ISSN 1392–6195 (print)
ISSN 2029–2058 (online)
JURISPRUDENCIJA
JURISPRUDENCE
2011, 18(2), p. 689–702.

DYNAMICS OF CRIMES AGAINST THE SECURITY OF ELECTRONIC DATA AND INFORMATION SYSTEMS, AND ITS INFLUENCE ON THE DEVELOPMENT OF ELECTRONIC BUSINESS IN LITHUANIA

Tatjana Bilevičienė

Mykolas Romeris University, Faculty of Economics and Finance Management,
Department of Business Economics
Ateities 20, LT-08303 Vilnius, Lithuania
Telephone (+370 5) 271 4733
E-mail tbilev@mruni.eu

Eglė Bilevičiūtė

Mykolas Romeris University, Faculty of Law,
Department of Administrative Law and Procedure
Ateities 20, LT-08303 Vilnius, Lithuania
Telephone (+370 5) 271 4545
E-mail eglek@mruni.eu

Received 19 April, 2011; accepted 18 June, 2011

Abstract. *The development of an information society and information technologies does not result in positive consequences only. Individuals with criminal intent also find their niche. Information security includes the creation of the input, processing and output processes of protection. The objective of information security is to protect the system of values, to protect and ensure accuracy and integrity and to minimize losses that may be incurred if the information is modified or destroyed. In the development of an information society, the new visible changes in the legislation for the classification of crimes–crimes against computers–altered the concept of electronic crime data and information system security concepts. This article presents a brief analysis on the concept of the change of crimes against security of*

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

electronic data and information systems, the legislation analysis, the crimes against security of electronic data systems and information dynamics and its relationship with business factors.

Keywords: *information technologies, crimes, computer crimes, information security, security of electronic data and information systems, e-commerce.*

Introduction

Today, along with the traditional flow of information, electronic information has become more important. Electronic information is created, managed, stored and transmitted using fast changing information technology. It is therefore an important problem in electronic information storage, retrieval and long-term opportunities, the use of information; it has a direct impact on the investigation of crimes committed in a specific environment. Investigators in criminal acts are facing a new phenomenon–cyber crimes that are changing the settled law of criminal investigation and working methods. Computer crimes are described here in order to understand how criminal law provides the public with a dangerous act, which is computerized information or criminal attacks on a tool or object[1].

Computer and electronic information networks are increasingly used for a variety of crimes, from unauthorized access to pornographic content, in particular concerning the portrayal and distribution of images of minors. These criminal activities are special in that they create a completely new and a virtual international space–in cyberspace. The variety of criminal offenses has forced states to unite in the fight against such crimes.

Much has been made of the capabilities to commit a crime that has a digital component, whether it is hacking, fraud, embezzlement, identity theft, organized crime, child pornography, or any other criminal act. While the capabilities of the perpetrators and the response of IT professionals are often discussed, what is often overlooked is the ability of law enforcement to investigate and prosecute digital crime. An information security plan that is not developed with prosecution as a possible outcome is short sighted[2].

1. Development of the Definition of Crimes against Security of Electronic Data and Information Systems in Lithuanian Law

The Commission of the European Communities Communication *Towards a General Policy on the Fight against Cyber Crime*[3] states that the security of the increasingly

1 Stračinskij, M. Kompiuterinių nusikaltimų pėdsakai: samprata, rūšys ir jų susidarymo mechanizmas [Trace-Evidence in Computer-Related Crimes: Conception, Types and Formalion. Jurisprudence]. *Jurisprudencija. Mokslo darbai*. 2006, 11(89): 50–56.

2 Nykodym, N.; Taylor, R.; Vilela, J. Criminal profiling and insider cyber crime. *Computer Law & Security Report*. 2005, 21(5): 408−414.

3 Commission of the European Communities. 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 COM(2007) 267 final [interactive]. Brussels, 22.5.2007. [accessed 01-12-2010] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.

important information systems in our society covers many aspects, of which the fight against cyber crime is a core element. Without an agreed definition of cyber crime, the terms *cyber crime*, *computer crime*, *computer-related crime*, or *high-tech crime* are often used interchangeably. For the purpose of this Communication, *cyber crime* is understood as *criminal acts committed using electronic communications networks and information systems or against such networks and systems*.

In practice, the term *cyber crime* is applied to three categories of criminal activities. The first covers traditional forms of crime such as fraud or forgery, though in a cyber crime context relates specifically to crimes committed over electronic communication networks and information systems. The second concerns the publication of illegal content over electronic media (child sexual abuse material or incitement to racial hatred). The third includes crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking. These types of attacks can also be directed against the crucial critical infrastructures in Europe and affect existing rapid alert systems in many areas, with potentially disastrous consequences for the whole society. Common to each category of crime is that they may be committed on a mass-scale and with a great geographical distance between the criminal act and its effects.[4]

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, phishing, spam and malicious codes may be used to commit large scale fraud. Illegal national and international Internet-based trade has also emerged as a growing problem. This includes trade in drugs, endangered species and arms.

Large scale attacks against information systems or organizations and individuals (often through so called botnets) appear to have become increasingly prevalent. Also, incidents with systematic, well coordinated and large-scale direct attacks against the critical information infrastructure of a state have recently been observed. This has been compounded by the merging technologies and accelerated interlinking of information systems, which rendered those systems more vulnerable. Attacks are often well organized and used for the purpose of extortion.

There are two key performance technologies of computer crime categories[5]: fraud (unauthorized information in the introduction, manipulation allowed for input of information, manipulation of files with incorrect information or the use of unauthorized files with information creation, internal bypass security measures) and abuse (as computers, software, information and equipment theft, unauthorized information, the introduction of unauthorized files with information creation, computer programs, not intended for official use, creation, manipulation or incorrect use of options, which enable computers to do any work).

4 *Supra* note 3.

5 Nusikaltimai ir piktnaudžiavimai [Crimes and Abuses] [interactive]. [accessed 29-12-2010] <http://www.straipsniai.lt/Kompiuterinis_saugumas/puslapis/8184>.

The Federal Bureau of Investigations (USA) recognizes four instances of cyber crime[6]:

1. Cyber crimes against children (usually involving child pornography or child rape).
2. Theft of intellectual property.
3. Publication and intentional dissemination of malware.
4. National and international Internet fraud.

Effective law enforcement authorities often depend at least partially harmonized definitions of crimes. Convention on Cyber Crime[7] (Cybercrime Convention on Chapter II—Measures To Be Taken at the national level), Chapter II—Measures to be taken at the state level, introducing a classification of computer crime: offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices), computer-related offences (computer-related forgery, computer-related fraud), content-related offences, offences related to infringements of copyright and related rights.

The European Convention on Cybercrime, signed and ratified by the State, requires its national law to be in line with conventional provisions criminalizing a whole range of offenses, and arranging the procedural steps for investigation of specific criminal acts, is applied.

In the Republic of Lithuania, cyber security and legal protection of the interest in well behind the technological development of telecommunications processes. Crimes on information technology–*crimes on electronic data and information systems security*–were criminalized in Lithuania in 2000, after adopting the new Republic of Lithuania Criminal Code[8] (CC). This code was introduced in Chapter XXX of Crime, which consisted of three items: Art. 196, Computer Information destruction or amendment; Art. 197, Computer software destruction or modification; and Art. 198, Computer utilization and dissemination of information. This section was constructed in pursuance of the Convention on Cybercrime of offenses described in the model. On 24 January 2004, amendments were made and two new articles were added to this Chapter, namely *Art. 198(1), Illegal access to a computer or a computer network* and *Art. 198(2), Illegal possession of hardware, software, passwords, log-in codes or other data, intended for the committing of crime*. In June 2007, a package of amendments to Chapter XXX of the CC was adopted, whereby the Chapter was renamed to *Crimes against security of electronic data and information systems* and the shortcomings of existing laws were corrected. It was amended in the title and content: *Art. 196 Unlawful Influence on Electronic Data* (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)*, Art. 197, Unlawful Influence on an Information System* (unlawfully

6 FBI Definition of Cyber Crime [interactive]. [accessed 31-01-2011]. <http://www.brighthub.com/internet/security-privacy/articles/65042.aspx>.

7 Konvencija dėl elektroninių nusikaltimų [The Convention on Cybercrime]. Official Gazette. 2004, No. 36.

8 The Criminal Code of the Republic of Lithuania. *Official Gazette*. 2000, No. 74 – 2262, with further amendments and supplements.

disturbs or terminates the operation of an information system thereby incurring major damage)*, Art. 198, Unlawful Interception and Use of Electronic Data* (unlawfully observes, records, intercepts, acquires, stores, appropriates, distributes or otherwise uses the electronic data which may not be made public)*, Art. 198(1), Unlawful Connection to an Information System* (unlawfully connects to an information system by damaging the protection means of the information system)*, Art. 198(2), Unlawful Disposal of Installations, Software, Passwords, Login Codes and Other Data* (unlawfully produces, transports, sells or otherwise distributes the installation of software, also passwords, login codes or other similar data directly intended for the commission of criminal acts, or acquiring and storing them for the same purpose). However, criminal acts which are currently qualified under Art. 196-198(2) of the CC had also been committed in Lithuania prior to the enactment of this law. These acts are rather specific due to their latency, the inherent character of these crimes, the personal qualities of the perpetrators, and the rapid development of information technologies. Crimes on electronic data and information systems security result in dire social and economic consequences.[9]

2. The Dynamics of Crimes against Security of Electronic Data and Information Systems

On a global scale, cyber crime has skyrocketed with the advancement of the electronic medium. While progress is being made in combating cyber crime (particularly with the Council of Europe's Convention on Cyber Crime), a large gap continues to exist in legislative compatibility across international borders. Often overlooked, in regards to profiling, is cyber crime. The idea that an individual committing crime in cyberspace can fit into a certain outline (a profile) may seem far-fetched, but evidence suggests that certain distinguishing characteristics do regularly exist in cyber criminals.[10]

Statistics of crime in Lithuania is presented in the portal for Centre for Crime Prevention in Lithuania.[11] Compared to other criminal acts stipulated in the CC, statistical indicators for crimes against security of electronic data and information systems are not very high due to their latency (see Table 1).

9 Novikoviene, L.; Bileviciute, E. Application of IT Examination in Investigation of Crimes on Safety of Electronic Data and Information Systems. *Jurisprudence*. 2010, 1(119): 317–329.

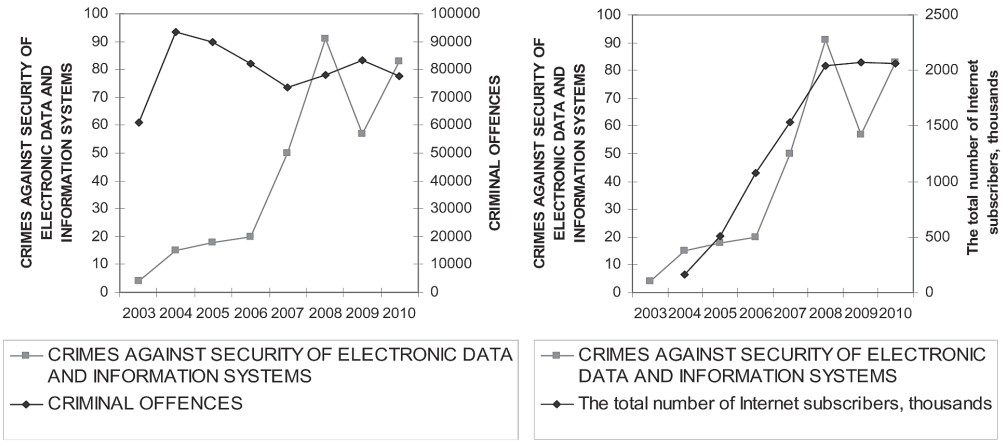
10 Gogolin, G.; Jones, J. Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business. *Information Security Journal: A Global Perspective.* 2010, 19(3): 109−117.

11 Centre for Crime Prevention in Lithuania. Automated Statistical Information System [interactive]. [accessed 31-01-2011] <http://www.nplc.lt:8000/asis/>.

1 Table. Crimes against security of electronic data and information systems[12]

	2003	2004	2005	2006	2007	2008	2009	2010
Article 196. Unlawful Influence on Electronic Data	2	4	1	2	4	10	8	7
Article 197. Unlawful Influence on an Information System		2		2	3	7	1	7
Article 198. Unlawful Interception and Use of Electronic Data	2	7	6	10	11	72	32	55
Article 198(1). Unlawful Connection to an Information System		1	10	6	30	2	9	10
Article 198(2). Unlawful Disposal of Installations, Software, Passwords, Login Codes and Other Data		1	1		2		7	4
Crimes against Security of Electronic Data and Information Systems	4	15	18	20	50	91	57	83

In findings of these types of crime, recorded in 2003, there were only four and a maximum number of these offenses shall not exceed one hundred. It should also be borne in mind that if a person uses information technology to commit the offense, the offense may be qualified under other articles of the Lithuanian Criminal Code. These criminal acts have completely different dynamics with common crime, criminal behavior (see Figure 1).



1 Figure. Dynamics of criminality and dynamics of Internet's development

12 Centre for Crime Prevention in Lithuania, *supra* note 11.

The total number of recorded criminal acts, 2004–2007 decreased steadily from 2008, had started to grow again, and again decreased in 2010. This is easy to explain, since economic stability during is decreasing as well, but in times of crisis–is increasing[13]. Crimes against security of electronic data and information systems from 2003 to 2008 continued to grow, extremely fast in 2006–2007, and in 2009 decreased, but only temporarily. 2010 again tended to increase the number of crimes. This indicates that this is a specific offense; it is developing in a stable economic and financial environment for media, because their realization requires complex technology (information technology, computers and computer networks, the Internet) and a sufficiently high level of skill and priests. Also, crime is the subject of a high-level information technology, a broader application of the stable economic development in time.[14]

The increase of the rate of crimes against security of electronic data and information systems is primarily related to the development of information technology in Lithuania (see Table 2). It may be noted that the present period shows a rapid growth in Lithuania of computers and the Internet. In 2010, households owning a personal computer and having Internet access was higher than 50%, and the use of information technology companies for banking and financial services exceeded 90%. Crimes against security of electronic data systems and information dynamics are analogous to the total number of Internet subscriber dynamics (see Figure 1).

However, based on the the number of registered crimes, classified according to each section of this article, the dynamics vary (see Figure 2). The dynamics of criminal offences (*Art. 196 Unlawful Influences on Electronic Data, Art. 197 Unlawful Influences on an Information System, Art. 198 Unlawful Interception and Use of Electronic Data)* is similar to crimes against security of electronic data and information systems in similar dynamics *($r = 0.91$, $r = 0.82$, $r = 0.92$, $p = 0.000$*, very strong and powerful positive correlation). This can be explained by the fact that these crimes are similar by nature; their development is also linked to the IT development. *Unlawful Interception and Use of Electronic Data* criminal offences decreased in 2010, despite the continuation of Crimes against Security of Electronic Data and Information Systems of successful growth can be explained by the introduction of data protection systems.

13 Justickis, V. *Kriminologija. 1 dalis*. [Criminology, I part]. Vilnius: LTU, 2001.

14 Kiškis, M.; Petrauskas, R.; Rotomskis, I.; Štitilis, D. *Teisės informatika ir informatikos teisė: vadovėlis* [Legal Informatics and Law of Informatics: handbook]. Vilnius: Mykolo Romerio universitetas, 2006.

2 Table. IT development in Lithuania[15]

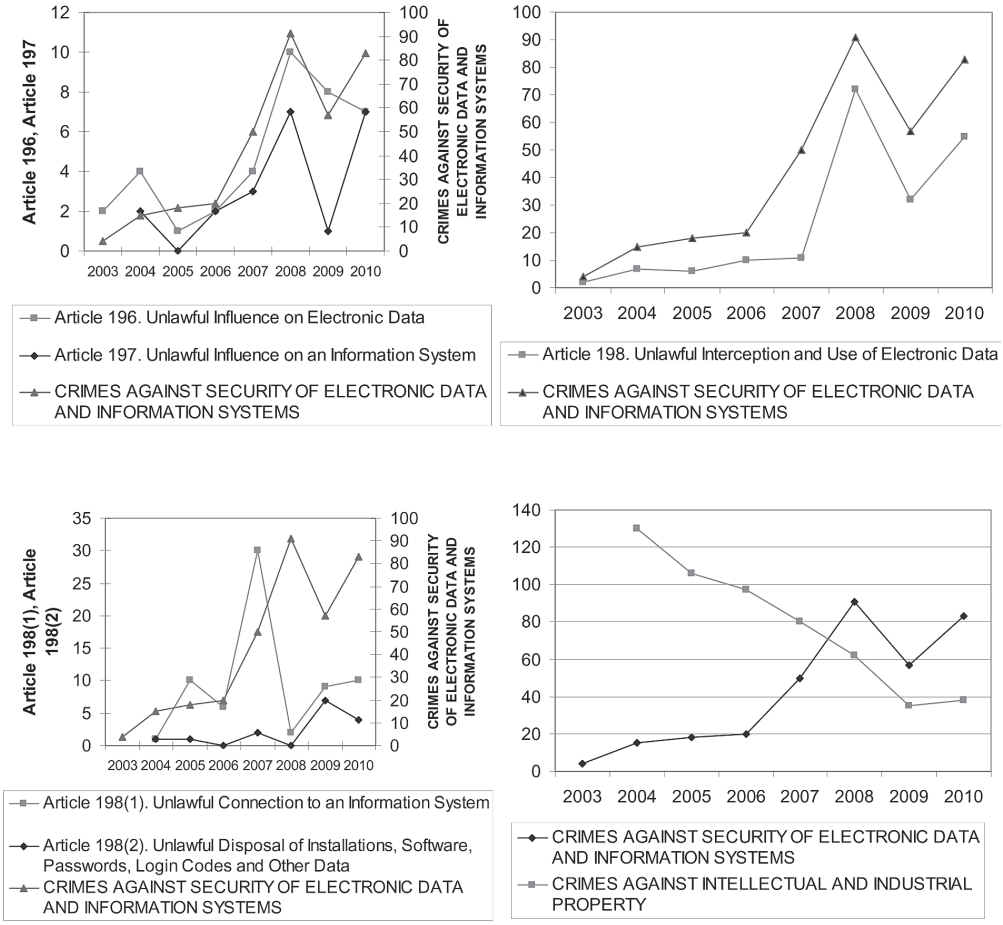
IT index	2004	2005	2006	2007	2008	2009	2010
Households with a PC, %	25	29	36,5	42	48	52,2	53,8
Households with Internet access, %	10,6	14,4	31,7	40,3	47,1	54,7	54,9
Population use the Internet for banking and financial services, %	3,5	6,7	10,3	14,7	21,0	27,2	32,4
The total number of Internet subscribers, thousands	161,4	512,2	1078,7	1533,6	2045,6	2070,5	2065,6
Companies that sell goods or services by e-networks, by percents	5,8	14,5	14,2	22,9	20,0	21,9	
Use of information technology in companies: for banking and financial services, by percentages	76,8	82,1	83,1	89,8	92,6	92,9	

Dynamics of criminal offences *(Art. 198(1) Unlawful Connection to an Information System, Art. 198(2) Unlawful Disposal of Installations, Software, Passwords, Login Codes and Other Data)* is similar, but differed from the crimes against security of electronic data and information systems dynamics. TThese criminal activities are more related to technological factors; the number of periodic variation increases when the criminals are adapting new technologies in the offense, then decreases, some enterprises, institutions, banks put in place the prevention of technical (software) tools. The part of companies that have problems in e-safety[16] showed in 2009 a sharp decline, a decrease in crimes against security of electronic data and information systems (see Figure 3).

It is interesting to compare crimes against security of electronic data and information systems and crimes against intellectual property and industrial dynamics (see Figure 2). The specific number of offenses are similar in scale, while an opposite ($r = \neg\ 0.77$, $p = 0.000$, a strong negative correlation). Only since 2008, the dynamics of these crimes are the same. It can be argued that by 2008 did not clearly understand the difference between these crimes have not been precisely determined based information, applications, databases, copyright infringement. This was done in the 2007 version of this chapter. Statistical analysis shows the impact of the CC change.

15 Statistics Lithuania. Statistics (pre-defined tables) [interactive]. [accessed 10-01-2011]. <http://www.stat.gov.lt/en/pages/view/?id=1349>.

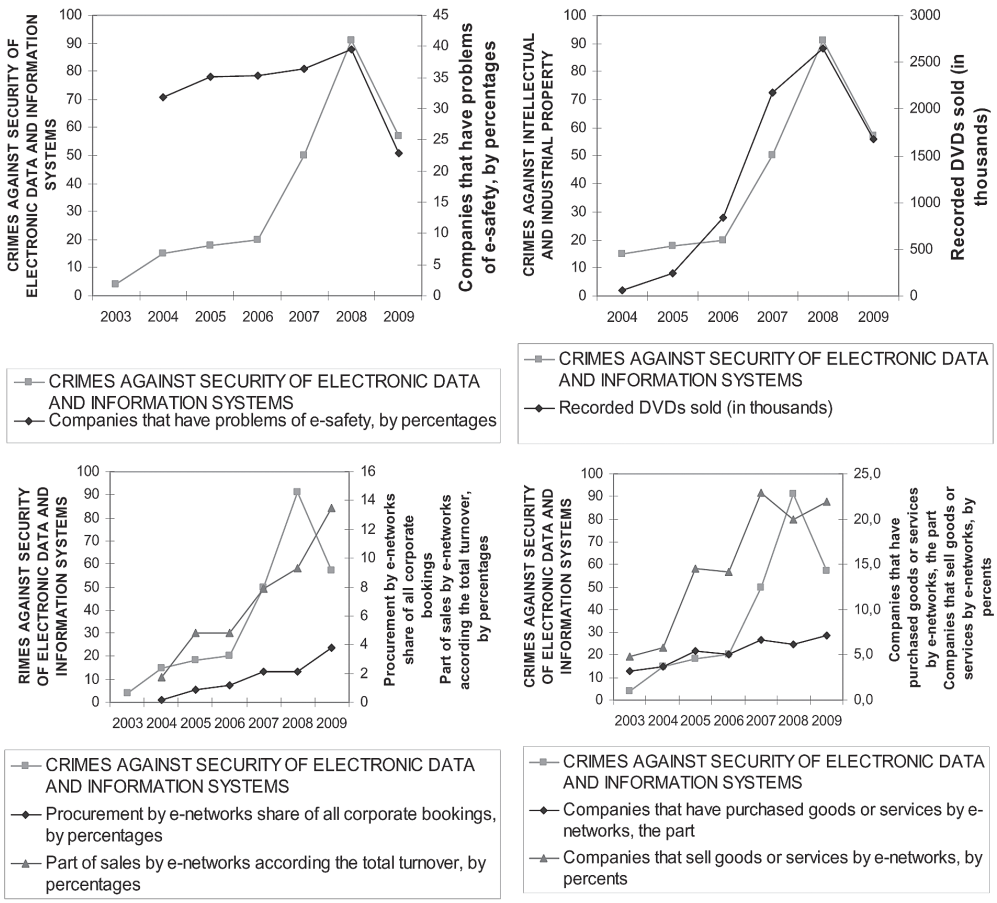
16 *Ibid*.



2 Figure. Dynamics of crimes against security of electronic data and information systems and crimes against intellectual and industrial property

3. Crimes against Security of Electronic Data and Information Systems and E. Business Factors Internship

The numbers of people who are interacting via computer networks are growing rapidly. Computer networks provide a framework for electronic business. The evolution of e-business or the uptake of e-business practices has become popular in depicting a process involving transitions toward increasing use of ICT coupled to organizational change and sophistication which can impact business performance. E-business infrastructure is part of an overall information technology infrastructure, hosting and e-business processes are carried out in e-commerce transactions.



3 Figure. Relationship of crimes against security of electronic data and information systems and e. business factors

E-commerce, which is defined as business transactions, and the business organization of the use of information technology data network environment may be many activities for profit—selling, marketing, distance learning, tele-working, banking, etc. E-business goes beyond the normal business operations, but also new, possible only in a virtual environment for business methods. Electronic commerce is buying and selling electronically, particularly via the Internet. Some of the newest, most easily implemented Internet technology, is ideal for e-commerce.

Crimes against security of electronic data and information systems result in dire social and economic consequences. Their development directly related to information technology development companies, e trade, etc. A successful e-business is subject to ongoing security operations. Statistical analysis shows crimes against security of electronic data and information systems and the companies that have problems of e-safety dynamic similarity (see Figure 3).

We could establish the relationship between the part of companies that have purchased goods or services by e-networks, the part of companies that sell goods or services by e-networks and crimes against security of electronic data and information systems (*r = 0,75, r = 0,79, p = 0,000,* strong positive correlation), relationship among the part of procurement by e-networks share of all corporate bookings, the part of sales by e-networks according the total turnover and crimes against security of electronic data and information systems (*r = 0,67, r = 0,74, p = 0,000,* strong positive correlation) (see 3 Figure). This shows that e business development is not adequately protected against cyber crime.

Computer networks allow copying and distribution of various authors' work much easier than ever before, as far as specific features of computer communication have been reviewing and redefining the scope of protection of copyrights. There are two major copyright infringement cases according to the sort of information attacks by computer networks. The first case is called software piracy, and the second relates to other types of copyright works (in the broad sense of the word), and publication of embezzlement. For example, the crimes against security of electronic data and information systems and closed DVDs sold[17] correlation was positive and very strong (*r = ¬ 0.99, p = 0.000*) (see Figure 3). This gives grounds to suspect that there was an attempt to realize a large quantity of pirated products.

Offences related to infringements of copyright and related rights are increasingly taking place in cyberspace, and therefore treated as a computer crime. Therefore, policies designed to combat cyber crime initiatives are known as the *Electronic Commerce Directive.*[18]

Lithuanian *National Crime Prevention and Control Programme*[19] states that Lithuania committed more crimes, which were previously rare: kidnapping, human trafficking, computer crimes and more. It is necessary to improve the legal, administrative willingness to disclose and investigate the economic and financial crimes carried out by using the computer, telecommunications, and counterfeit credit cards, to enhance interagency and international cooperation. However, the European Commissions Communication[20] states that the private and public sectors together develop an interest in criminal acts and this damages detection methods and techniques designed to prevent such damage. Total public and private sector participation, which is based on mutual trust and common purpose of reducing the damage, may be an effective way to enhance security, and combating cyber crime. Particular attention should be given training on cyber crime issues.

---

17 Statistics Lithuania. Statistics (pre-defined tables) [interactive]. [accessed 10-01-2011] <http://www.stat.gov.lt/en/pages/view/?id=1349>.

18 Directive 2000/31/EC of the European Parliament and of the Council of of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [interactive]. [accessed 31-01-2011] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF>.

19 Dėl nacionalinės nusikaltimų prevencijos ir kontrolės programos patvirtinimo. Lietuvos Respublikos Seimo nutarimas Nr. IX-1383 2003 m. kovo 20 d. [Concerning the national crime prevention and control programs. Resolution of the Seimas of the Republic of Lithuania Nr. IX-1383 2003 03 20]. *Official Gazette*. 2003, No. 32-1318.

20 *Supra* note 3.

There is a public-private exchange of information, with the specific knowledge and lack of best practice. Private sector entities, in order to protect business secrets and patterns, are often unwilling to provide relevant information to law enforcement authorities with regard to the prevalence of crime. However, such information may be necessary in order that the state authorities establish effective and appropriate policies for the fight against crime.

Conclusions

In Lithuania for the first time crimes which are subject to very specific computerized information and information technology in the legislature have been identified as socially dangerous acts in the new Criminal Code, which was adopted in 2000. However, by 2007 the name of the offense, and skills were improved. This complicates the determination of the number of acts as an information technology replaces only part of such offenses as fraud, theft, copyright infringement.

Statistical data shows constant crimes against security of electronic data and information systems growth. This can be linked to ICT development in Lithuania, as well as the CC and 196-198 (2) development of contents. These temporary reduction in the number of crimes in 2009 better explain how hardware and software protection application, so the economic situation worsening crisis.

You can set the crimes against security of electronic data and information systems to e business factors, primarily because the cyber crimes occur in e-commerce and e banking fields.

Lithuanian *National Crime Prevention and Control program* forecasts the prevention of computer crimes, but the main focus is on consular officials. In view of the European Commission's opinion, it is necessary to provide additional public and private sectors, including civil society organizations, the cooperation strategy for combating cyber crimes. Particular attention should be given to training on issues of cyber crime and online security.

References

Centre for Crime Prevention in Lithuania. Automated Statistical Information System [interactive]. [accessed 31-01-2011] <http://www.nplc.lt:8000/asis/>.

Commission of the European Communities. 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 COM(2007) 267 final [interactive]. Brussels, 2007 [accessed 01-12-2010] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.

Dėl nacionalinės nusikaltimų prevencijos ir kontrolės programos patvirtinimo. Lietuvos Respublikos Seimo nutarimas Nr. IX-1383 2003 m. kovo 20 d. [Concerning the national crime prevention and control programs. Resolution of the Seimas of the Republic of Lithuania No. IX-1383 2003 03 20]. *Official Gazette*. 2003, No. 32-1318.

Directive 2000/31/EC of the European Parliament and of the Council of of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on elec-

tronic commerce) [interactive]. [accessed 31-01-2011]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF>.

FBI Definition of Cyber Crime [interactive]. [accessed 31-01-2011]. <http://www.brighthub.com/internet/security-privacy/articles/65042.aspx>.

Gogolin, G.; Jones, J. Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business. *Information Security Journal: A Global Perspective.* 2010, 19(3): 109−117.

Justickis, V. *Kriminologija. 1 dalis* [Criminology, I part]. Vilnius: LTU, 2001.

Kiškis, M.; Petrauskas, R.; Rotomskis, I.; Štitilis, D. *Teisės informatika ir informatikos teisė: vadovėlis* [Legal Informatics and Law of Informatics: handbook]. Vilnius: Mykolo Romerio universitetas, 2006.

Konvencija dėl elektroninių nusikaltimų [The Convention on Cybercrime]. *Official Gazette*. 2004, No. 36.

Nykodym, N.; Taylor, R.; Vilela, J. Criminal profiling and insider cyber crime. *Computer Law & Security Report*. 2005, 21(5): 408−414.

Novikoviene, L.; Bileviciute, E. Application of IT Examination in Investigation of Crimes on Safety of Electronic Data and Information Systems. *Jurisprudence*. 2010, 1(119): 317–329.

Nusikaltimai ir piktnaudžiavimai [Crimes and Abuses] [interactive]. [accessed 29-12-2010]. <http://www.straipsniai.lt/Kompiuterinis_saugumas/puslapis/8184>.

Statistics Lithuania. Statistics (pre-defined tables) [interactive]. [accessed 10-01-2011]. <http://www.stat.gov.lt/en/pages/view/?id=1349>.

Stračinskij, M. Kompiuterinių nusikaltimų pėdsakai: samprata, rūšys ir jų susidarymo mechanizmas [Trace-Evidence in Computer-Related Crimes: Conception, Types and Formalion]. *Jurisprudencija. Mokslo darbai*. 2006, 11(89): 50–56.

The Criminal Code of the Republic of Lithuania. *Official Gazette*. 2000, No. 74 – 2262, with further amendments and supplements.

NUSIKALTIMŲ ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ SAUGUMUI KAITA IR TO ĮTAKA ELEKTRONINIO VERSLO PLĖTRAI LIETUVOJE

Tatjana Bilevičienė, Eglė Bilevičiūtė

Mykolo Romerio universitetas, Lietuva

Santrauka. *Pastebimi nauji informacinės visuomenės raidos pokyčiai teisės aktuose klasifikuojant nusikaltimus, t. y. kompiuterinių nusikaltimų bei nusikaltimų informatikai sąvokos keičiamos nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui sąvokomis. Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui – tai baudžiamojo įstatymo uždrausta visuomenei pavojinga veika, daranti žalą formuojant informacines sistemas ir naudojant informacines technologijas, saugant svarbią informaciją (duomenis) ir subjektų, dalyvaujančių informacinėje veikloje, interesus. Europos Tarybos 2001 m priimta Budapešto konvencija skirta stabdyti veiksmus, nukreiptus prieš kompiuterinių sistemų, tinklų ir duomenų konfidencialumą, vientisumą ir prieinamumą. Lietuva prie šios konvencijos prisijungė 2004 metais. Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui – tokia nusikalstamos veikos sąvoka nuo 2007 liepos 21 d. yra įtvirtinta dabar galiojančiame Lietuvos Respublikos baudžiamajame kodekse (BK) Dabar*

galiojančiame BK XXX skyriuje nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui yra skirstomi į tokias veikų rūšis: neteisėtas poveikis elektroniniams duomenims, neteisėtas poveikis informacinei sistemai, neteisėtas elektroninių duomenų perėmimas ir panaudojimas, neteisėtas prisijungimas prie informacinės sistemos, neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis. Reikia taip pat nepamiršti, kad jei asmuo tik naudoja informacines technologijas nusikaltimui padaryti, jo padarytą veiką galima kvalifikuoti ir pagal kitus BK straipsnius.

Straipsnyje pateikiama sąvokų kaita teisės aktuose, tiriant nusikaltimus, ir tai, kaip vienos labiausiai paplitusių sąvokų pasaulyje kompiuteriniai nusikaltimai bei nusikaltimai informatikai, dėl kurių kyla daug mokslininkų ir praktikų diskusijų, užleidžia vietą nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui sąvokai.

Statistikos duomenys rodo nuolatinį nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui augimą. Tai galima sieti ir su IT plėtra Lietuvoje, ir su BK 196–198(2) straipsnių turinio tobulinimu. Šių nusikaltimų skaičiaus laikiną mažėjimą 2009 m. galima paaiškinti ir geresnės techninės ir programinės apsaugos taikymu, ir ekonominės padėties pablogėjimu krizės metu.

Galima nustatyti nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui ir e. business veiksnių vyšį, nes kompiuteruniai nusikaltimai pirmiausia pasireiškia e. komercijos ir e. bankininkistės srytyse.

Lietuvos Nacionalinėje nusikaltimų prevencijos ir kontrolės programoje numatyta ir kompiuterinių nusikaltimų prevencija, tačiau daugiausia dėmėsio skiriama pareigūnų parengimui. Atsižvelgiant į Europos Komisijos nuomonę, reikia papildomai numatyti viešojo ir privačiojo sektorių subjektų, įskaitant pilietinės visuomenės organizacijas, bendradarbiavimo strategiją, skirtą kovai su elektroniniais nusikaltimais. Ypač daug dėmesio reikia skirti mokymui apie elektroninių nusikaltimų problemas ir elektroninę saugą.

***Reikšminiai žodžiai**: informacinės technologijos, nusikaltimai, elektroninių duomenų ir informacinių sistemų saugumui, informacijos apasauga, kompiuteriniai nusikaltimai, e. komercija.*

Tatjana Bilevičienė, Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Verslo ekonomikos katedros docentė. Mokslinių tyrimų kryptys: vadyba, informacinių technologijų taikymas teisėje ir vadyboje, matematika (statistika).

Tatjana Bilevičienė, Mykolas Romeris University, Faculty of Economics and Finance Management, Department of Business Economics, associate professor. Research interests: management, information technologies in law and management, mathematics (statistics).

Eglė Bilevičiūtė, Mykolo Romerio universiteto Teisės fakulteto Administracinės teisės ir proceso katedros profesorė. Mokslinių tyrimų kryptys: kriminalistika, administracinė teisė, mokslo ir studijų teisė, informacinių technologijų taikymas teisėje.

Eglė Bilevičiūtė, Mykolas Romeris University, Faculty of Law, Department of Administrative Law and Procedure, professor. Research interests: criminalistics, administrative law, law of science and studies, information technologies in law.