Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Fraud: A Comparative Legal Analysis

Miha Šepec[1]
University of Maribor, Slovenia

Abstract

The purpose of the article is to present modern criminal law approach to computer-related fraud. Modern concept of fraud in criminal law includes deceiving a computer system and is becoming an established concept in the developed countries. However, the Slovenian Criminal Code has not yet adapted to the changes the new technology has brought. We still cling to the traditional concept by which only a physical person can be deceived (and not a computer system).The Slovenian Criminal Code has not implemented the demands of the Convention on Cybercrime and should, therefore, be amended. My conclusions regarding computer fraud could also prove useful to some other countries coping with the same criminal legislation as Slovenia. After a careful examination of the term computer fraud and its forms, I will use a comparative method that includes examination of international documents, surveys and Criminal Codes. Comparative research is one of the essential methods of criminal law methodology, since it allows comparison with the achievements and approaches favored by other Legislatures and criminal law theorists. Compared to numerous other countries having already overcome the traditional concept of fraud, Slovenia and its law experts have, so far, neither faced the problem of computer-related fraud nor the need to overcome its traditional concept. In this regard, the article can contribute to domestic as well as comparative criminal law theory.

Keywords: Fraud, Deceit, False representation, Modern concept of fraud, Traditional concept of fraud, Computer system, Information system, Cybercrime, Criminal Law.

Introduction

The concept of "fraud" is one of the oldest criminal offences and has been around in the human society since the beginning of trade and commerce. In today's information age, where vast amount of trades, commercial services, and payments are made by means of the Internet and computer systems, the traditional offence of fraud has gained new

[1] Ljubljana Law University graduate, Criminal law assistant at European Law Faculty - University of Nova Gorica and Faculty of Criminal Justice and Security - University of Maribor, PhD candidate at Law Faculty of University of Maribor, Slovenia, email: miha.sepec@fvv.uni-mb.si and miha.sepec@hotmail.com

dimensions. Therefore, law theory soon realized that the traditional concept of fraud could not cover the new forms of computer related frauds. Due to the development of information technology, a modern concept of computer fraud was formulated - a concept that we will try to present in this paper.

Fraud in its essence basically means a willful misrepresentation of truth or concealment of material fact in order to induce another person to act to his or her detriment (Black's Law Dictionary, 2004). Albrecth et. al., (2011) argues that fraud is a deception that includes a representation about a material point, which is intentionally or recklessly false, and which is believed by the victim. Fraud, therefore, consists in taking advantage of a person or in misleading that person, regarding specific facts with the purpose of property or monetary gain. Deisinger explains (2002) that basic element of fraudulent criminal act is to create false representation in the victim's state of mind or to let the victim in this state. False representation of facts means, that the perpetrator creates a wrong idea of the circumstances and facts. Error in the victim's thinking process is created due to the offender's false claims about the actual circumstances.

The Slovenian Criminal Code (KZ-1, 2008) defines fraud in Article 211 as: "Whoever with the intent of obtaining for himself or a third person an unlawful material benefit, damages the property of another by causing or maintaining an error by pretending false facts or by distorting or suppressing true facts." It is clear that fraud can be executed by a commission ("causing or maintaining an error by pretending false facts") or by an omission ("suppressing true facts").

An essential element of fraud is the financial purpose of the offender. His goal is to gain material benefit or originate property loss. With no financial purpose involved, the offender's act cannot be termed as fraud but as deceit, which is often a statutory element of other offences. As Deisinger (2002) explains, deceit conceptually means cheating, but from the criminal law perspective this is not equivalent to the criminal offence of fraud. In case of fraud the fraudulent intent has to be present before the conclusion of a contract; in case of deceit, on the other hand, this intent can also occur later. Moreover, deceit is not necessarily connected with a direct financial gain of the offender; it can be a leading motive, though.

The Anglo-American criminal law system makes a clear distinction between fraud and deceit.[2] Unlike false representation (which is one-sided), deceit is a two-sided concept. The first requirement is a false representation by the offender. The second is that someone was deceived by this untrue representation. "The victim must have been taken in or "conned" by this false representation, so that the victim believed it to be true. False statement must have operated on the victim's mind" (Heathon, 2006, p. 327). On the other hand, fraud is a general term for a criminal offence that always includes a financial motive of the offender. Theorists also refer us to the problematic definition of fraud and deception in the economy and business world. In 1919, Page wrote that failure of one party to notify the other of the known facts, does not always constitute a fraud or affects the validity of an agreement.

It is considered that there is an exception to the duty to disclose information, when that information was obtained deliberately. According to Kovač (2010) this is clearly seen in Neil v. Shamburg (1983), where the buyers of a real estate ordered an expensive investigation of the estate, which showed that there was oil under the estate. They did not

[2] According to Ormerod (2005) there was no clear demarcation of the relationship between »fraud« and concepts such as »deception«, »dishonesty« and »with intent to defraud« in common law.

notify the seller about their findings. The court ruled that there was no fraud by omission committed by the buyers – they had no duty to inform the seller about the properties of his estate.

Kovač (2010) believes that parties should have the right to lie and conceal information when it comes to unverifiable statements, personal opinions and judgments. Such statements are completely subjective and, generally, not verifiable, which the other party should be aware of. Furthermore, to commit a fraud, the offender has to create a wrong idea of circumstances or facts in the perception of the other person. Another possibility is that the offender does not explain certain circumstances to the other person, although he was legally committed to do so by law or by a contract relationship that demanded such an explanation (Deisinger, 2002).

It is obvious that the duty to disclose information will depend on the nature of the contract and that the line between business deal and fraud committed by omission can often be blurred. It is fairly clear that the seller will have to notify the buyer about all the hidden faults of the item being sold, but on the other hand, the buyer will have no legal obligation to notify the seller that the item being sold is worth far more than the price the seller has specified. However, the appraiser who was hired by the seller to determine the price of an item, can be liable for fraud if he gives false information about the price of the item and offers to buy it (by the price that is far lower than the actual worth of the evaluated item).

There are also concerns regarding errors and mistakes of will. Theory of civil law teaches us that a mistake is relevant when the contractual partner would not have made the deal if he had known about the relevant circumstances and could reasonably assess the deal (Dolenc, 2003). Kovač (2010) warns us against economic and analytical shortcomings of such an approach. First, each and every change in the available information (in the condition of perfect competition) would lead to a different decision-making. Second, (in the condition of imperfect competition) knowledge of certain details will usually not change the decision of most buyers.

Computer-related fraud

When fraud is associated with computers, it can be broadly identified as computer fraud. Dragičević (1999) explains that computer fraud covers various manipulations of data, usually with the intent to acquire property gain or other benefit. It's important to note that by the traditional concept of fraud, the perpetrator has to make a false representation to the victim who is consequently defrauded of money or property. And now let us presume that it is not a physical person who is deceived by the perpetrator, but a computer system (the offender lies to an ATM machine that he is the owner of a bank card, although the latter has been stolen). Is this a computer fraud? Can a computer system be defrauded (in the classical legal term)? Leaving aside the questions of artificial intelligence, the answer of a traditional criminal lawyer is quite clearly no, since a computer has no mind and therefore cannot be defrauded.

While the purpose of a "hacker" is to trick and abuse a computer system, the purpose of a fraudster using a computer system is to defraud or deceive a person. However, this can be done directly or indirectly. The direct computer fraud consists of perpetrator cheating on a person using a computer system – a real person is deceived, while the perpetrator is using a computer system to do it. Indirect computer fraud, on the other hand, consists of perpetrator defrauding a computer system (the latter is programmed to

trust the perpetrator and to perform certain services for him – e. g. ATM machine unjustifiably provides money for him). The one actually cheated (indirectly of course) is a physical or legal person behind the computer system (bank, online shop owner, owner of a credit card).

The Slovenian criminal law acknowledges direct computer fraud, however, it should also recognize indirect computer fraud, the one established by the Convention on Cybercrime, which was also signed by Slovenia. The fact remains that the development of information systems and Internet presents new opportunities in the area of fraud. As Clough (2010, p. 183) writes: "The Internet is a paradise for those who prey over the gullible, the greedy and the naive, because it allows unprecedented access to the victim." Access to potential victims via Internet is virtually unlimited, anonymity on the Internet encourages offenders and with the combination of international dimensions hardens criminal prosecution of online frauds. The fact that the Criminal Code, as a country's elementary law regulation on combating crime, does not recognize indirect computer fraud, could lead to extreme difficulties in prosecuting cyber crime frauds.

Types of computer-related frauds

Clough (2010) divides types of computer-related fraud into the following categories:[3]

a) Fraudulent sales online
b) Advance-fee schemes (Nigerian fraud)
c) Electronic funds transfer crime
d) Fraudulent investments
e) Identity crime

a) Fraudulent sales online

Despite its simplicity, fraudulent sales online are still the most common type of fraud in the Internet space. Crime Complaint Center, working with the FBI, reports that in the year 2010, the number of frauds, where goods where not delivered or paid, are still at the top with 14.4 percent (Crime Complaint Report, 2010). The buyer commits a fraud by not transferring money for the goods, by sending counterfeited money or cheque without coverage. On the other hand, the seller commits a fraud when he undertakes to send the goods after the payment, but they are never sent or are of substantially lower quality than agreed.[4]

This is the most basic form of fraud where we must prove that the perpetrator intended to defraud the opposite side, that he intentionally misled the other party (that the goods will be sent, even though he never had any intention to do so, or that such goods do not even exist, or are not attainable) and that the inability to pay or dispatch the goods is not due to market or any other economic condition the »guilty« party had no control over (e.g. goods were destroyed in transport or lost in mail). These forms of fraud have been around since the beginning of trade and commerce. Information and computer

[3] There are of course numerous criminal classifications of computer-related frauds. Vriesde (2001), for example, classifies fraud in cyberspace into the following categories: In-company fraud, Virtual ghost shop, Telephone card fraud, Trade in hot air, Credit card fraud, Internet auctions, Stock exchange fraud and Diskette fraud.

[4] See also Conradt (2012), Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case.

technology have only contributed to expanding the range of these offences by adding some new forms.[5]

b) Advance-fee schemes (Nigerian fraud)

Electronic mail users treat the Nigerian fraud or Scam 419[6] as synonymous with the Internet fraud. The Nigerian fraud consists of e-mails in which the offender dishonestly makes a false representation and with it deceives the victim by promising huge benefits, but only after the victim has sent a certain amount of money to the perpetrator (for the purposes of bribery of officials, overcoming official barriers, airline tickets, payment of taxes, etc.). When the perpetrator receives the money, he cuts all connections with the victim or tries to swindle even more money out of the naïve victim with new excuses and lies. According to Peršak (2002) scam 419 is a relatively simple adaptation of the traditional advance-fee fraud in a highly complex organized criminal activity.

The perpetrators rely on greed and naïveté of the people and sometimes on the mercy and willingness to help (the offender presents himself as a poor man having suffered a severe accident and is now collecting money for heart surgery, tumor, or as a miserable man taking care of his sick child). This is certainly the most commonly practiced type of fraud today. There is basically no individual user of e-mail who has not received numerous Nigerian fraud attempts. Despite the simplicity and sometimes the stupidity of such emails, the investigations conducted in this sphere disclose (Ultrascan Advanced Global Investigations, 2009) that fraudsters are successful in about one message out of every ten thousand sent. As to Modic (2009) fraudsters can expect that individuals will respond to one letter out of every hundred. Among the respondents, at least, one person in every hundred will send the money. Dragičević (1999) notes that such frauds can be performed without significant expertise or technical knowledge.

c) Electronic funds transfer crime

Today money flows through credit and paying cards. Account balance is presented by a digital record of one's bank account. Various forms of fraud and theft of this money are therefore taking place in a digital form. There is often a link with an identity theft - the offender presents himself (with a forged or stolen document) as the owner of a bank account and thus defrauds the banking system or the employee of the bank and has the money drawn for him from the victim's bank account. More recent forms of fraud include fictitious investments in funds where perpetrators pose as bank or insurance agents collecting money for their investments. They collect money from several victims who deposit money on a certain bank account (set up with a false identity), then they empty the account and disappear.[7]

---

[5] We have lately been witnessing the so-called "scareware" programs which offer a free inspection of our system to verify if it is "infected" with malware (damaging codes like viruses). Free inspection reveals that the system is severely infected and that it needs to be cleaned. We are then offered to buy the program that eliminates the infection (which of course was never there, since it was generated by the program itself). Thus, the misled customers who are afraid that their system contains malicious codes, purchase the program, although there was really no need for it. It is quite clear that this is an example of a cyberspace fraud.

[6] After Article 419 of the former Nigerian Criminal Code.

[7] This is a sort of "Ponzi scam" named after a famous fraudster and swindler Charles Ponzi, who became famous in the early 1920s (Bell & Fleitas, 2004).

d) Fraudulent investments

Various forms of fraud connected with investments, stock trading and business practice are included in this segment. Clough (2010) lists examples of using the Internet to influence the stock price - the so-called "pump and dump" or "trash and cash" scams. Perpetrators operate on Internet forums, where they affect the stock price with false statements. Clough (2010) describes a well-known example of eleven offenders who with the usage of e-mail and Internet forums artificially raised the price of shares of Chinese "penny stock" companies and thus earned about 3 million dollars. Various forms of fraud on WebPages are also included in this segment. Perpetrators create an Internet page that is supposed to be an on-line store with excellent prices. Such websites usually "operate" only a week or two - just enough to defraud a certain number of customers. The website (together with the perpetrators and the money) will disappear before being reported to the police.

e) Identity theft

Identity theft is a new type of crime similar to fraud, where the offender steals the identity of the victim and presents himself as the victim, causing in this way damage to the person whose identity has been stolen. Adequate safeguards of personal data of the individuals are provided by the Article 38 of the Slovenian Constitution. Personal data define the characteristics of a person distinguishing him/her from the other individuals. The use of foreign personal data represents a serious intervention into one's identity, which can cause tremendous emotional or material damage. We should remember a BBC journalist who spent two days in custody in Slovenia, because a crime was committed abroad under his name (the real offender had used the passport of the journalist).

There is no internationally recognized definition of identity related crime. The Australian Centre for Police Research (2008) adopted some general definitions which are worth mentioning:

- **Identity crime** is a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity or a stolen/assumed identity to facilitate the commission of crime.
- **Identity fraud** is the gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity, or a stolen/assumed identity.
- **Identity theft** is the theft or assumption of a pre-existing identity (or a significant part thereof), with or without consent, and whether, in the case of an individual, the person is living or deceased.

Identity theft in practice is committed in the following forms:

- Credit card scams
- Theft of information from databases
- Social engineering: manipulation of people to trust the perpetrator with confidential information
- Falsification of profiles and personal data through databases (e.g. creating fake online profiles with the purpose of deception)

- Phishing: damaging e-mail that presents a business opportunity. The perpetrator attempts to lure the user in the name of his bank, insurance agency, etc., that he is required to enter personal data, which is then abused.

In the amendment to the Slovenian Criminal Code (KZ-1B, 2011) the main Article that deals with identity theft is the Article 143 (Abuse of personal data), which in paragraph 4 stipulates that whoever assumes the identity of another person or exploits the victim's rights by processing his or her personal information, or acquires monetary or nonmonetary benefit on his or her account, can be sentenced from three months up to three years of imprisonment.

The sixth paragraph of that article provides a higher sentence (up to five years imprisonment) if the act is committed by a public official. Other countries do regard the identity theft as a criminal offence, as well. The German Criminal Code (StGB, 1998) contains three Articles that deal with identity theft. The First paragraph of Article 273 of StGB (Tampering with official identity documents) stipulates that whosoever for the purpose of deception in legal commerce:

1. removes, renders unrecognisable, covers up or suppresses an entry in an official identity document or removes a single page from an official identity document or
2. uses an official identity document altered in such a way shall be liable to imprisonment of not more than three years or a fine.

Article 275 of StGB provides preparatory criminal offences in relation to Article 273.

When dealing with the identity theft in the German Criminal Code, Article 281 (Misuse of identity documents) is of fundamental importance. The article stipulates that whosoever for the purpose of deception in legal commerce uses an identity document which was issued to another, or whosoever for the purpose of deception in legal commerce supplies to another an identity document that was not issued to that person, shall be liable to imprisonment of not more than one year or a fine. The mere attempt shall also be punishable. The article also explains that certificates and other documents which are used as identity documents in commerce shall be equivalent to identity documents.

In the USA the identity theft is described in the Article 1028 (Title 18, Chapter 48) of the United States Code (2006). It offers quite a thorough definition of the identity theft. Core crime of the identity theft is described in paragraph a) point 7) as: "Whoever, in a circumstance described in subsection (c) of this section knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

Sentencing differs as to the characteristics of the crime - if the offence is committed to facilitate a drug trafficking crime or in connection with a crime of violence, or after a prior conviction under this section becomes final (up to 20 years), if the offence is committed to facilitate an act of domestic terrorism (up to 30 years), and a fine under or imprisonment for not more than one year, or both, in any other case. A sentence of fine or imprisonment for not more than 15 years, or both, is threatened if the offence involves the transfer, possession, or use of one or more means of identification if, as a result of the offence, any individual committing the offence obtains anything of value aggregating $1,000 or more during a one year period.

The first paragraph of Article 402.2 of the Criminal Code of Canada (1985) stipulates that everyone commits an offence that knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

The types of crime and legislations as described above make it clear that computer systems are bringing new forms of frauds into the criminal law. Computer systems are becoming key elements that substantially facilitate execution of a fraud by giving the perpetrator protection through anonymity and access to a wider circle of victims.

Convention on Cybercrime and international requirements

Article 8 (Computer-related fraud) of the Convention on Cybercrime demands that:

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) any input, alteration, deletion or suppression of computer data;

b) any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person."

Similar to forgery, fraud is a typical offence that can be performed with the help of a computer system – the latter is used as a tool or a device for committing the offence. However, the fact remains that with the arrival of computer systems and new technology on the scene new forms of frauds (Nigerian fraud, fraud by wire transfer of money laundering, identity theft) are being generated. These frauds consist mainly of input manipulations where incorrect data is fed into the computer, or by programmed manipulations and other interferences with the course of data processing. Countries that signed the Convention should therefore check their national legislation if it includes the criminalization of fraud carried out through a computer system or against a computer system. If so, the national law does not need to be amended.

The Explanatory report on the Convention on Cybercrime (2001) states that the aim of this article is to criminalize any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property. Therefore, the object of the Convention is to protect property. Frauds are committed by changing data, by falsifying documents or by misusing credit cards. The act itself is very similar to the traditional fraud with one important difference - the act takes place in the computer space ("cyberspace") or is associated with it. With the intent to cover all forms of computer-related fraud, the Convention provides that computer fraud can be committed with any input, alteration, deletion or suppression of computer data. This is clearly evident in Article 8b) which includes a general provision of any interference with a function of a computer system with fraudulent or dishonest intent of procuring, without right, an economic benefit. The term "without right" is crucial and excludes all acts committed upon consent or other legitimate common commercial practices which are intended to procure an economic benefit (Explanatory report on the Convention on Cybercrime, 2001).

However, pieces of advice and opinions cannot be related to a criminal offence of fraud. Heathon (2006) explains that a business director, who recommends that a person should invest £5000 in his company and that this is a good investment that will bring money, is stating an opinion and not a fact (so there is no fraud). It is important that the

director has a strong belief in his doings and works for the goal he has set to himself. If the director makes all kinds of empty promises (which he had no intention to fulfil), gets the money under the guise of investment, and spends the money on his own interests, he will, of course, have committed a fraud. Ormerod (2005) points out that the doctrine of opinions and pieces of advice (that exclude the notion of fraud) gains ground immoderately. It is extremely difficult in practice to distinguish deception, if it was rendered as an opinion or belief of someone, or as part of intent to defraud.

Overall, it is clear that the Convention on Cybercrime requires that the parties criminalize direct computer fraud (where the perpetrator deceives the victim with the help of a computer system) and indirect computer fraud (where the perpetrator directly deceives a computer system to perform some kind of a function or service that brings unjustifiable financial gain to the perpetrator or somebody else, or causes financial loss to the victim).

Criminal law review

A computer-related fraud has two different forms of execution. One is where computer systems are used as assets to commit a fraud, the other is where the computer system itself is deceived – computer system is the target of the offence. The Legislator has two options regarding the legislation of computer fraud. One option is to have two different offences – the first is a traditional fraud and the second a special computer fraud offence. The other option is that no special computer fraud offence is implemented in the Criminal Code; however, a computer related fraud should then be covered by a general offence of fraud. In this case the Legislator must be careful while prescribing a rather all-embracing offence which has to capture various types of computer-related frauds. Problems occur if the Criminal Code does not implement a special computer fraud offence and the general offence of fraud demands deceiving of a person. This means that only one form of computer fraud is covered by the Criminal Code – the other, where the computer system itself is the target of fraud, is not covered – which is not in accordance with the prescriptions of the Convention on Cybercrime. The first solution is clearly more practical and dogmatically correct. The Slovenian Legislator has unfortunately opted for the second option; consequently, the Slovenian Criminal Code contains only the traditional definition of fraud and no special offence of computer fraud.

Slovenian criminal law review

The Slovenian Criminal Code (KZ-1, 2008) comprises two basic fraud offences - one in Article 211 (Fraud) and the other in Article 228 (Business Fraud). In spite of the same name (Fraud), both offences are fundamentally different. Article 211[8] represents fraud in its true sense and requires fraudulent intent before concluding a deal, trade or exchange, while Article 228 is in fact a deception, where the consequence of the act is property gain or property damage that results on account of that deception. Offence under Article 228 has to be committed in connection with business activity; otherwise we are dealing with a "normal" fraud under Article 211.

[8] Paragraph 1 of Article 211 of the Slovenian Criminal Code stipulates: "Whoever with the intent of obtaining for himself or a third person an unlawful material benefit, damages the property of another by causing or maintaining an error by pretending false facts or by distorting or suppressing true facts, shall be liable to imprisonment of not more than three years."

The perpetrator of a business fraud after Article 228 can form criminal intent even after the business deal was made (Deisinger, 2002). For example: the director of a company A asks the victim B if she would invest into his company. In this stage A's intentions are to gain the money he needs for investments so that his company could profit and, later, everybody would benefit from it. But after receiving the money and before investing it in the company, something goes terribly wrong and the company is on the brink of collapse. A then decides to use the money for something else and lies to B that all the money invested in the company was lost. A is therefore, guilty of business fraud under Article 228. If A had already formed the intent to defraud B when asking for the money, he would have committed Fraud under the Article 211 of the Slovenian Criminal Code. Both Articles can of course be applied when a deception or fraud was committed using a computer system as means of the crime. The Slovenian Criminal Code has no special Article dealing with computer-related fraud or computer-related deception. Both are included in Articles 211 and 228 of the Slovenian Criminal Code.

However, there is a serious flaw in the concept of fraud that the Slovenian Legislature has overlooked. Article 211 and 228 can only be applied when a person (victim) is deceived or defrauded. This means that we can apply both Articles when the perpetrator deceives or defrauds another person using a computer system (e.g. the Nigerian Fraud, where the victim is defrauded via e-mail communication). These are the so-called direct computer frauds. And what about the indirect computer frauds and deceptions, where the computer system itself is defrauded.[9] Behind the defrauded computer system there is, of course, a true person (or legal person such as a bank) that is the actual victim of the fraud. Nevertheless, the Slovenian Criminal Code demands that another person is directly defrauded – which leads us to the conclusion that examples of indirect computer fraud are not a criminal offence of fraud according to the Slovenian Criminal Code, subsequently, all the Slovenian courts conform to this presumption. In the case VSL III Kp 4/2008 from 4th September 2008 The High Court of Ljubljana decided that fraud can only be committed by deceiving another person and not by deceiving a computer machine – e. g. an ATM machine.[10] This is an absurd position that directly opposes the demands of the Convention on Cybercrime which was ratified by Slovenia in the year 2004. Nonetheless, the Slovenian criminal courts have found a way around this explanation of the Criminal Code.

As to the case VSL III Kp 4/2008 from 4th September 2008 the High Court of Ljubljana confirmed the conviction of grand larceny, committed by an ATM machine intrusion according to the paragraph 1 point 1 of Article 212 of the Criminal Code (Grand Larceny). Criminal jurisprudence and legal theory agree that the use of counterfeit credit cards with a wrongfully obtained PIN code in order to intrude into a bank computer system that manages the ATM machine is considered as an intrusion into a confined space in terms of the paragraph 1, point 1 of the Article 212 (Grand Larceny).

[9] E.g.: The perpetrator presents a counterfeit identification to the ATM machine. Being deceived by the counterfeit ID, the ATM machine hands out money to the perpetrator. The same holds for the cases where the perpetrator puts stolen credit card information to an on-line shopping system that verifies the credit card and takes the money from the card in exchange for goods - a computer system was directly defrauded.

[10] The same conclusion was drawn by the District Court of Ljubljana in the matter I Kp 1216/99 from 17th November 1999 where the court argues that an offence of fraud committed with a foreign credit card can only be committed with a false presentation of the perpetrator pretending to be the rightful owner of the card. The perpetrator must hand over the card and is requested by the seller to sign the receipt (slip). Without his signature there is no criminal offence of fraud.

ATM machine is considered a confined space where money is kept. Unauthorized raising of money from that machine is therefore considered grand larceny. The same position can be found in the opinions of the Supreme Court of Slovenia in matters n. I Ips 98/2004 from 31st May 2005 and n. I Ips 461/2007 from 31st January 2008.

It is an interesting solution which in a way solves the poor methodological definition of fraud in the Slovenian Criminal Code. But can we really affirm the same in cases of the Internet shop frauds, where a computer system is deceived by the perpetrator. It is clear that we are dealing with fraud, not a larceny – the perpetrator does not steal an item, the latter is sent to him on the assumption that he will pay for it. How can this deception be larceny, where the essence of a crime, according to Allen (2007), is a dishonest appropriation of property from another? It is quite clear that when deception is present, we are dealing with fraud, which is neither theft nor larceny. We therefore believe that indirect computer fraud should be incriminated equally as direct computer fraud and should be considered on the same incriminating level as traditional fraud or deception. The same view is shared by theorists as Clough (2010) and Barrett (1997). In the Slovenian criminal law theory this problem has not yet been recognized (Klemenčič, 2007).

If fraud is in question, criminal legislations often require deception of another person according to Dragičevič (1999), which cannot be applied (using an analogy) when the perpetrator defrauds a machine or a computer system. Modern continental legislations have perceived the problem and have accordingly amended their Criminal Codes – the German Criminal Code contains a specific offence of computer fraud, as does the Criminal Code of Croatia, Austria and Finland.

Comparative criminal law review

Let us take a look at the Criminal Codes and legislations of other countries to see how they deal with the problem of computer-related fraud and deception. Comparative approach is an essential method of criminal law methodology, since it provides a comparison of achievements and approaches of other Legislators and criminal law theorists. The Croatian Criminal Code (1997) contains (beside the classical offence of fraud in Article 224) a special criminal offence of computer fraud after Article 224.a. After the first paragraph whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, inputs, uses, alters, deletes or in any other way makes computer data or programs unusable, or disables the functioning of a computer system or programs, and by doing so damages the property of another, shall be punishable by imprisonment of six months up to five years.

After the third paragraph of Article 224.a it is punishable to manufacture, purchase, sell, possess, or allow others to acquire special equipment, facilities, computer data or programs created or adapted for the criminal offence of computer fraud. We have already discussed the need for the Criminal Code to provide a special offence of computer fraud, because traditional concept of fraud demands defraudment of a person. Problems may occur when a computer system is directly defrauded, which is quite often the case with computer frauds. Traditional concept of fraud should therefore be adapted to cover more sophisticated forms of computer frauds. The Legislator can achieve this either by implementing a special offence of computer fraud or by an amendment to the traditional offence of fraud.

Unlike criminal offence under Article 224 (Fraud), the offence after Article 224.a differs as to its execution, i.e. no victim is directly mislead (Pavišić, Grozdanić, & Veić, 2007). The same legal approach is adopted by Germany. The first paragraph of Article 263a (Computer fraud) of the German Criminal Code (StGB, 1998) stipulates that whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorized use of data or other unauthorized influence on the course of the processing shall be liable to imprisonment of not more than five years or a fine.

The second paragraph of the Article states that the provisions of the traditional fraud after Article 263 shall apply mutatis mutandis. As indicated above the criminal law is to follow the changes of the new technology and adapt to the new forms of crimes this technology brings. The solution to computer fraud dilemma in Germany is therefore the same as in Croatia. Furthermore, Austria has also added a new Article to the Criminal Code (Strafgesetzbuch, 1974) regarding computer fraud. Article 148.a - Fraudulent misuse of data processing (Betrügerischer Datenverarbeitungsmißbrauch) was added as a needed response to the demands of the Convention on Cybercrime. The first paragraph of the Article stipulates that whosoever, with the intent of obtaining for himself or a third person an unlawful material benefit harms the property of another by affecting the outcome of data process by a reconfiguration of a program, entry, amendment, deletion or by concealing of data or other similar effect or impact on the data, shall be liable to imprisonment of not more than six months or a fine. It is evident that the legislation text is quite similar to that of Germany.

Similar steps were taken in an amendment to the Finland Criminal Code (1889) in the year 2003 (amendment 514/2003). Finland added a second paragraph to the Article 1 of Chapter 36 (Fraud) of their Criminal Code. The second paragraph stipulates that a person who, with the intention referred to in subsection 1[11], by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, falsifies the end result of data processing and in this way causes another person economic loss, shall be guilty of fraud and sentenced to a fine or imprisonment for up to two years.

As we can see, both Austria and Finland have accepted a specific offence of computer fraud. The United Kingdom legislation experienced a radical change in terms of fraud by passing of the new Fraud Act in 2006. Fraud under common law is a concept of unfairly obtaining material gain by deception. Fraud under common law is a two-sided concept. On one side, we have an act from the perpetrator who makes the false representation. And on the other, there has to be someone who was actually deceived by this untrue representation (Allen, 2007).

We must also point out that under the common law concept of fraud: "The general view was that this precluded "deceiving" a machine where the transaction was fully automated without the involvement of any human mind (e.g., internet orders, computerized banking)" (Heathon, 2006, p. 327). The perpetrator's statement should therefore operate on the victim's mind in a mode of deception, which must have, in due time, caused damage to the victim's property. (Heathon, 2006).

This is why the question of causation often occurred and subsequently changed the offence into a result crime. The new definition of fraud under the Fraud Act (2006)

[11] To obtain unlawful financial benefit for himself or herself.

focuses exclusively on the offender's behaviour and motivation, and does not require results (such as someone's actual deception) caused by this behaviour anymore.

Fraud under the new Fraud Act (2006) can be executed in three forms:

a) False representation after Article 2
b) Failing to disclose information after Article 3
c) Abuse of position after Article 4

After the second Article criminal offence of fraud is committed by a person a) who dishonestly makes a false representation,[12] and b) intends, by making the representation, to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss.

An essential provision is paragraph 5 of Article 2 which stipulates that for the purposes of this section a representation may be regarded as made, if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention). Taking into the account the above formulation, it is quite clear that, compared to the common law; the definition of fraud after the new Fraud Act (2006) has a much wider reach. The new concept does not require that the victim was actually deceived - even if the victim does not believe the offender's lies, this will be regarded as fraud, if, of course, the perpetrator acted with the purpose as described above.

The United Kingdom is now in the position to prosecute new forms of computer fraud that could not have been prosecuted after the common law and old legislation (e.g. indirect computer fraud). Similar legislation can also be found in the Australian Criminal Code Act (1995). Paragraph 1 of Article 480.1 (Definitions in the chapter Financial information offences) defines deception as an intentional or reckless deception, whether by words or other conduct, and whether as to fact or as to law, and includes:

(a) a deception as to the intentions of the person using the deception or any other person; and

(b) conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorized to cause it to do.

This definition of the Australian Criminal Code includes different kinds of computer-related deceptions. Deceptions are, therefore, not limited to cases where a physical person is deceived, but may also include cases where a computer system is deceived. USA has implemented computer fraud in the 18th chapter (§1030) of the U. S. CODE with the Counterfeit Access Device and Computer Fraud and Abuse Act (CFAA, 1984) that was amended in 1986, 1994, 1996, 2001 and 2002. One of criminal activities that are covered by the current CFAA is also accessing a computer to defraud and obtain value (Pollaro, 2010). Computer fraud is committed after U.S.C. Article 1030(a)(4) of Chapter 18 if whoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any one year period.[13] It is clear that USA acknowledges computer fraud

[12] A representation is false if (a) it is untrue or misleading, and (b)the person making it knows that it is, or might be, untrue or misleading - Article 2, Paragraph 2 of the Fraud Act 2006.

[13] There is a debate in criminal theory as to what constitutes an »unauthorized access«. Most courts (e.g. State v. Allen, 917 p.2d 848, Kan. 1996) use a »virtual reality approach«, where a user accesses a computer only by getting »inside« the device and interacting with the data (Dial & Schulof, 2009). However »some

even when an actual person is not directly defrauded, if value is obtained through defrauding a computer system.

Conclusion

Frauds in computer systems are extremely common offences where offenders pursue economic interests. Most common forms of computer-related frauds today are divided into the following categories: fraudulent sales online, advance-fee schemes (also called Nigerian frauds), electronic funds transfer crime, fraudulent investments and various forms of identity crime. The identity theft is, primarily, a constantly evolving crime, becoming more and more of a threat to information systems and everyday on-line life.

There are two basic appearances of fraud related to computer systems. The first one is where computer systems are used only as assets to commit a fraud (the so-called direct computer fraud) - which is conceptually not different from the traditional form of fraud. On the other hand, there are frauds committed against a computer system. The offender deceives or defrauds a computer system in order to obtain financial gain (without any personal deception whatsoever – which is an essential element of a traditional fraud). The so-called indirect computer fraud should, therefore, be recognized by a modern Criminal Code as a criminal offence. This can be achieved by implementing a special offence of computer fraud into the Criminal Code or by broadening the concept of a traditional offence of fraud so that it is not limited to a mere deceiving of another person. If the Legislator does not implement the computer fraud as a special criminal offence and fails to adapt the traditional concept of fraud, the law practice is forced to find a way around such a poor legislation. Since the Slovenian Legislator has failed to recognize the indirect computer fraud (unlike all modern comparative criminal codes), the established law practice now defines the indirect computer fraud as grand larceny. This is an interesting approach, however, it is methodologically questionable and will not work in all situations.

Cybercrime is the fastest developing form of crime in today's society. If the criminal law is to keep up with the advances of computer technology, it has to be more open to new criminal concepts and more receptive to further amendments to criminal legislation. Computer-related fraud is a typical example of a new cyber crime offence. The traditional criminal law concept of fraud that was developed in the pre-computer era, must therefore adapt to this new phenomena. This is fairly evident in the Slovenian Criminal Code. Slovenian legislation as it stands today, does not meet the demands of the Convention on Cybercrime, and hinders the prosecution of computer-related frauds and calls, therefore, for the need to be amended.

References

Albrecht, W. S., Albrecht, O. C., Albrecht, C. C., & Zimbelman, F. M. (2011). *Fraud Examination*, 4th edition. South-Western: South-Western Cengage Learning.

Allen, M. J. (2007). *Textbook on Criminal Law*, 9th edition. Hapshire: Oxford University press.

Australian Centre for Policing Research (2008). Identity Crime. In Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General (2008). Retrieved on 11th February 2012 from:

computer crime statues define the term »access« far broader than any common understanding of the word« (Dial & Schulof, 2009, p. 55).

http://www.scag.gov.au/lawlink/SCAG/ll_scag.nsf/vwFiles/MCLOC_MCC_Chapter_3_Identity_Crime_-_Final_Report_-_PDF.pdf/$file/MCLOC_MCC_Chapter_3_Identity_Crime_-_Final_Report_-_PDF.pdf

Australian Criminal Code Act. Promulgated on March the 13th 1995, last amendment with Act. no. 80 from the year 2011. Retrieved on 12th November 2012 from: http://www.comlaw.gov.au/Details/C2011C00590

Barrett, N. (1997). *Digital Crime: Policing the Cybernation*. Michigan: Kogan Page.

Bell, K., & Fleitas, A. (2004). Top 10 investing scams, Bankrate Archives 2004. Retrieved on 15th February 2012 from: http://www.bankrate.com/brm/news/investing/20020829a.asp

Clough, J. (2010). *Principles of Cybercrime*. Cambridge: Cambridge University press.

Conradt, C. (2012). Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case. *International Journal of Cyber Criminology*, *6*(1), 912–923.

Constitution of the Republic of Slovenia (Ustava republike Slovenije). Slovenian Gazette RS No. 33/1991 from 28th December 1991, with amendments No. 42/1997, 66/2000, 24/2003, 69/2004, 69/2004, 69/2004, 68/2006.

Convention on cybercrime. Council of Europe, ETS 185, 2001**.** Ratified in Slovenia with the Ratification Law: Zakon o ratifikaciji Konvencije o kibernetski krminaliteti in dodatnega protokola h konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih (MKKKDP). Promulgated in Slovenian Gazette No. 62/2004 from 7th June 2004.

Criminal Code of Austria (Strafgesetzbuch). Promulgated on 23rd January 1974 in Austrian Gazette No. 60/1974 i.d.F. BGBl. I with amendments up to the year 2008: Nr. 134/2002, 15/2004, 136/2004, 152/2004, 68/2005 and 56/2006. Retrieved on 5th January 2012 from: http://www.internet4jurists.at/gesetze/bg_stgb01.htm#%C2%A7_146

Criminal Code of Canada. Promulgated in 1985 (R.S.C., 1985, c. C-46), with amendments up to year 2011. Retrieved on 14th November 2012 from: http://laws-lois.justice.gc.ca/eng/acts/C-46/.

Criminal Code of Finland. Promulgated in Finland Gazette No. 39/1889 with amendments up to 940/2008, Finland's Ministry of Justice. Retrieved on 2nd February 2012 from: http://www.legislationline.org/documents/section/criminal-codes

Criminal Code of Slovenia (Kazenski zakonik, KZ-1). Promulgated in Slovenian Gazette No. 55/2008 from 4th June 2008.

Croatian Criminal Code (Hrvatski Kazneni zakon). Promulgated in Croatian Gazette No. 110/1997, with amendments up to the year 2011 - 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08 and 57/11. Retrieved on 4th January 2012 from: http://www.zakon.hr/z/98/Kazneni-zakon

Deisinger, M. (2002). Slovenian Criminal Code with commentary (Kazenski zakonik s komenatarjem, posebni del). Ljubljana (Slovenia): GV Publishing.

Dial A., & Schulof, D. (2009). The Computer Fraud and Abuse Act: An Underutilized Litigation Weapon. Technology Litigation Desk Reference, January 2009. Retrieved on 7th August 2012 from: http://www.kiltown.com/~/media/Files/articles/ADial%20DSchulof%20Technology%20Litigation%20Desk%20Reference_The%20Computer%20Fraud%20and%20Abuse%20Act.ashx

Dictionary of the Standard Slovene Language (2000). Institut Frana Ramovša for Slovenian Language, ZVC SAZU. Retrieved on 10th January 2012 from: http://bos.zrc-sazu.si/sskj.html

Dolenc, M. (2003). Slovenian Code of Obligations with commentary. In Juhart M, & Plavšak N. (ed). Obligacijski zakonik s komentarjem (pp. 346 - 347). Ljubljana (Slovenia): GV Publishing.

Dragičević D. (1999). *Computer Crime and Information Systems* (Kompjutorski kriminalitet i informacijski sustavi). Zagreb (Croatia): Infromator.

Explanatory report on the Convention on Cybercrime (2001). Council of Europe, ETS. 185. Retrieved on 16th December 2012 from:
http://conventions.coe.int/treaty/en/reports/html/185.htm

Fraud Act 2006 of United Kingdom. Promulgated on 8th November 2006. Retrieved on 12th January 2012 from: http://www.legislation.gov.uk/ukpga/2006/35/contents

Garner, B. A. (ed.). (2004). *Black's Law Dictionary*, 8th Edition. USA: West Publishing Company.

German Criminal Code (Strafgesetzbuch – StGB). Promulgated on 13th November 1998 in Bundesgesetzblatt I p. 3322, last amended on 2. October 2009 in Bundesgesetzblatt I p. 3214. Retrieved on 16th October 2011 from: http://www.gesetze-im-internet.de/stgb/

Heathon . (2006). *Criminal Law, Textbook*. Oxford: Oxford University Press.

Internet Crime Complaint Center. (2010). 2010 Internet Crime Report. Retrieved on 17th February 2012 from: http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf

Klemenčič, G. (2007). Cybercrime. In Makarovič B., & Toplišek J. (ed). *Legal Guide to Internet* (pp. 329 – 360), (Pravni vodnik po internetu). Ljubljana (Slovenia): GV Publishing.

Kovač, M. (2010). Pre-contractual disclosure of information: an essential error or fraud (Predpogodbeno razkrivanje informacij: bistvena zmota ali prevara). Podjetje in delo, 26(6-7), 1417-1424.

Law amending the Penal Code of Slovenia (Zakon o spremembah in dopolnitvah Kazenskega zakonika (KZ-1B). Promulgated on 14th November 2011 in Slovenian Gazette No. 91/2011.

Modic, D. (2010). Nigerian fraud letters (Nigerijska prevarantska pisma). In Završnik A. (ed.) *Crime and Technology* (pp. 85 – 93), (Kriminaliteta in kriminologija). Ljubljana: Institute for Criminology at Law Faculty of University of Ljubljana.

Ormerod, D. (2005). *Smith & Hogan Criminal Law*, 11th edition. Oxford: Oxford University press.

Page, W. H. (1919). Law of Contracts. The W. H. Anderson Company. Retrieved on 23rd February 2012 from: http://chestofbooks.com/business/law/Law-Of-Contracts-4-1/Sec-385-Non-Disclosure-Not-Operative-In-Absence-Of-Special-Circumstances.html

Pavišić B., Grozdanić V., & Veić P. (2007). *Commentary of the Croatian Criminal Code,* 3rd edition (Komentar Kaznenog zakona). Zagreb (Croatia): Narodne novine.

Peršak N. (2002). Fraud 419 or the revolution of a fraud (Prevara 419 ali (r)evolucija neke goljufije). Legal Practice (Pravna praksa), 22 (30), VI-VIII.

Pollaro G. (2010). Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope. *Duke Law & Technology Review*, *9*(1-12). Retrieved on 23rd

June 2012 from: http://dltr.law.duke.edu/2010/08/26/disloyal-computer-use-and-the-computer-fraud-and-abuse-act-narrowing-the-scope/

Ruling of the District Court in Ljubljana in the matter I Kp 1216/99 from 17th November 1999.

Ruling of the High Court in Ljubljana in the matter VSL III Kp 4/2008 from 4th September 2008.

Ruling of the Supreme Court of Slovenia in the matter I Ips 461/2007 from 31st January 2008.

Ruling of the Supreme Court of Slovenia in the matter I Ips 98/2004 from 31st May 2005.

Ultrascan Advanced Global Investigations (2009). 419 Advance Fee Fraud Statistics. Retrieved on 11th January 2012 from: http://www.ultrascanagi.com/public_html/html/419_fraud_trends_2006.html

US Code – Code of Laws in the United States (A comprehensive Code of the United States). First published in 1926, current edition published in 2006. Retrieved on 10th September 2012 from: URL: http://www.law.cornell.edu/uscode/

Vriesde, R. (2001). Fraud in Cyberspace, What ever happened to the petty thieves. International Policing Conference 2001. Adelaide, 6 - 8 march 2001, South Australia.