DE GRUYTER OPEN

ICLR, 2015, Vol. 15, No. 2.

Criminal Liability of Legal Persons in Case of Computer Crime: A European Union Response[1]

Libor Klimek[2]

Faculty of Law, Pan-European University, Bratislava, Slovak Republic
email: libor.klimek@paneurouni.com

KLIMEK, Libor. Criminal Liability of Legal Persons in Case of Computer Crime: A European Union Response. *International and Comparative Law Review,* 2015, vol. 15, no. 2, pp. 135–143. DOI: 10.1515/iclr-2016-0040.

Abstract: The contribution deals with the criminal liability of legal persons in case of computer crime. It is divided into three sections. The first section briefly introduces computer crime and relevant legislation of the European Union in the area of criminal law, which is the basis of that liability. While the second section is focused on provisions of criminal liability of legal persons, the third section is focused on sanctions for legal persons.

Keywords: criminal liability, legal persons, computer crime, Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment, Directive 2013/40/EU on attacks against information systems

1 Introduction

It is trite, but nonetheless true, to say that we live in a digital age. The proliferation of digital technology, and the convergence of computing and communication devices, has transformed the way in which we socialise and do business. While overwhelmingly positive, there has also been a dark side to these developments. Proving the maxim that crime follows opportunity, virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes.[3]

1 The contribution was elaborated as a part of the research project VEGA 'Súčasnosť a budúcnosť boja proti počítačovej kriminalite: kriminologické a trestnoprávne aspekty' [transl.: Present and Future of Cyber-crime: Criminological and Criminal Aspects] No. 1/0231/15.

2 Dr. et JUDr. Libor Klimek, PhD. graduated from the Faculty of Law, Pan-European University, Bratislava, Slovak Republic. Since 2013 he has been a research worker at the Criminology Research Centre at the Faculty of Law, Pan-European University in Bratislava, Slovak Republic; email: libor.klimek@paneurouni.com / libor.klimek@yahoo.com

3 Clough J (2010) Principles of Cybercrime. Cambridge University Press, Cambridge, p. 3.

ISSN 1213-8770 (print), ISSN: 2464-6601 (online).

The European Union has set itself the objective of maintaining and developing an Area of Freedom, Security and Justice. That concept has appeared as the second objective of the Treaty on the European Union.[4] The general policy objective of the European Union is to ensure a high level of security through measures to prevent and combat crime[5]. A crucial aspect of that field is criminal liability of legal persons[6].

The contribution deals with the criminal liability of legal persons[7] in case of computer crime. It is divided into three sections. The first section briefly introduces computer crime and relevant legislation of the European Union in the area of criminal law, which is the basis of that liability. While the second section is focused on provisions of criminal liability of legal persons, the third section is focused on sanctions for legal persons.

4 Article 3(2) of the Treaty on European Union as amended by the Treaty of Lisbon. Official Journal of the European Union, C 83/13 of 30th March 2010. In-depth analysis see: Blanke H J, Mangiameli S (eds) (2013) The Treaty on European Union (TEU): A Commentary. Springer, Berlin – Heidelberg, p. 157 et seq.

5 Article 67(3) of the Treaty on the Functioning of the European Union as amended by the Treaty of Lisbon. Official Journal of the European Union, C 83/47 of 30th March 2010.

6 See: Záhora J (2013) Zodpovednosť právnických osôb za trestné činy v európskej dimenzii – komparatívny prehľad. In: Jelínek J (ed) Třestní odpovědnost právnických osob v České republice – bilance a perspektivy. Conference proceedings. Leges, Praha, pp 15-27.

7 Towards criminal liability of legal persons in general see: Medelský J (2012) Trestná zodpovednosť právnických osôb, áno či nie? In Quo vadis, střední Evropo? : Metamorfózy práva III. Ústav státu a práva Akademie věd České republiky, Praha, pp 277–285; Medelský J (2012) Limity trestnej zodpovednosti právnických osôb. In: Limity práva. Leges, Praha, pp 447–456; Medelský J (2013) Od nepravej trestnej zodpovednosti právnických osôb k pravej trestnej zodpovednosti právnických osôb. Notitiae ex academiae Bratislavensi Iurisprudentiae 7: pp 33–43; Medelský J (2014) Vývoj trestnej zodpovednosti právnických osôb. Trestněprávní revue 13, pp 87–91.

ISSN 1213-8770 (print), ISSN: 2464-6601 (online).

2 Computer Crime: A Brief Overview

Worldwide, the total cost of computer crime (also known as 'cyber crime'[8], 'cybercrime'[9], 'cyber-crime'[10] 'high-tech crime'[11], 'virtual crime'[12], or even 'e-crime'[13]) to society is significant. A recent report suggests that victims lose around 388 billion $ each year worldwide as a result of computer crime, making it more profitable than the global trade in marijuana, cocaine and heroin combined.[14] The three-stage classification of computer-related has been known: crimes in which the computer or computer network is the target of the criminal activity – for example, hacking or malware; offences where the computer is a tool used to commit the crime – for example, child pornography or criminal copyright infringement; and crimes in which the use of the computer is an incidental aspect of the commission of the crime, however, the computer is not significantly implicated in the commission of the offence – for example, addresses found in the computer of a murder suspect, or phone records of conversations between offender and victim before a homicide.[15]

8 See, for example: Kirwan G., Power A (2012) The Psychology of Cyber Crime: Concepts and Principles: Concepts and Principles. Information Science Reference, Hershey; Johnson M (2013) Cyber Crime, Security and Digital Intelligence. Gower Publishing, Farnham.

9 See, for example: Wall D S (2007) Cybercrime: The Transformation of Crime in the Information Age. Polity Press, Cambridge – Malden; Milhorn H T (2007) Cybercrime: How to Avoid Becoming a Victim. Universal Publishers, Boca Raton; Clough J (2010) Principles of Cybercrime. Cambridge University Press, New York; Brenner S W (2010) Cybercrime: Criminal Threats from Cyberspace. Praeger, Santa Barbara; Chawki M, Darwish A, Khan M A, Tyagi S (2015) Cybercrime, Digital Forensics and Jurisdiction. Springer, Cham – Heidelberg – New York – Dordrecht – London.

10 See, for example: Pocar F (2004) New Challenges for International Rules against Cyber-Crime. In: Savona E U (ed) Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research. Springer, Dordrecht, pp 29–38; Angers L (2004) Combating Cyber-Crime: National Legislation as a Pre-Requisite to International Cooperation. In: Savona E U (ed): Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research. Springer, Dordrecht, pp 39–54.

11 See, for example: Newton M (2003) The Encyclopedia of High-tech Crime and Crime-fighting. Infobase Publishing, New York; Knetzger M R, Muraski J A (2008) Investigating High-tech Crime. Prentice Hall, New Jersey.

12 See, for example: Gray L (2010) Virtual Crime!: Solving Cybercrime. Enslow Publishers, New York.

13 See, for example: Tennyenhuis A, Jamieson R (2003) Multidisciplinary e-Forensics Methodology Development to Assist in the Investigation of e-Crime. In: Andersen K I, Elliot S, Swatman P M C, Trauth E M, Bjørn-Andersen N (eds) Seeking Success in E-Business: A Multidisciplinary Approach. Springer Science+, New York, pp 187–226.

14 Symantec (2011): 'Norton Cybercrime Report 2011', 7th September 2011; European Commission (2012): 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre', Communication from the Commission to the Council and the European Parliament, COM(2012) 140 final, p. 2.

15 See: Clough J (2010) Principles of Cybercrime. Cambridge University Press, Cambridge, p. 10; Brenner S W (2010) Cybercrime: Criminal Threats from Cyberspace. Praeger, Santa Barbara, p. 39; Smith R G, Grabosky P, Urbas G (2004) Cyber Criminals on Trial. Cam-

ISSN 1213-8770 (print), ISSN: 2464-6601 (online).

Nowadays, as argues the European Commission, no crime is as borderless as computer crime, requiring law enforcement authorities to adopt a co-ordinated and collaborative approach across national borders, together with public and private stakeholders alike.[16] The Treaty on the Functioning of the European Union lists computer crime as one of the areas of particularly serious crime with a cross-border dimension.[17]

Specific offences – including computer crime – are recognised as offences which are within the legislative competence of the European Union. The European Parliament and the Council of the European Union may, by means of directives (in the recent past framework decisions), establish *minimum rules* concerning *the definition of criminal offences and sanctions* in the areas of *particularly serious crime with a cross-border dimension* resulting from the nature or impact of such offences or from a special need to combat them on a common basis.[18] Two legislative measures have been introduced in the European Union in order to combat and prevent computer crime, namely the *Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment*[19] and the *Directive 2013/40/EU on attacks against information systems*[20].[21]

First, the *Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment* introduced three types of offences, namely the offences related to payment instruments, the offences related to computers and the offences related to specifically adapted devices. Moreover, it establishes common rules on sactions.

bridge University Press, New York, p. 7; Záhora J (2005) Počítačová kriminalita v európskom kontexte. Justičná revue 57: p. 207.

16 European Commission (2012): 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre', Communication from the Commission to the Council and the European Parliament, COM(2012) 140 final, p. 2.

17 Under Article 83(1) of the Treaty on the Functioning of the European Union as amended by the Treaty of Lisbon the areas of particularly serious crime with a cross-border dimension are 'terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, *computer crime* and organised crime' (emphasis added).

18 Article 83(1) of the Treaty on the Functioning of the European Union as amended by the Treaty of Lisbon.

19 Council Framework Decision 2001/413/JHA of 28th May 2001 on combating fraud and counterfeiting of non-cash means of payment. Official Journal of the European Communities, L 149/1 of 2nd June 2001.

20 Directive 2013/40/EU of the European Parliament and of the Council of 12th August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Official Journal of the European Union, L 218/8, 14th August 2013. The Directive is intended to be consistent with the approach adopted in the Convention on cybercrime of 2001, adopted by the Council of Europe. Council of Europe, European Treaty Series No. 185 [2001], Budapest, 23rd November 2001.

21 Ivor J, Klimek L, Záhora J (2013) Trestné právo Európskej únie a jeho vplyv na právny poriadok Slovenskej republiky. Eurokódex, Žilina, p. 307 et seq.

ISSN 1213-8770 (print), ISSN: 2464-6601 (online).

Second, the *Directive 2013/40/EU on attacks against information systems* establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve co-operation between judicial and other competent authorities. The Directive introduced common definitions of the offences involved in attacks against information systems at the level of the EU, namely illegal access to information systems, illegal system interference, illegal data interference and illegal interception.

Besides harmonisation of elements of crimes and sanctions for naturals, the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment and the Directive 2013/40/EU on attacks against information systems confirmed the liability of legal persons and sanctions for legal persons.

3 Criminal Liability of Legal Persons

Liability of legal persons for offences is an issue which has been coming and going on political agenda of the European Union.[22] For example, as far as money laundering is concerned, the financial institutions through which money is laundered are frequently corporations or some other form of legal person. If money is laundered through such an organisation, it is often very difficult to identify an individual who is subjectively aware of what is going on and who can be held criminally responsible.[23] A question which begs consideration is whether liability of legal persons should be governed by civil or criminal controls.[24] As seen, besides harmonisation of elements of crimes and sanctions for naturals, European Union law has confirmed the liability of legal persons, in particular in case of European crimes – including computer crime.

The definitions of European offences, i.e. the description of conduct considered to be criminal, almost always cover the conduct of the main perpetrator, but also in most cases ancillary conduct such as instigating, aiding and abetting. Moreover, in some cases the attempt to commit the offence is also covered. Almost all European Union criminal law instruments include in the definition intentional conduct, but in some cases also seriously negligent conduct. Some instruments further define what should be considered as aggravating circumstances or mitigating circumstances for the determination of the sanction in a particular case.

22 Vermeulen G, De Bondt W, Ryckman Ch (2012) Liability of Legal Persons for Offences in the EU. Maklu, Antwerpen – Apeldoorn – Portland, p. 9.

23 Boister N (2012) An Introduction to Transnational Criminal Law. Oxford University Press, Oxford, p. 109.

24 Wells C (2011) Containing Corporate Crime: Civil or Criminal Controls? In: Gobert J, Pascal A-M (eds) European Developments in Corporate Criminal Liability. Routledge, Oxon, p. 11.

ISSN 1213-8770 (print), ISSN: 2464-6601 (online).

Generally, European Union law covers offences committed by natural persons as well as by legal persons such as companies or associations. However, in existing legislation, the Member States of the European Union have always been left with the choice concerning the type of liability of legal persons for the commission of criminal offences, as the concept of criminal liability of legal persons does not exist in all national legal orders.

Under the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment and the Directive 2013/40/EU on attacks against information systems measures should be taken to ensure that legal persons[25] can be held liable for computer crime. Each Member State of the European Union shall take the necessary measures to ensure that legal persons can be held liable for offences committed for their benefit by any person, acting either individually or as a member of an organ of the legal person in question, who has a leading position within the legal person, based on one of the following: a power of representation of the legal person, an authority to take decisions on behalf of the legal person, or an authority to exercise control within the legal person.[26]

In addition, in case of the Directive 2013/40/EU on attacks against information systems each Member State of the European Union shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person has made possible the commission of the offence(s) for the benefit of that legal person by a person under its authority.[27]

On the other hand, the criminal liability of legal persons shall not exclude criminal proceedings against natural persons who are perpetrators, instigators or accessories. Indeed, the relevant legislation is based on the criminal liability of natural persons as well as legal persons.

4 Sanctions for Legal Persons

As far as sanctions for legal persons are concerned, under the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment and the Directive 2013/40/EU on attacks against information systems the Member States of the European Union shall take the necessary meas-

25 Under Article 1(b) of the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment the term *legal person* shall mean any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations; under Article 2(c) of the Directive 2013/40/EU on attacks against information systems the term *legal person* shall mean an entity having the status of legal person under the applicable law, but does not include States or public bodies acting in the exercise of State authority, or public international organisations.

26 Article 7(1) of the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment; Article 10(1)(a)(b)(c) of the Directive 2013/40/EU on attacks against information systems.

27 Article 10(2) of the Directive 2013/40/EU on attacks against information systems.

ISSN 1213-8770 (print), ISSN: 2464-6601 (online).

ures to ensure that a legal person held liable is punishable by 'effective, proportionate and dissuasive sanctions', which shall include criminal or non-criminal fines and may include other sanctions, such as, for example:[28]

- exclusion from entitlement to tax relief or other benefits or public aid,
- temporary or permanent disqualification from the pursuit of commercial activities,
- placing under judicial supervision,
- a judicial winding-up order,
- temporary or permanent closure of establishments used for committing the offence.

As seen, European Union law requires the Member States of the European Union to take 'effective, proportionate and dissuasive sanctions' for a specific conduct. *Effectiveness* requires that the sanction is suitable to achieve the desired goal, i.e. observance of the rules; *proportionality* requires that the sanction must be commensurate with the gravity of the conduct and its effects and must not exceed what is necessary to achieve the aim; and *dissuasiveness* requires that the sanctions constitute an adequate deterrent for potential future perpetrators.[29]

In should be noted that sometimes European Union law determines more specifically, which types and/or levels of sanctions are to be made applicable. Provisions concerning confiscation can also be included. It is not the primary goal of approximation to increase the respective sanction levels applicable in the Member States of the European Union, but rather to reduce the degree of variation between the national systems and to ensure that the requirements of 'effective, proportionate and dissuasive sanctions' sanctions are indeed met in all Member States.

5 Conclusion

No crime is as borderless as computer crime. The Treaty on the Functioning of the European Union lists computer crime as one of the areas of particularly serious crime with a cross-border dimension.

Specific offences – including computer crime – are recognised as offences which are within the legislative competence of the European Union. Two legislative measures have been introduced in the European Union in order to combat and prevent computer crime, namely the Framework Decision 2001/413/JHA

28 Article 8(1)(a)(b)(c) of the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment; Article 11(1)(a)(b)(c)(d) of the Directive 2013/40/EU on attacks against information systems.

29 European Commission (2011): 'Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011) 573 final, p. 9.

ISSN 1213-8770 (print), ISSN: 2464-6601 (online).

on combating fraud and counterfeiting of non-cash means of payment and the Directive 2013/40/EU on attacks against information systems.

Besides harmonisation of elements of crimes and sanctions for naturals, the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment and the Directive 2013/40/EU on attacks against information systems confirmed the liability of legal persons and sanctions for legal persons. Measures should be taken in the Member States of the European Union to ensure that legal persons can be held liable for computer crime. In addition, they shall take the necessary measures to ensure that a legal person held liable is punishable by 'effective, proportionate and dissuasive sanctions', which shall include criminal or non-criminal fines and may include other sanctions.

Bibliography

Literature

Blanke H J, Mangiameli S (eds) (2013) The Treaty on European Union (TEU): A Commentary. Springer, Berlin – Heidelberg.

Boister N (2012) An Introduction to Transnational Criminal Law. Oxford University Press, Oxford.

Brenner S W (2010) Cybercrime: Criminal Threats from Cyberspace. Praeger, Santa Barbara.

Clough J (2010) Principles of Cybercrime. Cambridge University Press, Cambridge.

Ivor J, Klimek L, Záhora J (2013) Trestné právo Európskej únie a jeho vplyv na právny poriadok Slovenskej republiky. Eurokódex, Žilina.

Smith R G, Grabosky P, Urbas G (2004) Cyber Criminals on Trial. Cambridge University Press, New York.

Vermeulen G, De Bondt W, Ryckman Ch (2012) Liability of Legal Persons for Offences in the EU. Maklu, Antwerpen – Apeldoorn – Portland.

Wells C (2011) Containing Corporate Crime: Civil or Criminal Controls? In: Gobert J, Pascal A-M (eds) European Developments in Corporate Criminal Liability. Routledge, Oxon, pp 11–32.

Záhora J (2005) Počítačová kriminalita v európskom kontexte. Justičná revue 57: pp 207–218.

Záhora J (2013) Zodpovednosť právnických osôb za trestné činy v európskej dimenzii – komparatívny prehľad. In: Jelínek J (ed) Třestní odpovědnost právnických osob v České republice – bilance a perspektivy. Conference proceedings. Leges, Praha, pp 15–27.

Legislation

Council Framework Decision 2001/413/JHA of 28th May 2001 on combating fraud and counterfeiting of non-cash means of payment. Official Journal of

ISSN 1213-8770 (print), ISSN: 2464-6601 (online).

the European Communities, L 149/1 of 2nd June 2001.
Directive 2013/40/EU of the European Parliament and of the Council of 12th August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Official Journal of the European Union, L 218/8, 14th August 2013.
Treaty on European Union as amended by the Treaty of Lisbon. Official Journal of the European Union, C 83/13 of 30th March 2010.
Treaty on the Functioning of the European Union as amended by the Treaty of Lisbon. Official Journal of the European Union, C 83/47 of 30th March 2010.

Other sources

European Commission (2011): 'Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011) 573 final.
European Commission (2012): 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre', Communication from the Commission to the Council and the European Parliament, COM(2012) 140 final.
Symantec (2011): 'Norton Cybercrime Report 2011', 7th September 2011.

ISSN 1213-8770 (print), ISSN: 2464-6601 (online).