ISSN 1392–6195 (print)
ISSN 2029–2058 (online)
JURISPRUDENCIJA
JURISPRUDENCE
2010, 4(122), p. 203–219.

LEGISLATION ON CYBERCRIME IN LITHUANIA: DEVELOPMENT AND LEGAL GAPS IN COMPARISON WITH THE CONVENTION ON CYBERCRIME

Darius Sauliūnas

Mykolas Romeris University, Faculty of Law,
Department of International and European Union Law
Ateities 20, LT-08303 Vilnius, Lithuania
Telephone (+370 5) 2714 669
E-mail d.sauliunas@euroteise.lt

Received 12 October, 2010; accepted 22 November, 2010.

Abstract. *The Convention on Cybercrime (the Convention) adopted in the framework of the Council of Europe is the main international legislative tool in the fight against cybercrime. It is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. Lithuania is among its signatory states, therefore, the provisions of the Convention have become binding on its legislator, obliging it to take all necessary measures to harmonize national legal acts with the framework set out therein. The Criminal Code of the Republic of Lithuania (the CC) in force is the legal act establishing liability for criminal offences known as computer crimes and Internet crimes. Although the legislator of Lithuania had been combating cybercrimes since as early as 1994 by means of the amendments to the Soviet era Criminal Code of 1961, a significant effort was required to transpose the requirements of the Convention into the Lithuanian law, starting from the year 2007. The end result was not always as expected, leaving several serious gaps in the field of criminalization, which are thoroughly addressed in the article. In particular, this article deals with the topic of computer-related crimes and the legal approaches related to substantive criminal law of the Republic of Lithuania. The study is based on a comparative legal analysis of the Lithuanian CC and the Convention.*

ISSN 1392-6195 (print), ISSN 2029-2058 (online)
http://www.mruni.eu/lt/mokslo_darbai/jurisprudencija/
http://www.mruni.eu/en/mokslo_darbai/jurisprudencija/

Keywords: *cybercrime, Criminal Code of the Republic of Lithuania, internet crimes, Convention on Cybercrime.*

Introduction

The phenomenon of cybercrimes has been a great challenge for the Lithuanian legislators, crime investigators and courts, and it is the right time to speak about the viability of the current criminalization of such acts in the Lithuanian Criminal Code (the CC)[1]. In the Lithuanian criminal jurisprudence, the term 'cybercrime' is used in its widest sense—illegal action in computer systems or computer networks. Cybercrimes are separated from ordinary crimes on the basis of their technology: digitalization, automatization and data transfer networking. Cybercrimes include offenses that are impossible without a computer (e.g. hacking) as well as offenses for which a computer is not usually necessary, but can involve the use of it (e.g. data theft, distribution of child pornography). Crime investigators also use the term cybercrime in cases when it is possible to collect evidence with the help of computers or their networks, though the crime itself might have been committed without using a computer.

Many scholars have tried to define cybercrime types. Parker[2] 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. In modern writings, the term cybercrime is usually applied to any crime for the commission of which the use of Internet is essential.[3]

The legislative practice approach proved to be less concerned with the role of a computer. The Convention on Cybercrime (the Convention)[4] proposed the following categorization:

---

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

2 Parker, D. B. *Crime by Computer*. New York: Charles Scribner's Sons, 1976; Parker, D. B. *Fighting Computer Crime*. New York: Charles Scribner's Sons, 1983.

3 Kaspersen, H. W. K. *Cybercrime and Internet Jurisdiction, Discussion paper (draft), version 5 March 2009, prepared in the framework of the Project on Cybercrime of the Council of Europe* [interactive]. [accessed 12-02-2010]. <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf>.

4 Council of Europe Convention on Cybercrime (adopted 23 November 2001, entered into force 7 January 2004). CETS No. 185. For more details about the offences covered by the Convention, see Sofaer, A. D.; Goodman, S. E. *Toward an International Convention on Cybercrime*. *The Transnational Dimension of Cyber Crime and Terrorism.* Stanford: Hoover Institution Press, 2001; Gercke, M. The slow awake of a global approach against cybercrime. *Computer Law Review International*. 2006, 141; Aldesco, A. The demise of anonymity: a constitutional challenge to the Convention on Cybercrime. *Entertainment Law Review*. 2002, 23(81): 82 [interactive]. [accessed 10-12-09]. <http://elr.lls.edu/issues/v23-issue1/aldesco.pdf>; Jones, J. *The Council of Europe Convention on Cybercrime, Themes and Critiques* [interactive]. 2005 [accessed 10-12-09] <http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf>; Broadhurst, R. Development in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management*. 2006, 29(3): 408; Adoption of Convention on Cybercrime. *International Journal of International Law*. 2001, 95(4): 889.

1) offences against confidentiality, integrity and availability of computer data and systems;

2) computer-related offences;

3) content-related offences;

4) offences related to infringements of copyright and related rights. This categorization may be therefore considered a de facto world standard due to the high acceptance of the Convention worldwide.

The present article is based on a research conducted using the method of comparative analysis of the international and domestic legal acts, the chronological method (comparison of legislation before and after amendments) and the teleological method (clarification of the purposes of the adopted legislation). A linguistic analysis was one of the tools to find out the possible discrepancies and collisions between the international and Lithuanian regulation.

There are two main objects this research is targeted at: the Convention and different editions of the CC of the Republic of Lithuania in effect from 1994 until present. Currently the Convention is the main international legislative framework for the fight against cybercrime. Forty-six countries have signed[5] and twenty-six countries have ratified[6] the Convention by 1 February 2010. Lithuania signed the Convention on 23 June 2003. It was ratified by the Lithuanian Parliament on 18 March 2004 and entered in force on 1 July 2004.

This article is aimed at analysing the development of cybercrime regulation in Lithuania, paying special attention to its inconsistencies and drawbacks and clarifying the possible discrepancies between the Convention and the CC of Lithuania. The purpose is to identify whether the implementation of the provisions of international legal acts was satisfactory and acceptable and whether the criminalization would satisfy the requirements of the rapidly developing information society. Previously this aspect of cybercrime regulation has not been discussed in the Lithuanian scholarly literature.

1. Changes in the Lithuanian Legislation Prior to the Convention: First Steps towards the Criminalization of Cybercrimes

The Lithuanian state faced the emergence of the digital era still using the decades-old CC with Soviet heritage, where there was no place for cybercrimes. The challenges of the digital era were to face the Lithuanian law enforcement together with the growing

5 Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, the United Kingdom, Canada, Japan, South Africa, the United States.

6 Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, the Netherlands, Norway, Romania, Serbia, Slovakia, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine, the United States.

use of computer technology. Inevitably, the fight against cybercrime was started by the legislator in1994 when the Parliament adopted the total and complex amendment to the old CC of 1961, which remained in effect until 1 May 2003.

The first regulation was not specific and by no means extensive. The legislator had mostly been interested in a more severe punishment of those involved in new modern ways to undertake fraudulent activities as well as cause damage to property. Therefore, the most widespread property crimes were affected by the earliest amendments. Obviously, the most prevalent misuse of computers and network back then was (and probably still is) the creation of computer viruses and similar malicious software.

Computer programs or databases emerged as novel objects of copyright violations.[7] Computer technology has made copying, modification, multiplication and distribution of digital data very easy resulting in its vulnerable nature. The major drawback of the regulation was that regardless of a significant number of initiated criminal cases and subsequently imposed imprisonment penalties (usually on the distributors of pirated software), the 'true criminals'—software professionals who cracked the secured software and made it available to the public—remained undisclosed.

In conclusion, the criminalization of cybercrime in the old CC was limited to a few qualifying provisions of fraud and damage to property. There was no separate chapter dedicated to computer-related crimes. As a result, a lot of cybercrimes were left outside the law. Nevertheless, as cybercrimes were still *terra incognita* for many potential criminals and victims ten–fifteen years ago, crime rates have been increasing steadily in Lithuania, with no signs of the situation going beyond control. This has changed only recently and, fortunately, the legislator did react in time by adopting the new laws.

In 2000, the Parliament adopted the new CC which entered into force on 1 May 2003. The entirely new Chapter XXX entitled 'Crimes against Informatics' was devoted to cybercrimes. Although the name of the chapter was changed after facing great criticism, several mistakes remained (e.g. terms 'data' and 'information' were not separated again). Probably the greatest mistake was the disregard of the Convention.

One of the fundamental novelties of the CC was the introduction of new subjects of crimes: legal persons and legal entities.[8] It is important to emphasize that the criminal liability of a legal entity does not release from criminal liability a natural person who has committed, organized, instigated or assisted in the commission of the criminal act. All 'crimes against informatics' were in the range of minor crimes: punished with a

---

7 For example, theft of the authorship of computer programs and databases (Article 142); illegal copying of computer programs and databases, importation, exportation, distribution and possession of illegal copies (Article 1421); deletion or amendment of information about the management of copyright (Article 1422); etc. (Criminal Code of the Republic of Lithuania, *supra* note 1).

8 Article 20 of the Criminal Code of the Republic of Lithuania stipulates:
A legal entity shall be held liable solely for the criminal acts the commission whereof is subject to liability of a legal entity as provided for in the Special Part of the Criminal Code. A legal entity shall be held liable for the criminal acts committed by a natural person solely where a criminal act was committed for the benefit or in the interests of the legal entity by a natural person acting independently or on behalf of the legal entity, provided that he or she, while occupying an executive position in the legal entity, was entitled: 1) to represent the legal entity, or 2) to take decisions on behalf of the legal entity, or 3) to control activities of the legal entity.

maximum penalty from one to three years of imprisonment.[9] Three specific cybercrimes were criminalized under the CC: abolition or amendment resulting in significant harm of computer information[10] or of a computer program[11] and interception of protected computer information about legal or natural person[12].

It is clear that such legal regulation was ineffective and again many cybercrimes were left outside the scope of the CC. The separation of computer information and computer programs resulted in the obvious duplication of the same crime as a computer program itself is a sort of computer information. There was no other difference between Articles 196 and 197 than the target of the crime. On the other hand, the legislator has described the 'abolition or amendment of computer program resulting in significant harm'[13] not only as a simple abolition, deterioration or amendment of a computer program, but also as an installation of software into a computer or its network that resulted in the interference into or modification of the operation of the computer network, database or information system causing significant harm. In other words, the legislator has criminalized the spreading of computer viruses.

On the other hand, despite being a step forward in the regulation of cybercrime, the new CC left some dangerous acts outside its scope, e.g. illegal access and misuse of devices.[14]

2. Implementing the Convention of Cybercrime in the Lithuanian Legislation

The Convention has effectively become the first instrument of global application dealing with crimes committed via the Internet and other computer networks, particularly, with infringements of copyright, computer-related fraud, child pornography and violations of network security. This is the list of crimes that each signatory state must transpose into its own law. It also contains a series of powers and procedures such as the search of computer networks and lawful interception. The purpose of the Convention was to harmonize criminal substantive law of offences and its provisions in the field of cybercrime in particular. Although the purpose of the Convention to make battling borderless Internet crimes more efficient is far-reaching, the actual transposition of the Convention's requirements into the domestic legal acts is by no means without difficulties. The procedures running counter the established constitutional principles in a particular country may be among the obstacles. To analyse the effect the Convention had on the Lithuanian law and to decide whether it has reached its envisaged purpose in

9 Article 11(3) of the Criminal Code of the Republic of Lithuania.
10 Article 196 of the Criminal Code of the Republic of Lithuania.
11 Article 197 of the Criminal Code of the Republic of Lithuania.
12 Article 198 of the Criminal Code of the Republic of Lithuania.
13 Article 197 of the Criminal Code of the Republic of Lithuania.
14 Articles 2 and 6 of the Convention on Cybercrime.

our country, it is necessary to look back to the criminalization of cybercrimes in the first decades of the independent Lithuanian state.

A substantial amendment to Chapter XXX of the CC was adopted by the Parliament on 28 June 2007. First of all, the Chapter was retitled to 'Crimes against Security of Electronic Data and Information Systems' instead of the previous misleading title 'Crimes against Informatics'. However, not only the name was changed, but also the content of the chapter was significantly improved as regards the Convention. The legislator showed a clear intent to abolish legal gaps in the regulation of liability for cybercrime and to establish a more severe liability for it.

The most significant amendment was made in Article 198, where the term 'misappropriates' was changed to 'observes, records, intercepts, acquires, stores, appropriates, distributes or otherwise uses'[15]. In addition, such features of electronic data as 'protected by law' and 'about legal and natural persons' were removed as having no legal background in regard of the Convention. The legislator has decided to apply more severe liability for cybercrimes that are targeted at electronic data or information systems having strategic importance for national security or of major importance for state government, the economy or the financial system.

3. Criminal Liability for Cybercrimes in Lithuania in Comparison to the Convention on Cybercrime

3.1. Timely Criminalization of Illegal Access ('Hacking')

Article 2 of the Convention provides the obligation of the signatory states to criminalize illegal access of computer systems:

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,* the access to the whole or any part of a computer system *without right* (emphasis added). A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.[16]

This provision of the Convention was included into Article 198(1) of the CC ('Unlawful Connection to an Information System'):

1. A person who unlawfully connects to an information system by damaging the protection means of the information system shall be punished by community service or by a fine or by arrest or by imprisonment for a term of up to one year.

2. A person who unlawfully connects to an information system of strategic importance for national security or of major importance for state government, the economy

15 Article 198 of the Criminal Code of the Republic of Lithuania.

16 Article 2 of the Convention on Cybercrime.

or the financial system shall be punished by a fine or by arrest or by imprisonment for a term of up to three years...[17]

Obviously, the term 'unlawful connection' used in the CC is just an alternative wording of 'illegal access'. The CC provides a more severe responsibility for the illegal access to an information system of strategic importance for national security or of major importance for state government, the economy or the financial system.

In Lithuania, some attempts to access e-banking systems were tracked, but the cyber attack in the summer of 2008 against more than 300 Lithuanian websites was a clear example that the criminalization of 'illegal access' in Lithuania was just in time. In the summer of 2008, the websites were defaced after Lithuania had passed a law prohibiting public display of symbols dating from the Soviet Union era as well as the playing of the Soviet national anthem. The hackers defaced the websites' homepages with pro-Soviet slogans and symbols, thereby committing a cyber attack that lasted for two days. The majority of the websites were hosted on a single physical web server, which had vulnerability either in the web server software or Linux operating system.[18]

3.2. Illegal Interception Expanded in the Lithuanian Law

Article 3 of the Convention provides for the obligation of the signatory states to criminalize illegal interception of computer data:

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, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data*. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system (emphasis added).[19]

This provision of the Convention was implemented in Article 198 of the CC ('Unlawful Interception and Use of Electronic Data'):

1. A person who unlawfully observes, records, intercepts, acquires, stores, appropriates, distributes or otherwise uses the electronic data which may not be made public shall be punished by a fine or by imprisonment for a term of up to four years.

2. A person who unlawfully observes, records, intercepts, acquires, stores, appropriates, distributes or otherwise uses the electronic data which may not be made public and which are of strategic importance for national security or of major importance for state government, the economy or the financial system shall be punished by imprisonment for a term of up to six years...[20]

The variations of the terms 'computer data' and 'electronic data' should be regarded as the same digital data. In the Lithuanian law, interception 'including electroma-

17 Article 198(1) of the Criminal Code of the Republic of Lithuania.

18 For more information see: http://vz.lt/Default2.aspx?ArticleID=a7e7328d-9cf9-42f6-81cb-47004e4299cb.

19 Article 3 of the Convention on Cybercrime.

20 Article 198 of the Criminal Code of the Republic of Lithuania.

gnetic emissions' is not mentioned *expressis verbis*. Nevertheless, the current edition of Article 198 should be interpreted as covering all types of interception including the one stated in the Convention. Personal communication (emailing, browsing and downloading information from a website) should be regarded as the one that may not be made public (or 'non-public transmissions' in the terms of the Convention).

Interestingly, the Lithuanian legislator is expanding the term 'illegal interception' to include all possible variations of it: observing, recording, interception itself, acquiring, storing, appropriating, distribution or other use. Interception is regarded as observation, recording, acquisition, storage, appropriation. However, distribution and other use of electronic data is something which is not covered by the term 'interception'. Therefore, it can be concluded that the Lithuanian law expanded criminal liability into the area of unlawful distribution and use of electronic data.

3.3. Criminalization of Data Interference Causing Serious Harm only

Another large group of cybercrimes is related to computers, networks and information systems; it includes various adverse activities and illegitimate modification of digital data. The digitalized information may be destroyed or changed (i.e. deleted or altered) easily even by non-professional users of personal computers. In the legal acts, such activity is referred to as 'data interference'. An indirect interference of computer viruses is the best and most widespread example.

Article 4 of the Convention obliges the signatory states to criminalize data interference. According to it, '[e]ach Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, *when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right*' (emphasis added) and 'a Party may reserve the right to require that the conduct described in paragraph 1 result *in serious harm*' (emphasis added).[21]

This provision of the Convention was implemented in Article 196 of the CC ('Unlawful Influence on Electronic Data'):

1. A person who unlawfully destroys, damages, removes or modifies electronic data or a technical equipment, software or otherwise restricts the use of such data thereby incurring major damage shall be punished by community service or by a fine or by imprisonment for a term of up to four years.

2. A person who commits the act provided for in paragraph 1 of this Article in respect of the electronic data of an information system of strategic importance for national security or of major importance for state government, the economy or the financial system shall be punished by a fine or by arrest or by imprisonment for a term of up to six years...[22]

---

21 Article 4 of the Convention on Cybercrime.

22 Article 196 of the Criminal Code of the Republic of Lithuania.

The Lithuanian legislator has chosen to require that the conduct of data interference result in serious harm (or 'major damage' in other words). Otherwise such conduct would only be regarded as misdemeanour.[23] According to the Lithuanian case-law, serious harm is amounted to more than LTL 18,750 (EUR 5,450). But still it is left up to the courts to decide whether a certain harm in a certain criminal case is significant.

The problem is that the Lithuanian information society is usually suffering from viruses that originate outside the Lithuanian territory, with few exceptions, what makes the application of this Article more difficult compared to others.

3.4. System Interference Lacking a Description of the Means of Committing a Crime

System interference is a more complicated cybercrime in comparison to data interference. Information system (such as an e-banking system or official state registry databank) is mostly attacked by professional users of personal computers or any other networking devices. Previously this crime was known as computer sabotage.

The obligation of the signatory states to criminalize system interference is imposed under Article 5 of the Convention: '[e]ach Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when *committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data* (emphasis added).'[24]

This provision of the Convention was included into Article 197 of the CC ('Unlawful Influence on an Information System'):

1. A person who unlawfully disturbs or terminates the operation of an information system thereby incurring major damage shall be punished by a fine or by arrest or by imprisonment for a term of up to four years.

2. A person who commits the act provided for in paragraph 1 of this Article in respect of an information system of strategic importance for national security or of major importance for state government, the economy or the financial system shall be punished by a fine or by arrest or by imprisonment for a term of up to six years...[25]

The terms 'influence', 'disturbance of operation' and 'termination of operation' should be referred to as 'hindering' in the meaning of the Convention. It is interesting that the CC does not include any provision regarding the way of such hindering while the Convention expressly puts it as follows: 'by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data'[26]. In case of doubt, the Convention should be used to eliminate the possible ambiguities of the CC.

The hindering must be 'serious' in order for a criminal sanction to be imposed for it. The Lithuanian legislator has determined it by introducing a criterion of 'major damage'

---

23 a small or minor crime, comparable to an administrative offence but still covered by the CC.

24 Article 5 of the Convention on Cybercrime.

25 Article 197 of the Criminal Code of the Republic of Lithuania.

26 Article 5 of the Convention on Cybercrime.

(amounting to at least EUR 5,450, according to the Lithuanian case-law). As 'serious hindering' the drafters of the Convention considered: the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g. by means of programs that generate 'denial of service' attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system).[27] Mere sending of unsolicited e-mail for commercial or other purposes (e.g. 'spamming') is not criminalized unless it causes serious harm to its recipient. The Convention and the CC are in line regarding this issue.

The hindering must be 'unlawful influence' ('without right'). Common activities such as authorized use, testing or common operational or commercial practices are legal. The 'without right' activities include, for example, the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Such a conduct is not criminalized under the abovementioned article, even if it causes serious hindering.[28]

3.5. Misuse of Devices where a Single one is Enough for Criminal Liability

These offences are related to the possession of the means of access ('hacker tools') with criminal purposes. Such devices may lead to the creation of a kind of black market in their production and distribution.

Article 6 of the Convention obliges the signatory states to criminalize the misuse of devices:

1. 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*:

a) *the production, sale, procurement for use, import, distribution or otherwise making available of*:

i) *a device, including a computer program*, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii) *a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed*, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b) *the possession of an item referred to in paragraphs a. i or ii above*, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5... (emphasis added).[29]

---

27 See Para. 67–68 of the Explanatory Report to the Convention of Cybercrime [interactive]. 2001 [accessed 20-12-2010]. <http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm>.

28 *Ibid.*

29 Article 6 of the Convention on Cybercrime.

This provision of the Convention was implemented in Article 198(2) of the CC ('Unlawful Disposal of Installations, Software, Passwords, Login Codes and Other Data'): '[a] person who unlawfully produces, transports, sells or otherwise distributes the installations or software, also passwords, login codes or other similar data directly intended for the commission of criminal acts or acquires or stores them for the same purpose shall be punished by community service or by a fine or by arrest or by imprisonment for a term of up to three years...'.[30]

The Lithuanian legislator has constructed a provision very brief and clear in comparison to the ones of the Convention. The description of criminal acts and devices is almost identical in both texts. Nevertheless, the Lithuanian approach is to criminalize all misuses of devices with criminal intent, in general. In the Convention, it is clearly stated that certain particular criminal acts are considered as the intent of misuse, i.e. offences established in Articles 2–5 of the Convention. In case of ambiguity and possible collision between national and international regulation, the narrower approach of the Convention is to be applied.

The Convention makes a difference between 'distribution' which refers to the active act of forwarding data to others and 'making available' which refers to making devices available for online access. The term 'otherwise distributes' used in the CC should be interpreted in both meanings. The creation or compilation of hyperlinks in order to facilitate access to such devices is enough to be qualified as 'other distribution'.

Though the Convention permitted to require by law that a number of devices adapted for the purpose of committing offences be possessed, the Lithuanian Criminal Code is silent about that. In other words, a misuse of a single device would be enough to incur criminal liability. Such an approach is not actually grounded, as the number of devices possessed goes directly to proving criminal intent.[31] A misuse of a single device is a very weak evidence of a crime established in Article 198(2) of the CC and Article 6 of the Convention.

3.6. Absence of Special Provisions on Computer-Related Fraud

From the historical perspective, computer-related offences as they are classified under the Convention have the longest tradition of criminalization in Lithuania. Computer-related fraud in particular was the first cybercrime to be criminalized in Lithuania. The criminalization of cybercrimes falling under this category had to be revised in all signatory states to make sure that their system of property crimes applies in the electronic environment as well. The old CC of the Republic of Lithuania contained a rather composite provision in essence encompassing a few separate crimes under the Convention which was adopted later. Originally, Article 277 concerning damage to property has been extended with part 2: '[d]amage to the property, made creating the knowingly wrong computer program, writing the wrong data into the memory of the computer, also

30 Article 198(2) of the Criminal Code of the Republic of Lithuania.

31 See Para. 75 of Explanatory Report to the Convention of Cybercrime, *supra* note 27.

interfering computer information in any other way, – is punished with imprisonment up to two years or correction works for the same period or the fine'.[32]

In addition to that, Article 274 of the old CC concerning fraud has been extended with the second part: '[f]raud, made… creating the knowingly wrong computer program, writing the wrong data into the memory of the computer, also interfering computer information in any other way, – is punished with imprisonment up to five years with or without the fine'.[33]

Although the legislator made it possible to prosecute other activities that would result in computer fraud, this legal regulation was generally ineffective, because the ambiguity of legal texts allowed interpretations favourable for offenders. For example, the term 'computer information' was used in the law by mistake: interference must, first of all, have an impact on computer *data* rather than computer *information*. An offender would seek to change data in such a way that the information would look the same.[34]

Previously it was considered that only a professional computer programmer could commit an offence. In order to differentiate computer fraud from a software mistake, the legislator decided to use the term 'knowingly'. One of the reasons behind this choice is the difficulty of proving deliberate action of a professional programmer, as there is always a possibility of making a mistake in a computer program source code. A deliberate writing of wrong data into computer memory means both the insertion of wrong data (e.g. about the age of a person, address, other personal data) as well as the deletion of truthful data (e.g. about the criminal history of the person, administrative offences, etc.).[35] 'Kite' is one of the most widespread computer frauds of such kind: a person opens fake accounts in several banks and with the help of fraudulent correspondence creates an illusion that there is enough money in one of the accounts so that a bigger amount could be transferred.

One may not argue that this type of cybercrime is the most widespread and will remain such in the future, as offenders committing computer crimes are usually driven by financial motivation only. Nevertheless, a separate provision regarding the so-called 'computer fraud' disappeared from the Lithuanian CC after the amendments adopted in 2003 and 2007, as the legislator has decided that the current general provision on fraud entitled 'Swindling'[36] is enough for the purposes of criminal liability for computer-related fraud.

---

32 Article 227 of the Criminal Code of the Republic of Lithuania.

33 Criminal Code of the Republic of Lithuania. *Official Gazette*. 1961, No. 18-147.

34 For more about data and information see: Sabaliauskas, G. Informacijos saugumas internete: teisininkų ir informatikų problema. [Information safety on the Internet: a problem of lawyers and information technology specialists]. *Justitia*. 2001, 1: 28.

35 Pavilionis, V., *et al. Baudžiamoji teisė. Specialioji dalis.* Pirmoji knyga. Antrasis leidimas [Criminal Law. Special Part. Book 1. 2nd ed.]. Vilnius: Eugrimas, 2001, p. 401–402.

36 What regards swindling, Article 182 of the Criminal Code of the Republic of Lithuania reads as follows:
1. A person who, by deceit, acquires another's property for own benefit or for the benefit of other persons or acquires a property right, avoids a property obligation or annuls it shall be punished by community service or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to three years.
2. A person who, by deceit and for own benefit or for the benefit of other persons, acquires another's property of a high value or a property right or the valuables of a considerable scientific, historical or cultural signifi-

In contrast to the Lithuanian choice, Article 8 of the Convention has set out a clear obligation for Lithuania to criminalize 'computer-related fraud' as a specific type of fraud.[37] The Convention Explanatory Report points out to fraud, including credit card fraud. It is therefore important to emphasize that Article 207 of the CC establishes a provision on 'Credit Fraud', but its contents appear unrelated to credit card fraud: '[a] person who, by deceit, obtains a credit, loan, subsidy, warranty or bank guarantee statement or another credit obligation...'[38]. In conclusion, only credit card forgery is criminalized *expressis verbis*.[39] Obviously, separate criminalization of computer-related fraud would eliminate possible discussions regarding the scope of application of the general 'swindling' provision. In the meantime, prosecutors and courts apply Article 182 against offenders using a computer as a tool for fraudulent activities of any kind.

3.7. Successful Criminalization of Child Pornography

Separate criminalization of child pornography was the most important obligation set for the signatory states of the Convention. Article 9 of the Convention obliges the signatory states to criminalize 'Offenses related to child pornography'.[40]

---

cance or avoids a property obligation of a high value or annuls it or swindles by participating in an organised group shall be punished by imprisonment for a term of up to eight years.
3. A person who, by deceit and for own benefit or for the benefit of other persons, acquires another's property of a low value or acquires a property right, avoids a property obligation of a low value or annuls it shall be considered to have committed a misdemeanour and shall be punished by community service or by a fine or by restriction of liberty or by arrest...

37 Article 8 of the Convention on Cybercrime:
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a) any input, alteration, deletion or suppression of computer data,
b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

38 Article 207 of the Criminal Code of the Republic of Lithuania.

39 See Articles 214–215 of the Criminal Code of the Republic of Lithuania.

40 Article 9 of the Convention on Cybercrime:
1. 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 following conduct:
a) producing child pornography for the purpose of its distribution through a computer system;
b) offering or making available child pornography through a computer system;
c) distributing or transmitting child pornography through a computer system;
d) procuring child pornography through a computer system for oneself or for another person;
e) possessing child pornography in a computer system or on a computer-data storage medium.
(2) For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
a) a minor engaged in sexually explicit conduct;
b) a person appearing to be a minor engaged in sexually explicit conduct;
c) realistic images representing a minor engaged in sexually explicit conduct.
3) For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Article 162(1) of the new CC stipulates criminal liability for the use of a child for pornography.[41] Initially, under the new CC, a legal person was not held liable for child pornography; however, in subsequent amendments, the liability of legal persons was established. The liability for such a crime can be applied only for those directly involved in the production of child pornography: photographer, cameraman and similar individuals. Criminal liability for the dissemination and storage of child pornography was provided for in Article 309 of the new CC[42]:

2. A person who produces, acquires, stores, demonstrates, advertises or distributes pornographic material displaying a child or presenting a person as a child shall be punished by a fine or by imprisonment for a term of up to two years.

3. A person who, for the purpose of distribution, produces or acquires or distributes a large quantity of pornographic material displaying a child up to ten years shall be punished by imprisonment for a term of up to five years...[43]

In general, the Lithuanian legislator has not left any gaps regarding the criminalization of child pornography.

3.8. No New Regulation of Copyright Crimes

Crimes against intellectual and industrial property have been criminalized in all editions of the Lithuanian CC including the current one and, therefore, did not require any modification compared the old CC and the articles remained almost unchanged.[44] These provisions meet Article 10 of the Convention which has set out the obligation of the signatory states to criminalize 'offences related to infringements of copyright and related rights'.[45] The punishments for these crimes do not exceed one to three years of

41 Article 162 of the Criminal Code of the Republic of Lithuania (n. 1): 'A person who involves a child in pornographic events or uses a child for the production of pornographic material or gains profit from such activities of the child shall be punished by a fine or by arrest or by imprisonment for a term of up to five years.'

42 Article 309 of the Criminal Code of the Republic of Lithuania:
1. A person who, for the purpose of distribution, produces or acquires pornographic material or distributes such material shall be punished by community service or by a fine or by restriction of liberty or by imprisonment for a term of up to one year.
2. A person who produces, acquires, stores, demonstrates, advertises or distributes pornographic material displaying a child or presenting a person as a child shall be punished by a fine or by imprisonment for a term of up to two years.
3. A person who, for the purpose of distribution, produces or acquires or distributes a large quantity of pornographic material displaying a young child shall be punished by imprisonment for a term of up to five years.
4. A person who demonstrates or advertises pornographic material shall be considered to have committed a misdemeanour and shall be punished by community service or by a fine or by restriction of liberty or by arrest.
5. A legal entity shall also be held liable for the acts provided for in paragraphs 1, 2 and 3 of this Article.

43 Article 309(2, 3) of the Criminal Code of the Republic of Lithuania.

44 Chapter XXIX of the Criminal Code of the Republic of Lithuania: 1) misappropriation of authorship (Article 191); 2) unlawful reproduction of a literary, scientific, artistic or other creative work, distribution, transportation or storage of illegal copies (Article 192); 3) destruction or alteration of information about management of author's rights or related rights (Article 193); 4) unlawful removal of technical protection means of author's rights or related rights (Article 194).

45 Article 10 of the Convention on Cybercrime:
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal

imprisonment which is in general less severe than the punishments for 'crimes against informatics'.

Conclusions

The Convention is the main international legislative tool in the fight against cybercrime signed by 46 countries, 26 of which have already ratified it by 1 February 2010. Lithuania obliged itself to be bound by the Convention on 23 June 2003. The Convention was ratified by the Lithuanian Parliament on 18 March 2004 and entered into force on 1 July 2004. One of the major goals ahead of the Lithuanian legislature after taking this step was a move forward by transposing the provisions of the international treaty into the local laws. Needless to say, not all of the concepts addressed in the Convention had already been regulated in Lithuania, which showed first attempts to criminalize certain computer-related activities as early as in 1994. The criminalization was further elaborated by adopting the new CC in 2000 which entered into force on 1 May 2003. It introduced a number of new cybercrimes into the Lithuanian legal system; however, such illegal activities under the Convention as access and misuse of devices had to wait for another amendment to be criminalized. Among the first offences under the Convention criminalized in Lithuania were intellectual property crimes. There was almost no need to modify this regulation anymore. On the other hand, such Internet-related crimes as child pornography had to be transferred to the Lithuanian criminal law. Unfortunately, some of the cybercrimes such as computer-related forgery in respect of credit cards remain outside the scope of the Lithuanian CC even after the last series of amendments.

In conclusion, Lithuania has basically implemented all requirements of the Convention. The remaining problems concern insufficient criminalization of computer-related forgery and fraud.

---

offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

References

Adoption of Convention on Cybercrime. *International Journal of International Law*. 2001, 95(4).

Aldesco, A. The demise of anonymity: a constitutional challenge to the Convention on Cybercrime. *Entertainment Law Review*. 2002, 23(81).

Broadhurst, R. Development in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management*. 2006, 29(3).

Burda, R.; Gudmonas, S. Modernios technologijos – modernūs nusikaltimai [Modern technologies – modern crimes]. *Justitia*. 1998, 4.

Council of Europe Convention on Cybercrime (adopted 23 November 2001, entered into force 7 January 2004). CETS No. 185.

Criminal Code of the Republic of Lithuania. *Official Gazette*. 1961, No. 18-147.

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

Explanatory Report to the Convention of Cybercrime [interactive]. [accessed 20-12-2010]. <http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm>.

Gercke, M. The slow awake of a global approach against cybercrime. *Computer Law Review International*. 2006, 141.

Gercke, M. National, regional and international approaches in the fight against cybercrime. *Computer Law Review International*. 2008.

Jones, J. *The Council of Europe Convention on Cybercrime, Themes and Critiques* [interactive]. 2005 [accessed 10-12-2009]. <http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf>.

Kaspersen, H. W. K. *Cybercrime and Internet Jurisdiction, Discussion paper (draft), version 5 March 2009, prepared in the framework of the Project on Cybercrime of the Council of Europe*.

Parker, D. B. *Crime by Computer*. New York: Charles Scribner's Sons, 1976.

Parker, D. B. *Fighting Computer Crime*. New York: Charles Scribner's Sons, 1983.

Pavilionis, V., *et al*. *Baudžiamoji teisė. Specialioji dalis*.pirma knyga. Antrasis leidimas [Criminal Law. Special Part. Book 1. 2nd ed.]. Vilnius: Eugrimas, 2001.

Sabaliauskas, G. Informacijos saugumas internete: teisininkų ir informatikų problema [Information safety on the Internet: a problem of lawyers and information technology specialists]. *Justitia*. 2001, 1.

Sofaer, A. D.; Goodman, S. E. *Toward an International Convention on Cybercrime. The Transnational Dimension of Cyber Crime and Terrorism*. Stanford: Hoover Institution Press, 2001.

ELEKTRONINIŲ NUSIKALTIMŲ REGLAMENTAVIMAS LIETUVOJE: REGULIAVIMO TOBULINIMAS IR TEISINĖS SPRAGOS PALYGINTI SU KONVENCIJA DĖL ELEKTRONINIŲ NUSIKALTIMŲ

Darius Sauliūnas

Mykolo Romerio universitetas, Lietuva

Santrauka. *Tarptautiniu lygiu elektroninius nusikaltimus reglamentuoja Europos Tarybos iniciatyva parengta Konvencija dėl elektroninių nusikaltimų, priimta Budapešte 2001 m. rudenį. Jos poreikis grįstas tuo, jog informacinėms technologijoms sparčiai vystantis, nusikaltėliams darosi vis paprasčiau įvaldyti naujus nusikaltimų padarymo būdus, o įstatymų leidyba labai atsilieka dėl skirtingų požiūrių į nusikaltimus elektroninėje erdvėje, įvairių valstybių nacionalinės teisės ypatumų, ir apibrėžiant patį nusikaltimą, ir nesutariant dėl jo užkardymo veiksmų. Konvenciją pasirašiusios šalys įsipareigojo nacionaliniais teisės aktais pripažinti nusikalstamomis veikomis joje numatytus veiksmus, taip pat nustatyti juridinių asmenų atsakomybę už šių veikų padarymą. Lietuvoje buvo itin svarbu laiku nustatyti atsakomybę už pavojingas nusikalstamas veikas, padaromas pasinaudojant kompiuteriais, viešaisiais tinklais ir panašiomis informacinėmis technologijomis, o tai ir buvo padaryta priėmus atitinkamus Lietuvos Respublikos baudžiamojo kodekso pakeitimus. Apskritai vertinant Lietuvos įstatymų leidėjas tinkamai į nacionalinę teisę perkėlė Konvencija prisiimtus įsipareigojimus. Vis dėlto lyginamoji Konvencijos ir Baudžiamojo kodekso analizė parodė, kad šiame procese buvo palikta tam tikrų teisinio reguliavimo spragų, į kurias reikia atkreipti dėmesį, pavyzdžiui, reikia tobulinti sukčiavimo, pasitelkiant kompiuterių tinklus, reglamentavimą.*

Reikšminiai žodžia*i: elektroniniai nusikaltimai, Konvencija dėl elektroninių nusikaltimų, internetiniai nusikaltimai, Lietuvos Respublikos baudžiamasis kodeksas.*

Darius Sauliūnas, Mykolo Romerio universiteto Teisės fakulteto Tarptautinės ir Europos Sąjungos teisės katedros lektorius, socialinių mokslų daktaras. Mokslinių tyrimų kryptys: tarptautinė informatikos teisė, ES informacinės visuomenės reglamentavimas, domenų vardų ginčų sprendimas.

Darius Sauliūnas, Mykolas Romeris University, Faculty of Law, Department of International and Eeuropean Union Law, lecturer, doctor of social sciences. Research interests: international informtics law, information society regulation in EU, domain name dispute resolution.