminates the the issuance, in every manner, of the forged electronic payment instruments or their hold in the view of putting them into circulation. From the

ISBN: 978-960-474-291-2

examination of the objective side of this offences, results that there are two different criminal offences, the first one concerning the forgery of an electronic payment instrument, and the second one, putting them into circulation or their hold with the purpose of the issuance of the forged electronic payment instruments. In this case, the issuance of the forged electronic payment instruments was done by the cash withdraw, not being necessary the transfer of the possession of the forged credit cards to other persons. Or, the offences of the four defendants which, on the basis of the criminal offence resolution, forged around 200 electronic payment instruments, gather the constitutive elements of the criminal offence of forgery of electronic payment instruments, provided by art. 24 paragraph (1) form the Law no. 365/2002, with the application of art. 41 paragraph (2) Penal Code. Also, the offences of the defendants which, on the basis of the same criminal offence resolution, held for the issuance and put into circulation forged electronic payment instruments, gather the constitutive elements of the criminal offence of forgery of electronic payment instruments, provided by art. 24 paragraph (2) of Law no. 365/2002, with the application of art. 41 paragraph (2) Penal Code. The provisions of art. 42 paragraph (1) of Law no. 161/2003 incriminates the access, without right, at an informatics system, this being punished with prison from 3 months to 3 years or with a fine, and paragraph (3) of the same article provides that, if the offence form paragraph (1) is done through breaking the security measures, the punishment is prison from 3 to 12 years. It must be specified the fact that the cash machine is a mean of collecting, processing and sending of some informatics data, represented by the holder's account number, that is stored on level 2 of the black magnetic band. On the other side, through assembling of the card's magnetic band reading device (skimmer) in the slot of the cash machine, through which the card is introduced and the reading of the magnetic band of each card is made, storing in this manner the information obtained, were broken the security measures that had as purpose to ensure that the account number and the operations made were kept secret, also the defence against the use by another person of these cards for forgery. So, from the evidences of the case results that the defendants accessed an informatics system, without having the right to do so, breaking in this manner the security measures. So, the defendants' offences which, on the basis of the same criminal offence resolution, assembled on different cash machines a cards' magnetic band reading device, also a mini video camera, accessing in this manner without the right, by braking the security measures, the Banks' cash machines, that represent a informatics system in the sense of the Law, gather the constitutive elements of the criminal offence against the data and informatics system's confidentiality and integrity provided by art. 42 paragraph (1) and (3) of Law no. 161/2003, with application of art. 41 paragraph (2) Penal Code. Because, in this case, the offences made by the defendant C.C. gather the constitutive elements of the criminal offences provided by art. 42 paragraph (1) and (3) of Law no. 161/2003, with the application of art. 41 paragraph (2) Penal Code, and art. 24 paragraph (2) of Law no. 365/2002 concerning the electronic trade, in the version of putting in circulation of the forged electronic payment instruments, with the application of art. 41 paragraph (2) Penal Code, there are no basis for his exoneration in the requested sense. For this reasons, the defendant's appeal was rejected (Î.C.C.J., Penal Section, decision no. 5288 from September 15th 2006). We consider that the decision of the High Court of Cassation and Justice is erroneous and rejected unjustified the defendants' appeal concerning some of their offences' classification in the provisions of art.42 paragraph (3), of Law 161/2003,Title III-Prevention and defence against the informatics criminal offences, that punishes with prison from 3 to 12 years, the illegal access at a informatics system, with the purpose of obtaining informatics data, by forcing the security measures. In the opinion of many authors, the cash machines (ATM) were included in the category of informatics systems because, technically, these respect the conditions in order to be considered as informatics systems. We can agree that the cash machine (Automatic Teller Machine – ATM) is an informatics system, accepting the definitions of Law 161/2003, because of the following reasons: 1. It is an electronic device, "a tool intended for collecting, processing and sending informatics data, represented by the account number of the owner" [5], interconnected with other electronic devices (in a bank network) and processes automatically informatics data through a informatics program (the cash machines are, in fact, some computers - with operation systems – at which some drawers are attached – vaults – were the banknote are stored). 2. The security systems of the cash machines are of the LOGICAL type. That means functions which offer a value of „true" or „false" according to the type of data stored on the magnetic band of a card and the PIN introduced from the keypad. 3. If at a cash machine we introduce a card that we have found, or we use it with false pretences, but we don't know the PIN code, this shall be rejected or

ISBN: 978-960-474-291-2

captured by the ATM, and the operations shall be blocked, because the correspondence does not take place. Although, the only security elements of the cash machines are the logical ones and that is informatics applications that establish the validity or the availability of a card on the basis of a mathematics function that offers the value of „true" or „false" for the combination of information stored on the magnetic band of the card or obtained through the introduction of the PIN code by the holder. A forced attempt of the security measures associated to this informatics system (the cash machine or the ATM) would suppose a direct and immediate interaction, of the perpetrator with the informatics security elements of this device or over the mathematics function, which is impossible to do from the point of view of using a skimmer in the analysed conditions.

Or, in the analysed case, the perpetrators attached to the interface from metallic or plastic material of the cash machine, a special device created to induce into error the users, letting them believe that they are in front of an original cash machine and in this manner, to use their own cards. The cash machine is a mean of collecting, processing and sending of some informatics data, represented by the account number of the holder, which is stored on the level 2 of the black magnetic band. Through the assembly of the card's magnetic band reading device („skimmer") in the slot of the cash machine, through which the card is introduced and the reading of the magnetic band of each card is made, storing in this manner the information obtained, there is no contact with the security informatics elements of the ATM so the informatics system is not at all accessed. The extraction of the data from the users' cards – inclusively the processing or combining them with the images caught by the mini video camera that entails the typing of the PIN codes– takes place only subsequently. We consider that in this case, it is not about an authorised access by breaking the security measures over a informatics system.

4 Conclusions

Analysing the mentioned aspects, we reach to the conclusion that in the nowadays legislation, with the legal existent instruments, the offence of Skimming made in the manner described previously, can't be legally classified in the dispositions of art. 42 paragraph (1) and (3) of Law no. 161/2003, and the extremely high number of this type of actions signals the need of a distinct norm of incrimination, its place nowadays being only in the content of art. 25 of Law 365/2002 and any reference at the criminal offence of illegal access at an informatics system is erroneous. According to art 25 of Law 365/2002:"The manufacturing or hold of equipment, including hardware or software, for forgery of the electronic payment instruments is punished with prison from 6 months to 5 years." For improving the Law 365/2002, we propose the following laws that would correctly and indisputably incriminate any type of skimming:

„The assembly, attachment or dissimulation of equipment or technical device of the hardware or software type, created for the false pretences obtaining of data or information associated to an electronic payment instrument or a bank account, constitutes a criminal offence and it is punished with prison from 6 months to 5 years"

„Obtaining by false pretences in any manner, including by using some technical devices created for this purpose, or using the communication electronic means (telephone, fax or informatics systems), of any data or information associated to an electronic payment instrument or bank account constitutes a criminal offence and is punished with prison from 3 to 12 years. "

References:

[1] Univ. prof. dr. Dan Banciu, univ. conf. dr. Ion Vladut, *Internet and Informatics criminal offence,* Bucharest, 2001 ;

[2] T.Amza,C.P.Amza, *Cybercrime*, LuminaLex Publishing, Bucharest, 2003, page 13 ;

[3] Gheorghe Alecu, PhD and Alexei Barbaneagra, PhD, *The criminal regulations and the informatics criminal investigation of the computer related crimes*, Pinguin Book Publishing, Buc.2006, pages 73-74;

[4] Romanian National Bank Regulation no. 6/2006 was published in "the Official Gazette of Romania" part I, no. 927 from November 15th 2006. The norms contained in this regulation are compatible with the Directive no. 2000/46/C.E. of the European Parliament and of the Council from September 18th 2000;

[5] Mihai Adrian Hotcă, Maxim Dobrinoiu, *Crimes envisaged by special laws. Comments and clarifications*, C.H.Beck Publishing, Bucharest 2008