Identity Theft in Electronic Environment:

Does the current approach to the penal legislation of European Union and Lithuania adequate for combating cybercrime?

University of Oslo
Faculty of Law

Candidate number: 8008

Supervisor: Kevin McGillivray

Deadline for submission: 12/01/2012

Number of words: 17,889

27.11.2012

Content

1 Introduction

1.1 Overview

This introductory chapter aims to stress the legal issues at hand by providing a short, contextualized legal and scholarly examination of the electronic identity theft in relation to existing legal background. The examples from ranging from the jurisprudence of the United States of America (USA) to the European Union (EU) are presented in this thesis work. The second aim of this chapter is to present and review the public criminal laws of Republic of Lithuania and propose a specific penal norm regarding the electronic identity theft for the Criminal Code of Lithuania (CC). In addition to this, the thesis provides the reader with a specific overview of the legal issues and interests concerning cybercrimes and particularly the theft of identity in the electronic environment. In order to arrange the proposals for cybercrime section to the CC of Lithuania, the legal attention is focused on revealing all the existing relevant issues regarding this cybercrime area.

1.2 Background and problem definition

1.2.1 The adequacy of the penal legislation of combating cybercrime in the EU and Lithuania

Cybercrime is a relatively novel legal sphere, which nowadays faces a number of legal challenges. One of the most vulnerable areas is the theft of identity in the electronic

environment. With the growth infrequency of the cybercrimes, identity theft has become one of the most prevalent crimes, used in collaboration with other crimes in order to reach the criminal aims. However, due to the novelty of these electronic crimes, not every legal system is able to provide efficient legal background to fight against it. One of these is the member of the European Union, Lithuania. In addition to these issues, it is highly necessary to enhance the legal background of those national states, which are still lacking specific judicial regulation due to the transnational nature of cybercrimes resulting in the negative legal consequences being spread worldwide. For these reasons, it is important to analyze e technical and legal issues as well as already existing legal background, which hinders the legal fight of these malicious electronic acts in order to propose effective criminal regulation for the countries with relatively less active legal development in comparison to the legal systems like that of the United States of America. The differences in the legal backgrounds and frameworks reveals that the understanding of electronic identity theft differs in different continents and it is illustrated by the amount of legal criminal acts enhancing the legal protection from identity theft in electronic environment. The leader in fighting these acts is the USA, despite the fact that huge number of cybercrimes still occur in the country. At the same time efficient legal regulation in the electronic environment supports the stability and legal certainty in this area. However, the regional unit, the European Union, as further chapters indicate, , has not provided proper legal attention to the issue of electronic identity theft compared to the USA. The legal focus on these legal gaps only started receiving attention in 1995, when the first directive of personal data protection was adopted in the EU. These were later followed by " a first legislative proposal, measures against credit card-fraud or fraud and forgery of non-cash means of payment, where the Commission took action as early as 1998, although the Council did not conclude its deliberations until 28 May 2001, when the Framework Decision on Combating Fraud and Counterfeiting of Non-.Cash Means of Payment was adopted."[1] However, EU legal measures of the EU to combat crimes regarding payment instruments related with the offline world were only adopted in 2001.[2] Therefore, all these comparatively late concluded legal initiatives have affected, smaller and less, lawfully developed states, which has faced its legal gaps in the section of cybercrimes, as a regional leader the EU has not provided efficient legal specific proposals regarding the legal measures to be legislated

[1] Erik Wennerström. EU-legislation and Cybercrime A Decade of European Legal Developments <http://www.scandinavianlaw.se/pdf/47-21.pdf> Accessed 5 October 2012
[2] EU Council Decision. Article 6

and implemented, in order to strengthen the contribution to the international legal fight against cybercrimes. Only in the last decade the EU has raised the proposals for the Parliament of the EU, hence the legal efforts to fulfill the legal gaps will measure up to the legal reality.

Furthermore, due to the harmonization of the laws in the European Union the EU member states, such as Lithuania, have to apply the legal penal norms, which are concentrated, more general and not specifically focused on the certain legal problem. Due to this reason, the efficiency is usually lost, or not achieved properly as a result of the existing legal gaps, which produce a perfect environment for the cybercriminals to perform their illegal electronic attacks. The diverging approaches to the necessity to criminalize electronic identity theft are clearly revealed as throughout the decades, the USA has developed efficient legal background against these electronic threats, while the EU is just starting to formulate the necessity of criminalization of these issues. Despite the legal disputes on whether the criminalization of the identity theft is necessary at all, this thesis work reveals the advantages of the criminalization as well as the necessity for this type of electronic threats to be criminalized and regulated by the EU directives and national penal acts in the nearest future.

1.3 Limitations and Purpose

This thesis predominantly envisages the European Union legislation as well as the proposals and the legal experience applying to the area of cybercrimes. The legal focus is only based on the public laws, without specific attention to the private laws. The legal review and analysis is based on the Communications of the Commission to the EU Parliament and Council, Community directives, international legal instruments, such as the Convention on Cybercrimes, public national penal laws and public criminal law of the Republic of Lithuania together with other specific public legal measures. All the legal review is linked to reveal the problematic issues concerning the theft of identity in the electronic environment, as the main aim of the thesis

is to mark the legal drawbacks of non-efficient legal penal regulation on the regional (the European Union) and national levels (the Republic of Lithuania). In order to arrange a proposal for the Criminal Code of Lithuania of the specific penal imperatives for fight against the electronic identity theft, the analysis of the existing legal measures will be taken in the first place.

1.4 Thesis Overview

First chapter provides a brief overview of the concerns rising from the lack of criminalization of specific cybercrimes. Specifically, the section will consider identity theft in the electronic environment. It envisages the legal aspects as the whole problematic issue, regarding the identity theft and the theft of identity in the electronic environment. It gives the reader the formulation of the abstract legal problem, which will be specifically presented in the further chapters of this thesis work. In accordance to it, the first chapter also provides the parameters of the thesis work.

Chapter two provides a brief theoretical part of the question of the personal identity personating the definition of the personal identity, its types and forms. It also provides the scholarly summaries regarding this issue. Together with these aspects, the identification process is presented, which is highly relevant regarding the further discussed aspects of electronic identity theft. Further this chapter provides the reader with a presentation of the novel part of the criminal world- cybercrimes, it also gives the information on the victims of the cybercrimes, as well as the types of these crimes. It reviews the legal background of the USA and the EU legal efforts to the fight with illegal electronic acts.

Chapter three presents the identity theft as a problematic issue, indicates the main trends for the identity theft and electronic identity theft to occur. This chapter also envisages the legal efforts of different regions to combat with this type of electronic crime, presenting the international and regional legal instruments together with the legal analysis and comments aiming to demolish these malicious electronic threats.

Chapter four analyses the specific European Union member state Lithuania as a research object in order to reveal the drawbacks of lacking penal norms in the main national legal criminal instrument – the Criminal Code. With a short overview and analysis of its specific sections of it, together with the analysis of the previous chapter, the remarks and conclusions are being made, which will be relevant for the proposal established in the chapter five.

Chapter five builds on chapter four providing the theoretical aspects of why there is a necessity of criminalizing the electronic theft of personal identity. It stresses the inadequacies of the current main legal penal act of Lithuania and the consequences of the absence of specific objective penal regulation. In addition to this analysis, the end of this chapter proposes a project of a specific penal imperative as a possible suggestion for the legal and legislative institutions of Lithuania for the nearest amendment of the main penal act of Lithuania.

2 Cybercrimes

2.1 Overview

This chapter aims to elucidate the new international problem in cyberspace- cybercrimes. Firstly, it will briefly illustrate the major issues concerning this nationally and internationally performed crime. First it presents the definition and the scope of this chapter, and considers the trends and practices for facilitating cybercrimes together with providing their classification. In addition to this, targets and victims of these crimes will also be indicated. This chapter will then look into the regulatory issues of the United States of America and the European Union area, providing the necessary legal information, which is the first measure seeking to prevent these malicious electronic actions.

2.2. Introduction

Cybercrimes are already considered to be one of the major legal problems of the information society. These electronic crimes have already shown that the electronic environment might be as dangerous area for crimes as the offline world, where until the end of the 20th century the vast majority of the crimes were performed. The Internet's rapid diffusion and digitalization of the economic activities have led to the emergence of a new breed of criminals. "Economic, political, and social impacts of these cyber-criminals' activities have received a considerable amount of attention in recent years as the individuals, businesses, and governments

rightfully worry about the security of their systems, networks, and IT infrastructures."[3] As most scholars agree, cybercrime is quite novel area. Despite that, it is shocking, how fast it absorbs all kind of spheres of the public society life: starting from the financial aspects and ending with moral issues. "The understanding of a cybercrime as a form of illegal economic activity could inform the development of strategies for crime prevention in the future was suggested."[4] It has also been noticed that "organized cybercrimes are linked to other criminal activities such as drug trafficking, gambling, prostitution, and terrorism."[5] These issues strengthen the concern that cybercrimes are not only electronically orientated, but also aim to be connected to the offlinel world, causing even wider disharmony and legal anarchy in the electronic environment. In order to prevent cybercrimes, it is necessary to establish a sufficient legal background, which would combat against them. The United States of America is one of the world leaders in the level of the legal measures already adopted by the federal government to combat cybercrime. It already has a brief and structured plan of how the legal battle against these types of crime should be addressed. At the moment, the USA might still be considered as a regulation leader in this area, therefore the vast majority of examples of the legal adopted measures will be demonstrated from its legal background for the regulation of cybercrimes.

2.2.1 Cybercrime Victims and Targets

2.2.2. Businesses

The USA Federal Bureau of Investigation (FBI) reported that "cyber-criminals have attacked almost all of the Fortune 500[6] companies."[7] According to the market research firm International Data Corporation (IDC), "39% of Fortune 500 companies suffered a security breach in 2003 and

[3] N. Kshetri. *The Global Cybercrime Industry. Economical, Institutional and Strategic Perspectives. USA., 2010,* p.6
[4] Ibid.,, p.6
[5] Antonopoulos, A. 2009. ATM hack: Organized crime or market forces? Network World. Southborough, 26(8), p. 20
[6] Fortune 500 - An annual list of the 500 largest companies in the United States as compiled by Fortune magazine <http://www.investopedia.com/terms/f/fortune500.asp#ixzz2DHgkxFgu> Accessed 1 October 2012
[7] Pollock, J., & May, J. 2002. *Authentication Technology Identify Theft and Account Takeover*. The FBI Law Enforcement Bulletins, 71(6), United States Department of Justice Federal Bureau of Investigation. <http://www2.fbi.gov/publications/leb/2002/june02leb.pdf>. Accessed

40% of global IT managers have rated security as their number one priority."[8] Likewise, according to the FBI, 9 out of 10 US companies experienced computer-security incidents in 2005 which led to a loss of US $67.2 billion.[9] In comparison to this, "an estimate of the European Network Information Security Agency (ENISA) indicated that cybercrimes cost businesses in the European Union 65 Euros billion annually, while a survey conducted among Irish businesses in 2007 revealed, that 98% of respondents indicated that they were cybercrime victims."[10] As it is seen from the public research, the growth of cybercrimes in the USA and the EU has been growing rapidly, concluding that there have not been enough legal measures provided in order to prevent these illegal actions.

2.2.3 Consumers

There is a fact that many consumers have weak technological and behavioral defenses against cybercrimes, which makes them vulnerable to such crimes.[11] According to a report released by the FBI in January 2006,"the respondents believed many of the incidents did not rise to the level of criminal activity or that reporting them would not lead to a positive outcome.[12]" A review of VeriSign has shown that most of the Australian web users lacked skills and 'knowhow' in protecting their personal information."[13] Due to the fact that, "businesses and consumers are

[8] Ibid., 71(6)
[9] United States Government Accountability Office. 2007. *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*: GAO-07-705, June.< http://www.gao.gov/htext/d07705.html.>
[10] *Cybercrime outranks other crimes on Europeans:* worry list: Almost half of German PC users believe they will eventually fall victim. <http://www.darkreading.com/document.asp?doc_id=156206.> Accessed
[11] N. Kshetri. The *Global Cybercrime Industry. Economical, Institutional and Strategic Perspectives*. USA., 2010, p. 15-16
[12] Ibid., p. 15-16
[13] Countries with the most cybercrime. 2009.

taking some measures in protecting themselves from becoming victims and targets by cyber-criminals, they are getting help and support from government agencies and online security companies."[14] As it is indicated, the consumers and businesses are starting to take some measures against cybercriminals, however the recent experience also reveals that such actions are usually taken after the consumer has been attacked. It could be proposed that higher public general education about the cyber crime activities would lead to enforcement of the effective protective measures would before these malicious acts occur.

2.2.4 Worldwide concern

The legal concern regarding cybercrimes has already reached its high levels. It is not only the concern, but also a huge challenge for every system of law, national or international. As this comparatively new branch of crimes has appeared the worldwide legal and technological methods were not developed efficiently even though it is completely necessary due to the fact that the vast majority of cybercrimes are committed internationally. The area of cybercrimes does not have any abstract physical point. In other words, this type of electronic crimes usually does not accept the principle of land jurisdiction, it has no physical boundaries. This aspect makes cybercrimes even more complex for the investigators and easier for the worldwide online world criminal performers. Legal background in major legal societies such as the USA, the European Union, Russia and Asian countries, has already developed some of the legal measures. Nevertheless, diversity in the legal systems, not equal levels of legal regulation in different

---

<http://images.businessweek.com/ss/09/07/0707_ceo_guide_security/17.htm.> Accessed 1 October 2012.

[14] N. Kshetri. *The Global Cybercrime Industry. Economical, Institutional and Strategic Perspectives.* USA., 2010, p. 16-17

continents provides an easy access to the illegal electronic actions for the cybercriminals to perform. Another major legal problem is that the prosecutors of the national states usually find it to difficult as well as time consuming to start the prosecution process due to the fact that the cybercrime sphere sometimes does not belong to their jurisdiction. There might be several options how a prosecutor could silently reject from starting a prosecution process (due to the limited nature of this thesis they are not going to be specified). In addition to this, the advantage is felt by the cybercriminals, who are and will be committing the crimes with less judicial surveillance to the cybercrimes they will be committing.

2.3 Definitional Issues

During the wide analysis of the academic literature based on cybercrimes, I have observed that the specific or universal definition of a cybercrime does not exist, as it varies in different scholarly sources, just a few were selected by this thesis work to reflect the meaning of the cybercrime. Cybercrime generally is defined as "a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules, or regulations."[15] Additionally might be mentioned, that "examples of cybercrimes include denial-of-service attacks, cyber-theft, cyber-trespass, cyber-obscenity, critical infrastructure attacks, online fraud, online money laundering, criminal uses of Internet communications, ID fraud, use of computers to further traditional crimes, and cyber-extortions."[16] Another scholar, D. Parker proposed a categorization based on the role of a computer during the performance of a crime: "computer as an object of a crime; computer as a subject of a crime; computer as the means for a crime; and computer as a symbol."[17] The last categorization might be easier to understand for the practitioners such as prosecutors, investigators, etc. As it is indicated in this definition, a

[15] N. Kshetri. Positive externality, increasing returns and the rise in cybercrimes. Communications of the ACM, 52(12). 2009.
[16] N. Kshetri.. The simple economics of cybercrimes, *IEEE Security and Privacy*, *4*(1), 33–39
[17] Parker, D. B. *Crime by Computer*. New York: Charles Scribner's Sons, 1976; Parker, D. B. *Fighting Computer Crime*. New York., 1983.

computer itself is categorized in several positions; according to the manner this electronic device is used in. Official acts of EU, cybercrimes define quite general as " criminal acts committed using electronic communications networks and information systems or against such networks and systems."[18]

2.3.1 Classification of cybercrimes

There are many existing classifications of cybercrimes. They can be classified by various criteria. One way to classify cybercrimes is to consider whether they are: "directed against an intended target, in targeted attacks, specific tools are used against specific cyber targets, these attacks are carried out by skilled hackers with expertise to do serious damages."[19] In other sources cybercrimes are also classified into categories based on whether they are predatory or market-based. Predatory cybercrimes can be defined as" illegal acts in the cyberspace in which someone definitely and intentionally takes or inflicts damage on the person or their property, examples of which include stealing money from someone's bank account and intellectual property infringement, hence it could be concluded that these acts do not produce new goods or services."[20] This type of cybercrime is considered to be committed when the bank card is stolen and according to its information illegal acts have been performed.

2.3.2. Trends that facilitate cybercrimes

[18] Communication COM (2007) 267 final. Brussels
[19] N. Kshetri. *The Global Cybercrime Industry. Economical, Institutional and Strategic Perspectives.* USA., 2010, p. 32
[20] Glaser, D. Social deviance. Chicago, IL: Markham 1971. p. 4

Three factors that have had an impact on the growth of malicious electronic acts: "(1) infrastructural susceptibility, (2) increased societal dependence on the Internet, and (3) the increasing availability of information"[21] and also "today's highly interconnected computing infrastructure represents a vast population of machines that is highly susceptible to a digital pathogen."[22]

The computing infrastructure is actually a collection of one type machines[23]: "in essence, a monoculture, hundreds of millions of computers run identical operating systems and applications, implying uniformly similar vulnerabilities, while the homogeneity in the computing infrastructure has brought great benefits to modern society and has been extremely important to the growth of the computing industry, it has also introduced a serious vulnerability."

The growth of Internet use during the last decade has led to an international legal problem: "A number of critical business operations and government functions are nowadays controlled through the internet, including transportation, business supply chain management, government services, business-to-consumer sales, physical infrastructure control, and even healthcare, moreover, internet adoption has revolutionized the business world, however, at a significant price, as virtually each and every one of the business systems have become potential targets for a malicious program attack."[24]

The third aspect indicated is: "the increased and ubiquitous availability of information is greatly facilitated by non-experts to synthesize malicious computer software, hence novice programmers can easily locate and download virus construction "toolkits" and pre-instilled self-mutation logic, enabling them to create computer viruses with polymorphic (self-mutating) capabilities."[25] These three general indicators have shown that committing a cybercrime has become increasingly easy even for non-experts of this sphere. Due to intensive use of internet services, the growth of cybercrimes performed by cyber criminals is believed not be decreasing, but opposite it will systematically search for its maximum, as legal and technical enhancing measures still suffer from regulation inadequacies.

---

[21] Ghosh, S., Turrini, E. 2010. Cybercrimes. A Multidisciplinary Analyzis. Springer., p.47
[22] Ibid., p. 47
[23] Ibid., p. 47
[24] Ibid., p. 47
[25] Ghosh, S., Turrini, E. 2010. Cybercrimes. A Multidisciplinary Analysis. Springer., p.47

2.4 Regulation on Cybercrimes. Comparative perspectives.

2.4.1 Review of the Legal Practices in the United States of America

Legal regulation against the cybercrimes is very important. However, different states and even different continents put different efforts to establish proper legal background for the legal fight against cybercriminals. One of the regulation leaders in the world is the United States of America. In the 1980s, the federal government revised the US criminal code "to address the nation's cybercrime problem, Congress chose to address federal computer-related crimes in a single new statute rather than to add new provisions to existing criminal laws for the first time"[26] [...] "Among the government's most significant milestones in this regard was the Computer Fraud and Abuse Act (CFAA) of 1986, which criminalized unauthorized access to certain computers and computer networks."[27] Moreover, this legal act was amended multiple times in order to reflect the changing background.[28] However, even though the United States of America started the regulation against the cybercrime comparatively early, during following decades the US was still finding legal gaps while regulating suddenly evolving cybercrimes.

[26] Ghosh, S., Turrini, E. 2010. *Cybercrimes. A Multidisciplinary Analysis. Springer.*, p.238 -239
[27] Ibid., p. 239
[28] Ibid., p. 239

2.4.2 Password and Access Device Theft

"The trafficking of passwords and theft of other access devices in computer networks is a rapidly increasing cybercrime threatening the global electronic security system.[29]" As it is indicated "passwords and access device theft can culminate in identity theft and provide criminals unfettered access to computer systems."[30] The USA has provided laws against this criminal activity. Ten separate activities relating to access devices are criminalized in 18 USC 1029.[31] The same legal instrument, specifically § 1030, protects from trafficking in computer passwords, and all other illegal acts regarding fraud and related activity in connection with computers, such as unauthorized accessing of a computer or exceeding of the authorized access.[32] Even though the presented sections of this legal act are not reflecting the new issues of electronic crimes in the sphere of password and access device theft, and it is not a new form of cybercrimes, it should be having a significant impact on the EU serving as an efficient legal example for its legal institutions when arranging proposals to the EU Parliament according to the descriptive and efficient legal imperatives of the US legislation.

[29] Ibid., 239
[30] Ghosh, S., S., Turrini, E. 2010. *Cybercrimes. A Multidisciplinary Anlysis. Springer*., p.274
[31] <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap47-sec1029.pdf> Accessed 12 October 2012
[32] Ibid., § 1030

3 Identity Theft: Background, International legal diversity and Problematic Issues

3.1 Overview

In order to thoroughly discuss electronic identity theft issues in this thesis work, this chapter aims to provide the reader a brief overview and definition of identity together with its systematic classification and allocation issues. However, the central focus of this chapter is to provide necessary and relevant information about the fast growing electronic criminal activity - the theft of identity in the electronic environment. To reflect all the issues that it is necessary to reveal, the reader will first be provided with the definitions of identity, identity theft, the scope of this issue. Then the reader will be presented with the trends, as well as the ways in which this type of criminal theft is performed. Finally, the international, national and regional legislative issues will be indicated in order to reveal the advantages as well as legal gaps that could still be a point for further discussions.

3.2 The Rationale, classifications, definition of Identity

The analysis of the methodological literature helps to reveal personal identity as such, together with existing definitions and classifications of it. The concepts of the personal identity contribute in keeping the correct delimitation from the irrelevant issues. It is recognized that an

exact definition provides a great advantage for every branch of law, as they play important legal role in the proper legal/illegal recognition and qualification processes. They provide accuracy to public relations, authority and judicial institutions. They also ensure the legal stability as well as confidence among the society as precisely developed law branch with its stated definitions, protects from every type of fraud and legal abuse. However, it is not always possible to have legal precision, as this precision could later cause legal controversy and leave major legal gaps. In order to avoid such legal disharmony in the public life concerning personal identity and the issues of its recognition, it is necessary to identify the concerning issues of personal identity such as classification of it, legal recognition, various definitions.

The identity has two main perspectives from which it could be seen and further development of concerning issues could be proceed. All the analyzed authors, such as Summit Ghosh, Sandra K. Hoffman or Tracy G. McGinley, develop the same structure of two perspectives how the identity should be recognized and understood, however the most structured points are declared by T. Nabeth, who divided identity into two main perspectives:

1. A structural perspective*: Identity as a representation*. Identity is seen as a set of attributes characterizing the person. [33]

According to this suggested perspective "it is used to refer to a set of attributes (permanent or temporary) describing the characteristics of the person in the context of practical activities. It also refers to "a set of attributes (permanent or temporary) describing the characteristics of the person in the context of practical activities [..] In the working context these attributes may relate to the competency of a person and the function of the person in the organization (such as the position)."[34] As it is necessary to acknowledge, this perspective is related to the environment in which the individual is connected with social, ethnical, or a religious group for instance, and could easily be identified by its members or the whole group. There is no necessity to have any other additional identification, such as name, personal code, social security code, passport or other legal document that is generally issued by the national

[33] Ibid., p. 26
[34] Thierry Nabeth . *The Future of the Identity in the Information Society.* p. 26

state. The social group can easily identify individual without any additional legal tools. According to this definition, representation is only linked to show or to prove that specific individual belongs to one or another social group, and could be recognized by its members.

2. A process perspective*: Identity for identification*. Identity is considered "according to a set of processes relating to disclosure of information about the person and usage of this information."[35]

The second category is more focused on identity in the perspective of disclosure of the information for identification purposes (Thierry Nabeth) "so as to define the boundaries of peoples' actions". According to this perspective, "identity refers to the elements that can be used to identify the person and to link her to some authorization, for instance, the I.D. card is a good illustration of this." The elements that may be included in this identity include (T. Nabeth) "the name of a person, her position in the organization, photograph, fingerprints, genetic characteristics and even behavioral patterns". In the case of the working context, for instance, this identity (T. Nabeth) "may be used in the identification process to grant a person access to a resource (such as a building or an information system) or give her the right to execute a transaction (such as signing a contract)".[36]

In addition to this, the prevailing opinion is that for the public relations it is necessary to have such personal identity model where legal identification procedure would be determined and approved by the state. Personal data, which links to a specific individual would be provided in the states' registers :"In such legal way, it may be assumed that the information gathered and stored in the registers of the state could be considered as the legal assumption of the personal identity, because it would be revealed according to the procedures based on the legal norms of the national state which would provide the individual specific digital codes and would be straightly connected with the identified person (i.e. personal codes, social security numbers, personal identification codes)."[37] This legal identification procedure has already found its way in a vast majority of the democratic states and is considered to be one of the most proper in a democratic as well as properly secure society. Great Britain, for instance, acknowledges three

---

[35] Thierry Nabeth . *The Future of the Identity in the Information Society.* p. 26
[36] Thierry Nabeth . *The Future of the Identity in the Information Society.* p. 26
[37] Cane P., Conaghan J. *The new Oxford Companion to Law. Oxford University Press Inc.*

different types of identity cards as a legal instrument, and which helps in to identify the subordination of the individuals:[38]

• the identity card for British citizens

• the identification card for European Economic Area citizens living in the UK

• the identity card for foreign nationals[39]

Historically, personal identity has been used to try to uniquely identify persons, and "such identity was meant to refer to somebody without ambiguity."[40] Official identities, which are usually ensured and developed by the national state, and "the corresponding official identity documents could be utilized to create a bank account, to rent a room in a hotel, or to find a job, the uniqueness of the identity also permits the enforcement of the legal rights and duties of each individual (citizen or foreigner, consumer, employee, etc)."[41] Oxford dictionary describes identity as "1) the fact of being who or what a person or thing is [..] 2) serving to establish who the holder, owner, or wearer is by bearing their name and often other details such as a signature or photograph".[42] Throughout the analysis of the scholar literature it was noticed that personal identity has many allocations: *national, regional, profession, personal.* Scholars argue that "such allocations connect individual with some social group (religion, profession, ethnic, cultural), which have the same features as the person, individual who is related to one of these social groups, and according to these features could be easily identified."[43] Identity is also defined as "the specification about the individual."[44] According to one of the most respected researcher's in identity theft area "personal identity basically provides an explanation of the person - wife, pianist, author [..] however, if we are focused not in the specific identity, but also in the privacy and the theft of such identity, then all the legal attention has to be concentrated on the identity which is related with personal data and the protection of it"[45], or in other words, to an

[38] Identity cards. <http://www.findlaw.co.uk/law/government/other_law_and_government_topics/8793.html> Accessed 12 October 2012
[39] Ibid., Identity cards
[40] David-Olivier Jaquet-Chiffelle. The Future of Identity in the Information Society. 2009. Springer. p. 76
[41] Ibid., p. 76
[42] Oxford Dictionaries.<http://oxforddictionaries.com/definition/english/identity> Accessed 10 November 2012
[43] D.Stitilis., P.Pakutinskas. Identity theft in Cyberspace. The aspects of Social, Legal and Electronic Business. Vilnius, 2011 p.18
[44] Sileo J.D. Stolen lives*:* Identity theft prevention made simple. 2005, p. 31
[45] Ibid., p. 31

information regarding the individuals that connects them with states institutions, organizations, or other private or public entities. The United States Electronic Authentication Guideline provides interesting definition of personal identity. It defines personal identity "as individual, unique name of the specific person."[46] However, in comparison to the aforementioned definitions of a personal identity it could be said that last definition from the USA Authentication Guideline does not provide clarity. A description of "unique name of the specific person" does not suffice as the uniqueness of the name does not assure the efficient level of briefness, nor does it assure that the individual will be always recognized without any fail. In comparison with the definitions provided by afore mentioned authors (T. Nabeth, D. Olivier, D. Stitilis), where the definition of identity is arranged in structured, briefly indicating points, which actually leaves no variations regarding the recognition process. Also, the specific features of the individual make them recognizable to the social group to which they might belong.

Hence, even though the construction of the identity definition might vary, the basis of it remains the same in most of proposals presented by the scholars and could thus be described as the existence of the specific features about the specific person as well as legal, official facts that systematically represent and recognize one or another individual.

It is possible to distinguish various types of identities, as for instance: professional identity, legal identity, social identity, electronic identity. The specific circumstances determine, which personal identity appears and applies in that specific environment. In this thesis work, we are mostly interested in the electronic identity.

"With the appearance of the internet, the security level of personal identity has decreased, due to the risk of cybercriminals and their illegal activities."[47] Electronic identity is basically a novelty compared to other types of identities, it is still developing and evolving sub-identity of personal identity. According to scholars, "the concept of the virtual or electronic identity has been raised in order to better describe and understand new forms of identities in the information

[46] Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology. NIST special publication 800-63 Version 1.0.2, 16p.
<http://www.usda.gov/egov/egov_redesign/intranet/eauth/SP800-63V6.pdf>. Accessed 15 September 2012
[47]" The history of Identity Theft"<http://www.spamlaws.com/id-theft-history.html> Accessed 9 November 2012

society, in relation to rights, duties, obligations, and responsibilities coming from it."[48] Official identity, which is issued by the state and recognized by its legally verified methods and "the corresponding official identity documents could then be exploited to create a bank account, to rent a room in a hotel, or to find a job [..] its uniqueness also permits the enforcement of the legal rights and duties of each individual (citizen or foreigner, consumer, employee, etc."[49] It is recognized that "sometimes facing persons in the online world that, while having an identity, are not real persons, but artificial (intelligent) agents moving avatars in video games, and expert systems administering forums or dealing on the stock exchange."[50] As it can be seen, virtual or electronic identity is a complex electronic novelty, as it serves as a tool to describe a real person in the electronic environment. Artificial e-commerce agents, for instance, might be considered as artificial instruments of a physical identity of the offline world, which perform for simple commercial practices instead of the real persons. The analysis of concerning issues reveals that the importance of this type of identity has no legal doubts, however in order to have this electronic identity functioning properly and safely, it is necessary to ensure legal standards, of the legal protection.

Before further discussing the electronic identity theft and its legal issues, it is necessary to familiarize the reader with the identification process in the online world, as the vast majority of the electronic crimes regarding the electronic identity theft is performed due to the negligence, the lack of information of how to use the issued secret information properly and other negligent ways, which will be discussed under this section of the thesis. This section reveals the major legal and technical mistakes concerning the identification process. This section will mostly pay its attention to the acts performed in the online world

. ***Offline world***: The identification process in offline world is not as complex as it is considered to be in cyberspace.[51] An individual person may be identified using such legal measure as passport, which is issued by the national state, and provides the insurance that specific person pictured in the passport will be identified in real time and space, however it is

[48] David-Olivier, J. Chiffelle, E. Benoist, R. Haenni,F. Wenger, H.Zwingelberg. The Future of Identity in the Information Society. Challenges and Opportunities. 2009 p. 92-95
[49] Ibid., p. 76
[50] Ibid., p. 77
[51] Cyberspace require individual's identification even for the least important procedure, that is because every time a specific person must be identifies and confirmed by the electronic system, which the individual is using.

necessary to indicate, that official documents can also be fabricated by the criminals. Moreover, such identification process "where legally issued individual document is used to identify a specific individual is usually named - official identification."[52] As a comparison with most of European identification systems, United States are facing a large amount of identity theft for the reason that there is a very flexible identification system, allowing the usage a variety of identifying personal documents. Hence, the identification process is basically very similar in the offline world as it essential to provide a legally issued personal document, assure that such document is not fraudulent.

Electronic Environment : Identification process in electronic environment has become essential. This is in part due to the heavy use of cyberspace including increased commercial transactions, voting, and use of social networks. There is a notice in academic literature, that identification in cyberspace is several times higher in the level of risk in comparison offline world. Due to that, it is logical observation that more identity theft occurs in cyberspace, compared to real time and space offline world.[53]

The online world is also more specific comparing to offline world due to the reason that identification process does not require the person to be present, as online world provides an opportunity to perform a wide variety of actions through great distance and time. These actions might include "data transaction, data saving, and use of the data, with the help of the technical measures, usually with the help of computers".[54] Moreover identification process in the electronic environment is considered to be more complex comparing to real space, as electronic environment usually has many intermediaries which make the identification even more complex, and it is facing with the mechanism of the identification of the specific person, as well as with the rights of consumers and data protection, privacy protection.[55] The electronic environment sphere where it is required to identify the individual differs: electronic commercial services, administrative services and etc, in addition to this the methods of identification also vary, "An individual might be recognized and identified using the electronic signature, the address of the

---

[52] Ibid., p. 20
[53] Higgins H.E. 2010. *Cybercrime: An Introduction to an Emerging Phenomena. McGraw-Hill,* p. 74
[54] D. Stitilis,P. Pakutinskas,M. Laurinaitis,I. Dauparaite. *Identity theft in Cyberspace. The aspects of Social, Legal and Electronic Business. Vilnius, 2011 p. 23*
[55] D. Stitilis,P. Pakutinskas,M. Laurinaitis,I. Dauparaite. *Identity theft in Cyberspace. The aspects of Social, Legal and Electronic Business. Vilnius, 2011 p.* 22

computer IP, wireless station address, domain name, etc". [56] The definition and classification, as well as the structure of identity definition remain very important in understanding the relevant issues of the identity theft in online world, as legal analysis in this chapter reveals, that the approaches regarding this definition still differ. In order to have a perfect legal background for national, regional, international legal regulation of cybercrime area and its specific crime identity theft, it is necessary to establish one main theoretical approach for identity, which would reflect all the necessary legal aspects and points, that are relevant and necessary to reach efficient legislative aims and legal harmony in this area.

3.3 Identity Theft

3.3.1 Important comparative statistics of Identity theft

It would suffice to start a presentation of identity theft with a simple survey conducted in the United States of America: "Identity theft is the fastest-growing worldwide financial crime, the United States is considered to a leader in this area: several years ago CBS News reported that someone's identity is stolen every 79 seconds, what is more, the Federal Trade Commission (FTC) survey in 2006 found that 8.3 million American adults were victims of identity theft, that same study estimated the total identity theft losses to be $15.6 billion."[57] Whatever are the exact losses, the growth of identity theft has been tremendous. Kiplinger's Personal Finance magazine in its July 1995 edition reported, that "the credit reporting bureau Experian received 600 to 700 identity theft complaints each day, additionally, MasterCard International reported that identity theft represented 96 percent of member banks fraud losses in 1997, identity theft losses grew from 450 million in 1996 to over 2 billion in year 1999."[58] As it is indicated, "the identity theft has become one of the most beneficial crimes, for cybercriminals to commit, among the other

[56] IP (Internet Protocol) - computer identification in the network, a unique number that is used to identified the sender and receiver of the data flow.
[57] Martin T. Biegelman.2009. *Identity Theft Handbook*. Detection, Prevention, and Security. p. 1
[58] Ibid., p. 1

crimes."[59] These simple statistics and public information reveal an outstanding damage being made to the international environment, ranging from economic aspects to humanity issues and human rights, ensured by the European Convention on Human Rights Article 8 declaring: " Everyone has the right to respect for his private and family life, his home and his correspondence."[60] This type of electronic crime has major negative aspects. The reason for that is the breach of one of the basic constitutional rights - the Right of Privacy, together with a huge economic and social damage for the individuals and institutions, both private and public ones.

3.3.2 Factors and Trends

The usage of electronic environment together with the internet has grown rapidly during the past decades. First of all, it is necessary to mention that many economic subjects have fully or at least partly moved their economic activities into the electronic environment, as "electronic services have become truly related and complex system together with internet." According to the recent survey in Lithuania, during the years 2009-2010, the consumer usage of the electronic services has almost doubled and, compared to earlier periods, is up 69percent. [61] The numbers of electronic services users are rising enormously. As a result, it can be concluded that unless the efficient legal protective measures are implemented in the near future, the identity theft as illegal activity will increase even more, due to number of users of services that are provided through the electronic environment and the number of cybercriminals acting in this sphere. Organization for Economic Cooperation and Development has indicated the importance of electronic transactions performed via internet for the public and commerce, however this organization has also raised the concern about the drawbacks that will predictably appear very soon due to the growing number of electronic services users, as the economic relations in the electronic environment are performed without knowing each other in a physical space, making the possibility of fraudulent acts is highly predicted.[62] It is basically clear that a vast majority of researchers of this criminal

[59] Higgins G.E., 2010. *Cybercrime: An Introduction to an Emerging Phenomenoma*. McGraw-Hill, p. 67
[60] European Convention on Human Rights. Article 8
[61] Usage of the Internet in Lithuania. <http://www.lrytas.lt/-13281748951328122396-internetu-naudojasi-69-proc-lietuvos-gyventoj%C5%B3.htm>
[62] Online Identity Theft. OECD. 2009. <http://www.oecd.org/internet/consumerpolicy/oecdguidelinesforprotectingconsumersfromfraudulentanddeceptivecommercialpracticesacrossborders2003.htm >. Accessed 6 October 2012

area agree that "the usage of electronic identity stimulates the amount of identity thefts performed in electronic environment."[63] This aspect has also been repeated by the Digital Agenda of Europe 2010 claiming that in relation to the high usage of the internet services the amount of the identity theft's has increased.[64]

3.3.3 What is Identity theft?

The study of academic resources indicates a variety of opinions of how identity theft should be described, as the definition is not only highly important for academic research, but also provides a huge benefit for legal practices as well as the legislative process, which is the main legal measure in the fight against cybercrime.

The process of identity theft is recognized when :"criminals acquire key pieces of personal identifying information- such as name, address, date of birth, mother's maiden name, employment information, credit information, and other vital facts in order to impersonate and defraud the victim, this stolen information enables the thief to commit numerous forms of fraud, including taking over the victim's financial accounts: applying for loans, credit cards, and Social Security benefits, purchasing homes and cars and establishing services with utility and phone companies for instance."[65] Other resources repeatedly indicate almost the same situation: "Identity theft occurs when a criminal steals key pieces of personal identifying information to gain access to a person's financial accounts."[66] In comparison to this, the United States Secret

[63] Rannenberg K., Royer D., Deuker A.,2009. *The Future of Identity in the Information Society*. Springer-Verlag, p. 316
[64] Digital Agenda of Europe. 2010
[65] Ibid., p. 1-4
[66] United States Postal Inspection Service, Publication 280.
< http://about.usps.com/publications/pub280.pdf.> Accessed 2 October 2012

Service defines identity crimes as ‘‘the misuse of personal or financial identifiers in order to gain something of value and/or facilitate other criminal activity."[67]

An interesting summary of many scholar resources and opinions is provided by the US President’s Identity Theft Task Force Report issued in April 2007. It declares: "although identity theft is defined in many different ways, it is, fundamentally, the misuse of another individual’s personal information to commit fraud, as this report goes on further: ‘‘Criminals must first gather personal information, either through low-tech methods- such as stealing mail or workplace records, or through complex and high-tech frauds, such as hacking and the use of malicious computer codes."[68]

All these definitions firstly indicates the necessity to acquire the information legally or illegally, the method is not so important, because the purpose in such cybercrimes is still illegal- to gain the benefits from person, who owns the personal information related to his finance or medical status, for instance. The impersonation process is the part of the crime as it provides the ability for the fraudster to pretend to a specific person and commit his illegal intellectual and physical actions. Usually the final step is, "when financial accounts have been taken over, the identity theft crime is considered to be finished completely, for instance, the acquired information was used to apply for a loan, purchased a car, a house ant etc."[69] Without a specific legal regulation and technical enhancing measures it is very easy for criminals to obtain our personal information and our identities.

Consequences. Victim will be already suffering from this dangerous crime even though the cybercrime will be revealed shortly, they will be forced to go into the process of the litigation, provide evidence to the courts and other institutions in order to prove that the acts were not performed by the victim:" many variables determine the effect that identity theft has upon victim: financial, social, medical, psychological, and familial costs may be associated with victimization, upon discovery of the crime, victims are forced to confront and resolve the

---

[67] United States Secret Service, Financial Crimes,
< www.ustreas.gov/usss/criminal> Accessed 9 October 2012
[68] President’s Identity Theft Task Force. Combating Identity Theft*: A Strategic Plan*,
< http://www.fraudaid.com/how-to-deal-with-having-been-conned/fraud_report/jurisdictions/federal/Secret_Service.htm.> Accessed 9 October 2012.
[69] Ibid

problems surrounding the theft of their identities, they must act quickly to stop the victimization, to clear their names of fraudulent activities and to reduce the risks of being victimized again."[70]

Hence, this type of cybercrime if one of the most malicious and dangerous, because once the victim has suffered, the usage of electronic commerce, or electronic services in the future will be obviously reduced, due to the lack of trust of these services. This type of crimes leaves an impression for the users that no electronic service or commerce is be reliable and, what is more, the following t electronic purchases or commercial services will probably be replaced by the physical performance in order to reduce the risk to the minimum. In accordance to this, with every identity theft, the enormous drawbacks occur not only for the specific individual, but also for the whole worldwide electronically based economy, as well as efforts dedicated to easy and less expensive electronic services. The importance of stopping these types of cybercrimes is vital.

3.3.4 Classification of Identity theft

The methodological classification of identity theft might indicate the problematic issues more easily. Classification provided by the scholars:

1. *Personal Identity theft*. " Personal identity theft is the use of an individual's personal identifying information[71] without his or her knowledge and with the intent to aid or abet in any unlawful activity such as the fraudulent obtaining of services, merchandise, money, and/or credit, it also occurs when an individual's identifying information is used to file for bankruptcy."[72]

The most severe form of identity theft is" a complete identity take over: this occurs when a key piece of personal identifying information is stolen and used by a thief to take control of every

[70] Sandra K. Hoffman., Tracy G. McGinley. *Identity Theft. A Reference Handbook.* 2010. p. 41
[71] Personal identifying information such as person's name, passport number, biometric data and etc
[72] Sandra K. Hoffman., Tracy G. McGinley. *Identity Theft. A Reference Handbook.*, p. 1 ,2

aspect of the victim's life, hence a complete identity take over usually begins with a stolen SSN or mother's maiden name, either piece of personal information can be used to obtain a breeder document, a government-issued identification record that leads to the issuance of additional identification documents."[73] As "social Security numbers are another key piece of personal identifying information, each number is unique and permanently assigned to one individual, a stolen SSN can facilitate a complete identity take over in the same manner as a stolen mother's maiden name, unfortunately, victims have very few options if their numbers are stolen and used to commit fraud and/or other crimes, they may request a new number, however, the process for securing a new number requires an extensive amount of time and paperwork."[74]

2. Business Identity theft. Thieves also steal the identities of businesses: "the term businesses refers to small companies, corporations, financial institutions, healthcare related organizations, and government entities, business identity theft involves the use of a business identifier without permission and with the intent to aid or abet in any unlawful activity such as fraudulently obtaining services, merchandise, money, and/or credit, this also occurs when business-identifying information is used to file for bankruptcy."[75] In some cases, the identifying information of businesses is stolen in order "to gain access to the company's financial accounts, business checking accounts are often targeted by identity thieves, for example, criminals may steal a business check and duplicate it electronically, the checks are often cashed or used to make purchases without being detected because they bear a legitimate account number or business name, hence the business owner may not find out about the fraud until they balance the accounts, verify the account activities online, or receive notification that the account is overdrawn."[76]

Therefore, identity theft is a malicious threat which encompasses not only single individuals, but also the entities of business structure. Nowadays, personal or identifying information is at a high risk of theft at any moment, as it later can be used for "fraudulent obtaining of services, merchandise, money, and/or credit"[77]. These reviews of the possible victims of identity theft indicate the high risk of possible threats that might be committed by the criminals. Stronger legal

[73]Sandra K. Hoffman., Tracy G. Mcginley. *Identity Theft. A Reference Handbook*. 2010, p. 2,3
[74] Ibid., p. 2
[75] Sandra K. Hoffman., Tracy G. McGinley. *Identity Theft. A Reference Handbook*., p. 3,4
[76] Ibid., p. 3
[77] Ibid., p. 1 ,2

attention on this crime area is also expected due to the vulnerability of rights of privacy, together with a conclusion, that the defense against such type of crimes is much more difficult comparing to other type and forms of theft crimes. These aspects require specifically orientated legal attention, as well as efficient technological and legal measures to be implemented into the national public laws.

3.3.5 The Way of Committing Electronic Identity Theft

Identity theft in electronic environment is a dangerous, structurally developed illegal act, performed by the cybercriminal, who has the aim to acquire personal electronic information, which is issued by a financial institution, an administrative institution, social network page and etc. Usually it has a further incentive to use the acquired information for committing other crimes or to distribute stolen information. As the classification of the identity has been previously discussed above in this thesis work, the classifications of identification or allocations of this process will not be analyzed in this chapter. The identity theft in the offline world will be also considered an irrelevant issue in this thesis chapter.

In addition to this, it is necessary to establish the clear view of what are the illegal ways of collecting personal information. Due to rapid growth of internet use, and fast developing software, which makes the way even easier illegally gather personal information. It is becoming enormously hard to stop the process of electronic identity theft. In order to develop significant technological and legal measures against these types of electronic crimes it is necessary to indicate, what are the most popular ways to gather the private electronic information. It is also important to indicate, that often people "selling stolen information online and do not personally

steal that information but rather purchased it from another thief."[78] Buying stolen information from the cybercriminals is believed by the fraudsters to be more secure, also it is does not require to commit primary criminal acts yourself, and these aspects usually are the stimulation to purchase the stolen electronic information from the cyber criminals.

It is indicated that identity theft is usually performed, "while the user is in the process of the electronic authentication, due to the fact, that in order to get the access to the electronic information system, the users have to provide identifying information."[79]

Basically, almost all the reviewed scholar resources provide the same classification of performing the electronic identity theft, the most famous ways of committing the identity theft is presented:[80]

1. *Phishing*. "This well-known tactic typically involves setting up a fraudulent Web site designed to look like the legitimate Web site of a bank or other financial institution, and then spamming out e-mails that appear to be sent from that legitimate institution."[81]

2. *Network Intrusion*. "Another common method of stealing financial information involves directly breaking into the network of a retailer or other possessor of such information."[82]

3. *Trojan Horses*. "One of the most sophisticated types of malicious code is a “key logging Trojan horse”, this program automatically installs itself on the victim’s computer and remains dormant until the victim visits one of a predetermined strings of Web site URLs (for example, a banking Web site), the key logger then “activates” and stores the first few dozen or so keystrokes entered by the victim (a string that will include his or her login and password) and then sends it back to the attacker (typically via an IRC channel)."[83]

4. *“Real-World” Theft.* This type of identity theft, related with a real world, is exceptionally presented here, due to the connection of the whole reviewed context. "This is still the most

[78] Cyber Fraud: Tactics, Techniques and Procedures. Florida. 2009. p 27
[79] D. Stitilis,P. Pakutinskas. *Identity theft in Cyberspace. The Aspects of Social, Legal and Electronic Business. Vilnius*, 2011 p. 120
[80] D. Royer, FIDIS Network, deliverable 5.2b,, ID- related crime: towards a common ground for interdisciplinary research. <http://www.fidis.net/resources/deliverables/forensic-implications/int-d52b000/doc/29/>. accessed 5 October 2012
[81] Ibid., *p. 27*
[82] Ibid., p. 27
[83] Ibid., p. 27

popular means of stealing financial information: it includes such tactics as installing “skimmers” on ATM machines that record information from cards inserted in the machine and waiters at restaurants stealing the information from credit cards used to pay for meals, often, the thief does not directly exploit such information but instead sells it online in batches of dozens, hundreds, or even thousands of compromised accounts."[84]

5. *Spoofing of biometric sensors. "*The identification process is performed without the individual who has the legitimate right to act so in accordance to such biometric measures. First the information is gathered from the individual, for instance, the photography and it is illegally used later."[85]

6. *Pharming.* "Pharming attacks are similar to phishing attacks in that they are designed to extract confidential data from victims by pretending to be a trusted source and requesting information, the difference between pharming and phishing is that pharming attacks resolve the victim’s DNS to a malicious server when attempting to visit a legitimate Web site, as opposed to a phishing attack, which requires that victims be tricked by social engineering into visiting the fraudulent Web site."[86]

It would be dangerous to state, that one or two of aforesaid methods of acquiring personal electronic information are dangerous, systematically all of them are negatively affective and damaging.

Furthermore, in order to prevent identity theft in electronic environment, and stop these mentioned illegal acts, as a malicious, it is necessary to establish specific legal regulation on these issues, providing legal dispositions in the legal norms, specifically establishing the complex of actions which should be considered as an electronic crime, and how would it be recognized, evaluated and qualified through the dispositions of the legal norms. However, due to the novelty of these type of acts, and the fast changing public national and international relations, the vast majority of the new developing democratic countries, such as Lithuania, has not been able to pay adequate amount of legal attention on these legal issues, neither it corresponded to

[84] Cyber Fraud: Tactics, Techniques and Procedures. Florida. 2009. p 46
[85] D. Royer , FIDIS Network, deliverable 5.2b,, ID- related crime: towards a common ground for interdisciplinary research. <http://www.fidis.net/resources/deliverables/forensic-implications/int-d52b000/doc/29/>. accessed 5 October 2012
[86] Cyber Fraud: Tactics, Techniques and Procedures. Florida. 2009. p 47

these criminal acts, nor established proper legal criminal response against fast evolving cybercrime sphere. Before reviewing the Lithuania's legal penal background regarding cybercrime area, first of all it is necessary to indicate, what regional and international legal measures and tools have been already adopted and are expected to be properly ensuring the security in this criminal area. According to what types of legal instruments it is possible to find and what is the scope of them, they could be divided into two groups:[87] "a) legal documents, which has only recommendation value, b) legal documents, which are binding." The Lithuanian criminal law system, regarding cybercrimes and especially identity theft is considered to be inadequate to ensure legal protection in this cybercrime area. The lack of legal attention to the cybercrime area in the CC, and the penal regulation regarding the threats performed via computer systems or with the help of the computers, has made the Lithuania's legal system to be insufficient to react to the new emerged crimes, discussed above. The current penal regulation extensively will be declared in the chapter four.

3.4 Legal Response

United States. The efforts to stimulate the criminal legislation was widely recognized even before the year 2000, the worldwide leader and greatest sufferer from these types of crimes was the US, due to that it has provided huge legislative efforts to fight against this cybercrime as early as 1998. Much of the legislation that has been enacted in United States, for instance, regarding identity theft focuses on large-scale governmental and corporate responsibility to protect citizens and consumers.[88]

Identity Theft and Assumption Deterrence Act of 1998 . "The enactment of the Identity Theft and Assumption Deterrence Act of 1998 made identity theft a felony, the Act amended and enhanced existing federal criminal code, the 1998 Act made it a federal crime for a person to knowingly

[87] D. Stitilis,P. Pakutinskas. Identity theft in Cyberspace. The Aspects of Social, Legal and Electronic Business. Vilnius, 2011 p. 120

[88] Sandra K. Hoffman., Tracy G. Mcginley 2010, *Identity Theft. A Reference Handbook*. p. 64

transfer or use the personal identifying information of another with the intent to commit a crime or to aid in the commission of other crime."[89]

Identity Theft Penalty Enhancement Act. 2004. The Act created the offense of "aggravated identity theft" and introduced mandatory sentences for the crime: Aggravated identity theft is defined as the unlawful transfer, possession, or use of another person's identifying information related to the commission of specific felonies, a conviction for wire, bank, or mail fraud, for example, involving stolen personal information results in two sentences (i.e., one for the fraud conviction and an additional mandatory two-year sentence for aggravated identity theft).[90]

International legal documents*: Convention on Electronic Crimes*- is one of such legal international tool, which ensures adequate legal protection in the area of cybercrimes. According to the scholar literature, this international instrument is considered to be one of the most successive international legal measures in the war against cybercrimes, as well as against identity thefts in electronic environment, using computer as an instrument to perform these acts.[91] This convention is signed by 30 different states, but it is ratified only by 17 of them. The act has been in force since 2004, but it could be easily noticed, that perfect results using this legal tool will be not achieved one hundred percent, further more this legal tool could be very important, however it should not be the only one.[92] As it is necessary to pay legal attention, that the first section (Article 2 to Article 6) of this Convention provides the material legal imperatives which is binding for the parties. This section ensure, that necessary legislative and other measures would be adopted in the national level, as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.[93] Other sections of this main legal regional instrument are also relevant, they indicate, what kind of illegal electronic offences should be criminalized and what legal measures should be adopted by the national states in the fight against them. The act focuses on

[89] Theft and Assumption Deterrence Act. 1998
[90] Identity Theft Penalty Enhancement Act. 2004
[91] D. Stitilis,P. Pakutinskas. Identity theft in Cyberspace. The Aspects of Social, Legal and Electronic Business. Vilnius, 2011 p. 120
[92] Brenner, S.W. 2010. Cybercrime. Criminal Threats from Cyberspace. Library of Congress Cataloging, p. 209 is stitilis
[93] Convention on Cybercrime. 2001. Budapest. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> accessed 10 October 2012

such areas as: detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation.[94]

It has to be mentioned, that comparing to other geographic regions, such as United States, European Union, has started to focus its criminal sight in these criminal offences comparatively late. Due to this reason, there are not so many enforced and adopted legal measures, except afore mentioned Convention on Cybercrimes. However, during the research, it is able to indicate a few existing legal proposals to the European Parliament in the fight of electronic crimes, also involving Identity theft in electronic environment.

31 May 2006. *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions.*

This Communication announced, that the Commission is inviting interested parties to take the initiative, catalyzing such goods as open dialogues, partnership, empowerment as these goods are the main tools in order to prevent the personal identification data theft, or other illegal electronic offences which highly damage the constitutional right - the right to human privacy. According to this Communication, "this partnership would build on mutual interests, identify respective roles and develop a dynamic framework to promote effective public policy-making and private sector initiatives."[95]

26 August 2012. *Communication from the Commission to the Council and the European Parliament, and Social Committee and the committee of the Regions. A Digital Agenda for Europe.*

This proposal form communication indicate the main aim of the Digital Agenda, which is to deliver sustainable economic and social benefits from a digital single market

[94] Ibid., Preamble of the Convention.

[95] 31 May 2006. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. COM(2006) 251 final. <http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf> accessed 10 October 2012

based on fast and ultra fast internet and interoperable applications.[96] As well as the main objective of this electronic legal measure: "Agenda is to chart a course to maximize the social and economic potential of ICT, most notably the internet, a vital medium of economic and societal activity: for doing business, working, playing, communicating and expressing freely.[97] What is more, the Commission has identified the seven most significant weaknesses, where the attention has to be focused with a priority.[98]

It is stressed that due to the high growth of this new type of criminality- digital criminality, which is related with cyber attacks and mostly with identity thefts on electronic environment, and what is more, due to that in order to start solving these issues, the new legal mechanism has to be provided.[99]

28 March 2012. *Communication from the Commission to the Council and the European Parliament. Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre.*

The concern in this communication is focused on the revolution of digital environment. As it is indicated, that no crime is as borderless as cybercrime, requiring law enforcement authorities to adopt a coordinated and collaborative approach across national borders, together with public and private stakeholders alike, and in addition to this tt is here that the EU which is able and does, add significant value.[100]

This Communication indicates the EU initiatives to tackle cybercrimes, as well as identity theft with the establishment of a new institution for the fight against cybercrimes - European Cybercrime centre. It is stressed in the communication that one of many functions of this centre would be providing support to Member States for cybercrime investigations. Among the other many functions this would definitely help to make the investigation and prosecution process easier and approachable. To have the short review of this communication done, it is

---

[96] 28 March 2012. Communication from the Commission to the Council and the European Parliament, and Social Committee and the committee of the Regions. A Digital Agenda for Europe. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> accessed 10 October 2012

[97] Ibid., p. 3

[98] Ibid., p 5- 7

[99] 28 March 2012. Communication from the Commission to the Council and the European Parliament, and Social Committee and the committee of the Regions. A Digital Agenda for Europe. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> accessed 10 October 2012

[100] 28 March 2012. Communication from the Commission to the Council and the European Parliament. Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. <http://ec.europa.eu/home-affairs/doc_centre/crime/docs/Communication%20-%20European%20Cybercrime%20Centre.pdf#zoom=100> accessed 10 October 2012

necessary to mention, that this proposal has a reasonable value, as in the near future all the EU member states would have the central institution, which would collaborate in revealing cybercrimes and, especially, rapidly evolving crime such as electronic identity theft. As directly, there has been not mentioned about the fight against electronic identity theft, however, it could be noticed that all the legal efforts of this institution would also help to reveal this type of crime.

22 May 2007. *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cyber crime.*

This Communication might be evaluated as the strategic legal proposal for the fight of cybercrimes, including electronic identity theft. In the section 1.2.2 it is declared that: "most crimes can be committed with the use of electronic networks, and different types of fraud and attempted fraud are particularly common and growing forms of crime on electronic networks, instruments such as *identity theft*, phishing2, spam and malicious codes may be used to commit large scale fraud."[101] It is highly important to notice, that this section indicates the identity theft (among the other electronic crimes) as an instrument to perform other fraudulent acts. What is more, the section 3.3 of this document declares that: "A particular issue which may require legislation relates to a situation where cyber crime is committed in conjunction with identity theft".[102] As it is indicated, "in most of Member States, a criminal would most likely be prosecuted for the fraud, or another potential crime, rather than for the identity theft; the former being considered a more serious crime [..] Identity theft as such is not criminalized across all Member States."[103] This 3.3 section of Communication reveals the dispute, whether identity theft itself is a dangerous performance and comes with a suggestion, basically not to focus on national penal law legislations to criminalize this type of electronic crime, adding that the vast majority of EU member have not done that yet. However, the vast majority, does not mean absolute ruling, and other EU legislative proposals, as well as scholars stands with a different approach.

---

[101] 22 May 2007. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cyber crime. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF> accessed 17 October 2012

[102] Ibid., section 3.3 (p. 7)

[103] Ibid., section 3.3 (p. 7)

It should be highlighted, until these legal proposals and initiatives, the personal data and protection of privacy issues were only protected by data protection Directive (95/46/EC)[104] and telecommunications Directive (97/66/EC)[105]. The data protection Directive was considered to be more general legal instrument, that protects personal data, which encompass various spheres of data. However, neither Directive 97/66/EC nor Directive (95/46/EC) was helpful against the fight with the new innovative cybercrime area, such as identity theft, as its sphere is to regulate the specific data area's regarding the telecommunication sector. Only the Council Framework Decision 2005/222/JHA has started to focus EU legal penal attention to the frauds and electronic threats committed via information systems, together with fraud and counterfeiting of non- cash means of payment.[106] And it might be considered that this legal decision is one of the first significant regional legal measure against the cybercrime in EU jurisdiction.

To sum up, what has been reviewed and revealed, it might be stressed that EU has already provided legal efforts for the productive fight of cybercrime, with the issue of specific legal proposals, decisions, which will contribute in the fight against cybercrimes and electronic identity theft. The only international instrument that is already enforced and has a judicial power for its signed parties is only the Convention on Cybercrimes, in addition to this the number of proposals from the EU Commission has been published in order the strategic issues against cybercrimes could be seen and evaluated systematically. It has already given its legal fruits in the EU, as the position on the necessity to establish stricter laws regarding cybercrime area has been indicated in all aforementioned initiatives, especially in EU Communication COM (2007) 267final, where the specific cybercrime sphere's such as identity theft is concerned as malicious and has a significant role in committing further computer-related crimes or other type of crimes. These initiatives also indicate that " approximation of penal laws is necessary for establishing common minimum levels of protection in the EU [..] as it also concerns the procedural law aspects of fighting the cyber crime- fighting [..], practical co-operation at international level,

[104] EU Directive 95/46/EC
[105] EU Directive 97/66/EC
[106] Council Framework Decision 2005/222/JHA., 2005. Articles 2-6; 7-8

jurisdiction in procedural issues."[107] According to what has been discussed, I would like to stress, that expanding the scope of conventions, such as the Convention on Cybercrime is not necessary. In order to achieve legal goals established in the Communications and other EU initiatives it is rather better for EU to concentrate on the penal legislation directions for the EU member states, even more, these directions has to be specific and well orientated, according to the cyber criminal reality and reflect all the necessary legal defense against these type of crimes. The international legal instruments such as Convention on Cybercrimes is of course very much important and relevant, however usually establishing only general provisions in these type of legal acts are not sufficient enough to have a successful combat against cybercrimes, moreover the signatory parties are usually deciding themselves what specific legal regulation will be implemented into the national laws, and they vary from state to state. Moreover, only these discussed initiatives, as such, are not sufficient enough to absorb all types of cybercrimes, including electronic identity theft, which is becoming more and more popular among the cyber criminals, neither they are legally influencing member states, before these initiatives become mandatory directives and regulations . Hence, legal situation, regarding this sphere in EU right now shows its drawbacks, as the regional regulation inadequacies reveals major legal problems. Compared to the United States, EU is still quite far away from the sufficient regional regulation which could provide the guarantees of safe use and development of electronic market in the cyberspace, however recently provided legal efforts in regulating such malicious threats is believed will be implemented in the near future.

[107] Erik Wennerstrom. EU Legislation and Cybercrime. A Decade of European Legal Developments. Stockholm. 2010., p. 10

4 Electronic Identity Theft and Penal Laws in Lithuania

4. 1 Overview

This chapter aims to indicate the specific penal law gaps, that are specifically connected with cybercrime area in the Republic of Lithuania. It will lead the reader to the public penal law system of this State, declaring the drawbacks that can, and usually do occur, when the absence of specific legal penal laws are missing in the system. It will be declared, what are the main reasons that do not let the state to legislate the necessary legal provisions in its Criminal Code (CC) in order to contribute in helping stop one of the most dangerous forms of electronic crimes. The specific section, which provides the penal issues in the CC of Lithuania, will also be reviewed, revealing what norms have already served in solving other types of electronic crimes. In addition to this, the reader will also have the ability to notice the necessity of legal provision to be incorporated into this national legal penal instrument, in order to contribute in the fight against the growing specific electronic threat. Moreover, at the end of this chapter some of the legal alterations will be proposed in order to change current legal situation.

4.2 Specific Penal Laws for the fight against Identity Theft

4.2.1 The Criminalization of the Identity Theft

Through the review of public penal laws in Lithuania it is clearly seen that there are basically limited specific criminal regulation, defining cybercrimes as illegal activities. The only national legal penal document is the Criminal Code of the Republic of Lithuania (CC). As democratic penal legislative initiatives started only after Lithuania got its independence in the 1990s, the legal gaps were always felt. Through the amendments of CC made in the year 2000, there have been important changes implemented in it. The section for cybercime in the Criminal Code is comparatively small comparing to the basis of the criminal laws in other democratic countries, especially in the United States, where the fight against the electronic identity theft is criminalized by various penal acts. However, Lithuania's first initiatives to criminalize computer related frauds were in the year 1994. The section of CC which is linked to the crimes performed in electronic environment or with the help of computer consists of only 5 articles, these articles will be discussed in further sections of this chapter. The disadvantage of absence of the amount of the specific legal formulations or dispositions, which would describe specifically the illegal electronic activity, in this case identity theft, has already led legal institutions for the problematic criminalization of the investigated acts. Moreover, in order to criminalize the identity theft, a prosecutor has to apply penal norms that are not established in the section for cybercrime, it suppose the situation when Article 166 of the CC must be applied, which protects the privacy of the use of communication networks and establish the liability for illegal use of personal information.[108] However this general Article is not specific enough to encompass all the action regarding identity theft.

[108] Criminal Code Of Lithuania. Article 166

4.2.2 Legal concern in State of Lithuania

The Constitution of Lithuania, at Article 22, indicates general imperative for the national legislators to provide such legal penal imperatives, which would ensure the stability for the constitutional right of the independence of human privacy.[109] Scholars provide the opinion, that the national legislator always has a duty to take all the necessary legal measures, and legislate the needed public laws, hence, the public criminal law is not the exception. What is more, it is marked, that the national legislator is only able to criminalize (legislate penal imperatives) such illegal activities which are known for the general public and law experts at that specific period of time, and are considered to be doing serious harm for the goods protected in the main act of the state- Constitution of Lithuania[110] This is not a legal factor, which stops the further development of public laws, however, with the contribution of the public relations, law experts and practitioners, where is always a legal possibility to legislate and propose such penal imperatives, which would absorb more illegal electronic acts. However, the pure generalization might and usually cause the dysfunction, or inappropriate level of legal regulation against some specific illegal acts. This situation currently appear in the Criminal Code of Lithuania. The generalization of legal imperatives regarding cybercrime sphere are linked to provide more general penal regulation for illegal electronic threats, however such general and not specific regulation is not able to provide the necessary level of legal protection and ensure legal stability in this criminal area..

Despite the fact that Lithuania's main Penal National Act - Criminal Code's section for the electronic crimes has been developed with less legal efforts and attention as it actually

[109] The Constitution of the Republic of Lithuania. Article 22
[110] D. Stitilis,P. Pakutinskas,M. Laurinaitis,I. Dauparaite. Identity theft in Cyberspace. The Aspects of Social, Legal and Electronic Business. Vilnius, 2011 p. 261-262

should, for the last twenty years, after Lithuania got its independence from the Soviet Union, it has been indicated, that legal disadvantages of legal regulation insufficiency still occur. The lack of legal development and innovation in the section for the electronic crimes, have led to the inability of specifically qualifying the illegal electronic acts, such as electronic Identity theft.

On the other hand, Lithuania has adopted the main legal instrument Convention on Cybercrimes and it is bound by Convention from the year 2003. The Convention was ratified by the Lithuanian Parliament on 18 March 2004 and entered into force on 1 July 2004.[111] Lithuania has already implemented the vast majority of the Convention legal provisions, which were binding, after the signing this international legal document. However, as the last amendment of the Criminal Code (CC) of Lithuania has been adopted in the year 2000, with the comparison of the Convention which got its binding power in the year 2004, other illegal activities under the Convention such as access and misuse of devices had to wait for another amendment to be criminalized.[112] Even though internet related crime such as child pornography was criminalized in the CC by Article 162 and its force together with the new amendments of the CC.[113]

However, computer related forgery crimes, together with the identity theft, have not been implemented into the new amended Criminal Code. This legal gap has been negatively affecting the process of the investigation and finally the prosecution of electronic crimes. With the absence of the specific legal norms in the CC, legal gaps occur. With the efforts to criminalize electronic identity theft, the prosecutor has only the ability to search for the indirect laws, which would define the illegal electronic act at its closest.

However such criminalization process is not only lasting, but also not specific enough to qualify the illegal acts. The potential legal solution, when criminalizing electronic identity theft, according to the CC of Lithuania is to adapt several existing legal penal imperatives which elements of its complexity would be relevant to identity theft as the crime itself, but not the complex part of the other electronic or non electronic crimes. Scholars indicate, that in Lithuania, as in other many European countries the identity theft has not been criminalized, as also, for instance, in UK, Estonia, Russia, Finland, etc. The reason for that is that the legal penal

[111] D. Sauliunas. 2010. Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime. p. 217
[112] Ibid., p. 217
[113] Criminal Code of the Republic of Lithuania. Official Gazette. 2000, Article 167., No. 89-2741

imperatives are implicated in other more general penal norms in the national penal acts, however it is marked, that criminal liability still occur when the general norms are applied correctly.[114]

Legal norms that are related to the frauds performed through the internet are provided in CC Article 198, which indicates that: "The person who has observed, kept, took over, spread or in over way has used this personal non-public information will be punished with the fine, or sentenced for up to four years in prison."[115] Article 198 (1) stress the liability for illegal access to the information structures: "The person who has illegally accessed the information structure, breaking the security enhancing measures, will be punished with the public work, fine, arrest or sentence up to one year in prison".[116] The Criminal Code of Lithuania also indicate legal liability for the possession of the devices, illegal software, passwords, connection codes stating that: "The person, who illegally produced, transported, sold or in other illegal way has disseminated these aforesaid devices, personal information, for the purpose to perform illegal activities, will be punished with public work, fine or will be sentenced up to three years in prison.[117]

With the review of the main legal provisions in the Criminal Code of Lithuania, it has been noticed, that legal regulation for the fight for computer or information systems related fraud, especially in identity theft sphere, is more primary than specific and is seen to be more general than specific. Due to this reason it is hard to criminalize such electronic acts performed by the fraudsters, because the criminalization process might not be as effective as it could be with the specific penal norms provided in the CC. These legal gaps should not only be filled with prosecutor's judicial decision combining the actual criminal situation with the existing penal norms, but rather the whole state problem, as Lithuania is one of the signatory states the Article 8 of the Convention on Cybercrimes and it is binding on the state. [118]: "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,

---

[114] D. Stitilis,P. Pakutinskas,M. Laurinaitis,I. Dauparaite. Identity theft in Cyberspace. The Aspects of Social, Legal and Electronic Business. Vilnius, 2011 p. 252
[115] Criminal Code of Lithuania. Article 198
[116] Ibid., Article 198^1
[117] Criminal Code of Lithuania, Article 198^2
[118] Convention on Cybercrimes. Article 8

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."

The Convention Explanatory Report points considers fraud, including credit card fraud. Credit card fraud is highly connected with the use of the personal information issued by the private banking system and all the procedures regarding it are only possible with the use of personal information (ATM banking, Electronic banking and etc.). As the example of a problematic criminalization and applying process would be credit card fraud, which according to the Convention on Cybercrimes has to be implemented into the national legal system of Lithuania.

Scholars emphasize, that Article 207 of the CC establishes a provision on 'Credit Fraud', but its contents appear unrelated to credit card fraud:[119] "person who, by deceit, obtains a credit, loan, subsidy, warranty or bank guarantee statement or another credit obligation…"[120] The electronic identity theft might also be qualified by the existing imperative norms or its complexity.

However, when qualifying identity theft which was used for the illegal acts described in Article 207 of the CC, it is very often necessary to combine Article 214[121], which describes the criminal liability of the use, manufacture, illegal disposition of the fraudulent use of electronic paying instrument or fraudulent usage of its data (electronic cards, for instance), these acts would cause a fine, arrest or imprisonment up to six years. At the moment, combining these two penal imperatives, the identity theft might be caught and qualified according to them, but then again, this qualifying process is rather more difficult, than just the application of these two norms. Article 167 indicates[122] that illegal gathering of the personal information about the individual may result in a fine, arrest or imprisonment up to three years. Article 168 states[123], that publishing or illegal use, of the personal information of any kind will cause a fine, arrest, public work, or imprisonment up to three years. Article 186 provides[124] a security from the loss of material of any kind, which appeared after the fraudulent acts, these fraudulent acts will be

[119] D. Sauliunas. 2010. Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime. p. 215
[120] Criminal of Lithuania. Article 207.
[121] Ibid, Article 214
[122] Criminal Code of Lithuania. Article 167
[123] Ibid., Article 168
[124] Ibid., Article 186

punished by the state by the fine, public works, or imprisonment up to three years. Not less important penal norm, which also qualifies the identity theft, is Article 215[125], which indicates, that illegal use of the electronic payment instrument or its data will cause the fine, arrest or the imprisonment up to six years. Together with these norms, Article 300[126] describes the individual liability for the manufacture of the fraudulent electronic payment instrument, and disposition of it, which will cause the arrest, fine or imprisonment up to three years.

Article 178 of the Criminal Code remain the main penal imperative, which establish the individual liability for the theft in general. It might be made a common mistake while qualifying illegal electronic acts according to this penal norm as a base one. The scholars envisage a very important aspect, that CC of Lithuania and its article 178 is only applied when the object which is secured by this imperative is material, portable good, or in other words, according to this article legal security is only guaranteed to only those goods, that have physical parameters .[127] In the case of electronic identity theft personal information might not be considered as a good which has a physical parameters. The secret personal or public information is a valuable good though, however according to the rule of Law, due to this, electronic identity theft could not be qualified according to Article 178 of CC of Lithuania. In decision nr. 52 of the Supreme Court of Lithuania was stressed what are the goods that are secured according to this article: "Property according to Article 178 of CC are only those goods which have a value, physical parameters

(dimension, weight, number, quantity), such as a car, house wares, personal belongings, money, funds."[128]

These penal imperatives illustrate the abstractness of the legal dispositions. None of the reviewed legal imperatives have an ability to criminalize the identity theft, which negative impact, have caused legal disputes worldwide, as well as in Lithuania. Moreover, from the analysis of the provided legal imperatives it is able to indicate, that complex penal imperative has

[125] Ibid., Article 215
[126] Ibid., Article 300
[127] Professor Oleg Fedosiuk. Criminal Law. Criminal Offences to the Real Property and the Rights of Real Property. <www.mruni.eu/mru_lt_dokumentai/...teises.../Nusik_turtui_1.ppt> *Accessed 28 October 2012*
[128] 23 June 2005. The Decision nr. 52 (4) of the Supreme Court of Lithuania. "Due to Equal Judicial Practice of the National Courts in the Cases of Theft and Robbery. "
<http://www.lat.lt/4_tpbiuleteniai/senos/nutartis.aspx?id=29259>. Accessed 30 October 2012

not been arranged after the second amendment of the Criminal Code of Lithuania in the year 2000. This situation, without an incentives to do that, had made easier situation for cybercriminals to steal, acquire identity electronically and feel secure. The evidence and qualification process is considered to be very complicated, as well as time-consuming , makes the submission of evidence more problematic.

The penal imperatives that are single, isolated theft norms, linked to protect one or more valuable goods were legislated for other purposes, but not to protect from the electronic identity theft *per se*. The aim was not to spot and qualify the identity theft as a vulnerable sphere, due to the reason, that the public relations, together with the authoritative institutions of Lithuania were not able to foresee the necessity of the identity theft criminalization itself. As later practice has shown, the vast majority of electronic fraud has been performed primary using the electronic theft of the individual's identity. Scholars indicate, that the legal penal imperatives that are provided in the CC describes different parts, and different contribution of the identity theft, however there is no specific norm, which would indicate this illegal electronic threat.[129]

On the other hand, Lithuania has adopted and amended its penal norms, specifically Articles 162, 166, 167, 196, 197, 198, 198(1), 198(2), 214, 215, 262, 309.[130] These penal norms were amended and corrected in such way, that would illustrate the penal aims of the Convention. This had led to a result, that some of the aforementioned penal norms of Lithuanian CC would reflect the international contribution against the fight of cybercrimes, not even in national aspect, but internationally as well.

[129] D. Štitilis P. Pakutinskas I. Dauparaitė., M. Laurinaitis. "The Establishment of Legal Environment in Order to Prevent the Identity Theft." 2011., p. 73

[130] Explanatory Report on the CC of Lithuania. <http://tar.tic.lt/Default.aspx?id=2&item=results&aktoid=82D0D069-6EC6-4C14-AE35-44FFE0A9D885> Accessed 28 October 2012

4.3 The Proposal for the Criminal Code of Lithuania

4.3.1 Overview

This chapter will represent the necessity of the specific legal penal regulation in the Criminal Code of Lithuania. The current legal situation has already been reviewed, so that by the conclusion, there has been seen a necessity for a new amendments in the Criminal Code. The proposal will be declared according to the practice of other national regulations in the states such as United States. The reader will be informed of the possible legal alterations, or the establishment of a new legal imperative. The national legislator of Lithuania might pay its legal attention when the new amendment of the Criminal Code of Lithuania will take place.

4.3.2 The Legal Proposal in Response to the Electronic Identity Theft

The scholars of IT Law have started to dispute about the necessity to criminalize electronic identity theft. It is considered that such vulnerable sphere negatively affect the users of the electronic environment (physical, legal persons). The criminalization process has to be brought up to date, and reflect the actual reality and situation that is situated in the public society at the moment. The theory of law indicates, that no legal imperative is able to take legal roots, before the relations between the subjects has not settled down, and became visual and clear for the society. [131] The illegal acts have to be considered in the same manner. The national legislator is only able to provide such penal imperatives, that would be protecting existing tangible or

[131] "Theoretical Problems on the Criminal Prevention". Criminology., Jurisprudence, 2003. Vilnius

intangible goods, or prohibit the illegal acts, in this case, performed in the electronic environment. There is no possibility for the legislator to predict totally specifically the acts, or performances that he is not able to know about, at the legislation moment, moreover, that criminal laws has to be imperative and direct, too huge generalization of the illegal act might cause the legal gaps, that will help the criminals to avoid the liability or make it lighter. Hence, according to the legal and real situation penal laws has to be legislated, or amended if necessary.

The actual afore presented situation has illustrated the necessity of the new penal law amendments in the Republic of Lithuania, in the sphere of cybercrimes, more specifically in electronic theft of the identity.

4.3.3 The Proposal

It is important to notice that criminalization of a specific illegal act has to have an objective reason and legal aim. The illegal act, which might be prohibited by the penal norm, has to have incentive to commit a crime. It means, that an illegal act must not only go against morality, but as well leave harm for the whole society, more specifically, the illegal drawbacks will not only damage moral norms, but also will have criminal initiatives. Therefore, theoretical literature indicates the necessity to have these criminal initiatives prevented "before the illegal actions are committed [...], the criminal legal prevention has to be linked to the levels of national, regional, social groups, but the legal criminal prevention has to be especially focused on specific individuals, which is defined as "special individual prevention".[132] Hence, criminalizing electronic identity theft as such, the legislator has to foresee which values will be damaged and weigh whether such an illegal act is worth for the penal norm to be established in the main criminal act of the state. If, for instance, the performer has the incentive to steal the user name and password of social network account that belongs to his friend in order to check some

[132] Theoretical Problems of the Criminal Prevention". Criminology., Jurisprudence, 2003. Vilnius

personal messages, then, of course, the electronic identity theft will occur. On the other hand, the secret theft or secret occupancy of this personal information, without an incentive to commit a felony therein will not be as injurious, as it would be, if the infringer would have had such incentives.

Due to the novelty of cybercrime in Lithuania and rapidly growing amount of cybercrimes related or straightly connected with an electronic identity theft, has raised the scholarly disputes of the necessity for establishing a legal norm, which would enhance the protection against these type of electronic threats. However, in my opinion, not all of the proposal parts presented by one scholar is considered to be correct. As it was revealed in the previous chapter, the Article 178 of the Criminal Code is basically linked to protect the objects that have physical parameters.

The current Article 178 declares[133]:

1. "The person, who has abducted vicarious property, will be punished with public works, fine, restriction of freedom, or imprisonment up to three years."

2. " The person, who has abducted vicarious property by invading into the room, storage, or private territory, will be punished with fine, arrest, restriction of freedom, or imprisonment up to five years."

3."The person, who has abducted a large amount of assets, will be punished by imprisonment up to seven years."

4. "The person, who has abducted a small amount of assets, has made a misdemeanor and will be punished by public works, arrest, fine or restriction of freedom."

The proposal for a specific penal legislations presented in 2011 in one of the Lithuanian monographs, could be evaluated as not ensured and specific enough. One part of the proposal was to modify the definition *non-public data* to only *data* in Article 198 (1), so that the disposition of the norm would be: "The person who without a permission has observed, fixate, took over, kept, spread or used not his personal *data* in other form". So definition *public data* is would be changed with a definition *data.* However, such definition still would not reflect and

[133] Criminal Code of the Republic of Lithuania. Article 178

establish the necessary features of electronic identity theft, so that such disposition would not contribute against the fight of this illegal electronic threat.[134] The proposal finds its end by suggestion to establish a new penal norm, \ establishing a more specific theft[135], especially in the electronic environment. However, the scholars have suggested to establish one penal norm, which would absorb both electronic and offline world identity theft. In addition to this, according to the proposal, the legislated penal imperative would be seen as follows: the liability appears for the physical identity theft by one part of the penal norm, stricter liability would be established by the second part of the penal norm. However, this abstract suggestion should be criticized, for the following legal reasons.

Firstly, the initiative to criminalize an illegal act has to be weighed and fulfill its stated legal aims. In order to reach the efficiency of the criminal prevention, increased attention to the penal norms has to be paid. The necessity for the criminalization of the electronic identity theft has more supportive legal arguments than the offline world's identity theft. The reason of it is the vulnerability aspect. The illegal threats performed through the electronic environment using information and communication measures, special software and similar techniques are more dangerous comparing to the identity theft performed with the offline world. In addition to this, the importance of separation of these two illegal acts by the penal norms is vital. The legal aim of it is strict attention that would be expressed in a stronger manner when having an electronic identity theft as a separate penal Article with an index one. The establishment of the identity theft in a physical space is also vital, as its negative consequences leave no legal doubt, however, due to the reason that defense from such form of identity theft is much easier comparing to the identity theft performed in the electronic environment.

In accordance to what has been indicated, the following penal norm establishing liability for the electronic identity theft might look as follows:

178 [1] Electronic Identity Theft

[134] Proposal for Criminal Code of Lithuania ., Article 198 (1)
[135] The current Article 178 of CC establish liability only for such theft, which object has physical parameters, hence the electronic identity theft could not come into the protecting area of this article.

1. The person, who abducted, took over, stole or in other form illegally acquired vicarious electronic information, or personal information, which could be used to acquire the access to an individual profile or account, will be punished with fine, restriction of freedom, or imprisonment up to four years.[136]

2. The person, or qualified group of persons, who has committed the illegal acts, mentioned in the part one of this Article, with an incentive to cause regional, international disorder in the electronic environment, or with an aim to perform a terrorist attack, will be punished with an imprisonment up to ten years.[137]

[136] The duration of the penalties, such as imprisonment is the matter of the evaluation of the legal consequences, and should be decided by authoritative institutions, or law experts.
[137] Ibid.,

5 Conclusion

`

The aim of this last chapter is to provide the brief overview, expressing the concluding remarks regarding the analyzed legal topic and its legal issues.

To start with, the analyzed section of criminal law has revealed: despite the legal dialogues and initiatives among the EU institutions, the legal diversity still exists in the sphere of cybercrime area - electronic identity theft. During the last decade, the electronic identity theft has become one of the most notorious electronic threats in the cyber environment. Due to this reason, first, the necessity to criminalize such illegal electronic acts has been realized in the United States of America, which has adopted various specifically orientated penal acts for the legal fight against the electronic identity theft. The USA legislated penal acts have enhanced its abilities to control cybercriminals and impose criminal penalties for the electronic identity thefts. However, such necessity of criminalization for these types of cybercrimes has not caught legal attention among the legal institutions of the European Union until almost 2001, when the first binding legal decision was adopted, the combating fraud and counterfeiting of non-cash means of payment in the EU 2001/413/JHA has been adopted, until this decision EU regulation on related crimes was basically formulated only in the initiative forms, as there has not been almost any legal measures regarding this criminal plot.

Legal deliberations, whether at all there is a necessity for a criminalization of identity theft was in process. Nevertheless, the discussions were beneficial and starting from the year 2007 the EU Commission has started to arrange the necessary proposals to the EU Parliament and the Council. These types of legal proposals were a significant impulse for the European Union legal institutions, noticing the importance of the rapidly growing electronic threats performed in the cyberspace. However, these initiatives are still being concluded as theoretical

and have not given any substantial legal benefits. On the other hand, the necessity of amending existing or establishing new legal mechanism to fight against cybercrimes is extremely necessary, especially in electronic identity theft, on the EU level was established on 22 May 2007.The identity theft as such is still being evaluated as tool to commit other, more fraudulent illegal acts, but not as a single dangerous threat, which should be criminalized under the specific penal imperatives. However, it should be indicated that the review and analysis of this sphere reveals that the necessity for criminalizing this electronic threat leaves no legal doubts. The current situation has showed: without a adequate legal penal background in the European Union it is not able to contribute not only in regional legal fight against specific types of cybercrime, but also international legal co-operation is concluded to be very poor. Due to the novelty and evolving information society, the EU has to focus its legal attention regarding this area, by proposing specific directives of aforementioned issues, with a proper guidelines, which would contribute in legally fighting with specific type of cybercrimes, within EU member states first.

The EU's legal conditional passivity has also affected a vast majority of its member states, which criminal legal background in the area of cybercrimes is considered to be weaker comparing to other older democratic legal systems. The post-soviet countries such as Lithuania were not able to use the proposals or directives of the EU, because before the last amendment of the Criminal Code of Lithuania there have been no EU initiatives in this penal criminal plot. This lack of proper legal penal background has started to reveal its drawbacks, as many of the nowadays electronic crimes are performed with the former theft of identity in the electronic environment. Due to the lack of specific penal imperatives linked to the fight against such criminal activities in the main penal act of Lithuania, the cybercriminals have full freedom to commit cybercrimes without being penalized and circumventing criminal investigation and prosecution. The reason for this is the abstractness of national public laws and too wide generalization of the national public penal imperatives regarding these types of electronic crimes in the Criminal Code of Lithuania. In order to impose the legal penal process, the national prosecutors are forced to formulate the accusation according to the existing penal imperatives provided in the different sections of the Criminal Code, however as revealed in the former chapters of this thesis work, these penal imperatives have their drawbacks, such as lack of specification of the cybercrimes or even sometimes insufficiency for the electronic identity theft to be criminalized and the accusation formed and later presented to the court in a proper legal

context. The inabilities and insufficiencies in the above indicate that penal norms of CC of Lithuania implicate the available circumventions of the criminalization, which is of course very helpful for the legal defense of cybercriminals

In order to provide proper legal penal regulation in the Criminal Code of Lithuania, the necessity to implement the specific penal norm has been discussed. The proposed specific penal norm would differ from the other norms, which are also linked to the protection of the goods and values from the theft, however this specific imperative would have an incentive to protect the intangible mode of good -the personal information of the individual., due to the above discussed reason, that the scope of the Article 178 of CC is not legally able to protect this type of good, because, according to the Supreme Court of Lithuania, the protective object of this penal norm is different. [138]

Moreover, the discussed suggestions to legislate such penal norm, which would encompass both the physical identity theft and electronic identity theft should be and have been criticized with the supportive arguments declared in above section. The dangerousness of electronic identity theft as such implicates the specific attention declared in the main penal act of Lithuania. The more dangerous the illegal activity is, the higher criminalization level, place and legal penal attention it gets in the main national penal legal act, and Criminal Code of Lithuania is not an exception. As an example could be provided the Article 129, which provides the liability for killing a person and Article 131 of the same section, which provides much stricter liability for killing the pregnant woman, however this provision of killing a pregnant woman is not established under some paragraphs of Article 129 in order to reflect the seriousness of the criminal act. Due to this reason, the dangerousness of this illegal act, which has been discussed, supported and proved, it would be suggested to establish the electronic identity theft penal norm as single, independent with its own disposition and sanction in the same article, without the establishment of the liability for identity theft in the physical space, provide this illegal activity with another legal imperative or make it additional part of aforesaid Article 178 of CC.[139] The consideration, whether the current penal legislation of combating cybercrime in the EU and

[138] 23 June 2005. The Decision nr. 52 (4) of the Supreme Court of Lithuania. "Due to Equal Judicial Practice of the National Courts in the Cases of Theft and Robbery. "
<http://www.lat.lt/4_tpbiuleteniai/senos/nutartis.aspx?id=29259>. Accessed 30 October 2012

[139] Criminal Code of the Republic of Lithuania. Official Gazette. 2000, Article 178., No. 89-2741

Lithuania is adequate has to be answered as not, at the moment. Even though the European Union has started to provide legal efforts to concentrate on the cybercrime area quite extensively, however it is done by the initiative form only, excepting few legal instruments which already have binding force for the whole Community. However, the vast majority of the analyzed legal measures in this thesis work, that are still in the deliberation process does not assure the legal stability and harmonization in this sphere of criminal plot and it is expected that these initiatives will become binding acts in the very near future, also facilitating the penal politics for EU member states when establishing common, adequate, efficient penal laws in the specific section of cybercrimes.

6 References

Legislation

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA)

Council Framework Decision of 24 February 2005 on attacks against information systems (2005/222/JHA)

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Brussels, 31.5.2006 COM(2006) 254 final

Communication from the Commission to the Council and the European Parliament, and Social Committee and the committee of the Regions. A Digital Agenda for Europe. Brussels, 26.8.2010COM (2010) 245 final/2

Communication from the Commission to the Council and the European Parliament. Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. Brussels, 28.3.2012 COM(2012) 140 final

Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cyber crime. Brussels, 22.5.2007 COM(2007) 267 final

Convention on Cybercrime. Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer system. Strasbourg, 28.I.2003

Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 ((amending 18 U.S.C. § 1028). 1998. USA

Identity Theft Penalty Enhancement Act and the Identity Theft Investigation and Prosecution Act. Washington., USA. 2004

Constitution of Republic of Lithuania.

25 October 1992, Vilnius, Lithuania**.**

Criminal Code of the Republic of Lithuania. Official Gazette. 2000., No. 89-2741. Vilnius, Lithuania

The Supreme Court of Lithuania. The Decision nr. 52 (4) "*Due to Equal Judicial Practice of the National Courts in the Cases of Theft and Robbery"*. Vilnius, Lithuania. available at: <http://www.lat.lt/4_tpbiuleteniai/senos/nutartis.aspx?id=29259>.

Literature

N. Kshetri. *The Global Cybercrime Industry. Economical, Institutional and Strategic Perspectives.* North Carolina., USA.2010

Antonopoulos, A. *ATM hack: Organized crime or market forces? Network World*. Southborough. 2009

N. Kshetri. Positive externality, increasing returns and the rise in cybercrimes. *Communications of the ACM,*). 2009

Parker, D. B. *Crime by Computer*. New York.,1976

Ghosh, S., Turrini, E. *Cybercrimes. A Multidisciplinary Analysis. Springer*. 2010

Rannenberg K. Royer D. Deuker A. *The Future of the Identity in the Information Society.* Frankfurt. 2009

Cane P., Conaghan J. *The new Oxford Companion to Law*. Oxford University Press Inc. Oxford. 2008

David-Olivier Jaquet-Chiffelle. *The Future of Identity in the Information Society*. Springer. 2009

Stitilis D, Pakutinskas P. Laurinaitis M. Dauparaite I. *Identity theft in Cyberspace. The Aspects of Social, Legal and Electronic Business*. Vilnius, 2011

Biegelman T. M. *Identity Theft Handbook. Detection, Prevention, and Security* New Jersey. 2009

Sileo J.D. Stolen lives: *Identity theft prevention made simple.* California, USA. 2006

Higgins H.E. *Cybercrime: An Introduction to an Emerging Phenomena.* Louisville. 2010

Sandra K. Hoffman., Tracy G. McGinley. *Identity Theft. A Reference Handbook.* Santa Barbara, California..2010

Bryan K., Dunnesen K., Jean J., Jellenc E., Lincoln J., Ligh M., La Pilla M., Olson R., Scholnick A., Sinclair G., Wills T., Zenz K. *Cyber Fraud: Tactics, Techniques and Procedures*. Auerbach Publications, Florida. 2009

Brenner, S.W. Cybercrime. *Criminal Threats from Cyberspace*. Oxford University Press. 2009

Articles

Pollock, J., May, J.. *Authentication Technology Identify Theft and Account Takeover*. The FBI Law Enforcement Bulletins, United States Department of Justice Federal Bureau of Investigation., 2002. available at : < http://www2.fbi.gov/publications/leb/2002/june02leb.pdf >

United States Government Accountability Office. *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*., available at: < http://www.gao.gov/products/GAO-07-705>

Tim Wilson. *Cybercrime outranks other crimes on Europeans: worry list: Almost half of German PC users believe they will eventually fall victim.* 2008

Rachael King. *Countries with the most cybercrime.* 2009., available at: <http://images.businessweek.com/ss/09/07/0707_ceo_guide_security/1.htm>

N. Kshetri. *Positive externality, increasing returns and the rise in cybercrimes. Communications of the ACM*, 52(12). 141-144 ., 2009. available at: <http://libres.uncg.edu/ir/uncg/f/N_Kshetri_Positive_2009.pdf>

N. Kshetri.. *The simple economics of cybercrimes, IEEE Security and Privacy*, 4(1), 33–39., 2006. available at :<http://libres.uncg.edu/ir/uncg/f/N_Kshetri_Simple_2006.pdf>

Authenticated US Government Information. *Crimes and Criminal Procedure*. available at:

<http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap47-sec1029.pdf>

Find Law UK. *Identity cards.* available at: <http://www.findlaw.co.uk/law/government/other_law_and_government_topics/8793.html>

Burr E.W. ,Dodson F.D., Timothy W.P . Electronic Authentication Guideline. *Information Security.* available at: <http://www.usda.gov/egov/egov_redesign/intranet/eauth/SP800-63V6.pdf>

Spam Laws. *The History of Identity Theft.* available at:

<http://www.spamlaws.com/id-theft-history.html>

OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders *Online Identity Theft*. 2003 available at :

<http://www.oecd.org/internet/consumerpolicy/oecdguidelinesforprotectingconsumersfromfraudulentanddeceptivecommercialpracticesacrossborders2003.htm>

United States Postal Service. *Identity Theft. Safeguard Your Personal Information*. 2009 available at:

<http://about.usps.com/publications/pub280.pdf>

Royer D. *D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research*

<http://www.fidis.net/resources/deliverables/forensic-implications/int-d52b000/doc/20/>

Prof. dr. Babachinaite G., Prof. dr. Kuklianskis S. *Theoretical Problems of the Criminal Prevention.* Criminology., Jurisprudence, 2003. Vilnius

Reports

Explanatory Report on the Criminal Code of Lithuania. available at:

<http://tar.tic.lt/Default.aspx?id=2&item=results&aktoid=82D0D069-6EC6-4C14-AE35-44FFE0A9D885>

Dictionaries

Official Oxford Dictionaries. available at :
<http://oxforddictionaries.com>

Other sources

Criminal Law. Prof. Fedosiuk O. *Criminal Offences to the Real Property and the Rights of Real Property*.

available at: <www.mruni.eu/mru_lt_dokumentai/...teises.../Nusik_turtui_1.ppt>