UNIVERSITY OF TIMISOARA
FACULTY OF LAW

UNIVERSITY OF PÉCS
FACULTY OF LAW

JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW

No. 1/2019

Edited biannually by courtesy of the Criminal Law Departments within the Law Faculties of the West University of Timisoara and the University of Pécs

UNIVERSUL JURIDIC

2019

Universul Juridic Publishing House

Edited by Universul Juridic Publishing House

Copyright © 2019, S.C. UNIVERSUL JURIDIC S.R.L.

All rights on this edition are reserved to Universul Juridic Publishing House

No part of this volume can't be copied without the subscription of Universul Juridic Publishing House

The journal is indexed in databases SSRN, EBSCO, HeinOnline.

ISSN 2360–4964

Redactor: Raluca Teodoru
Tehnoredactor: Tania MIlitaru
Copertă: Aurelian Leahu

Redacție:
tel.: 0732.320.666
e-mail: redactie@universuljuridic.ro

Distribuție:
tel.: 021.314.93.15
fax: 021.314.93.16
e-mail: distributie@universuljuridic.ro

editurauniversuljuridic.ro

Editura Universul Juridic

Portal:
tel.: 0725.683.560
e-mail: portal@universuljuridic.ro

universuljuridic.ro

Universul Juridic

Librăria UJmag:
tel.: 0733.673.555; 021.312.22.21
e-mail: comenzi@ujmag.ro

ujmag.ro

Ujmag.ro

WEST UNIVERSITY OF TIMISOARA
FACULTY OF LAW

UNIVERSITY OF PÉCS
FACULTY OF LAW

Center of Research in Criminal Sciences
FACULTY OF LAW
West University of Timisoara

JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW

❍ BOARD OF EDITORS ❍

Editors-in-Chief

Lect. dr. LAURA STĂNILĂ
West University of Timisoara
Faculty of Law

Prof. dr. ZORAN PAVLOVIC
University of Novi Sad
Faculty of Law

Conf. dr. FLAVIU CIOPEC
West University of Timisoara
Faculty of Law

Prof. dr. ISTVÁN GÁL
University of Pécs
Faculty of Law

Honorary Member
Prof. dr. VIOREL PAȘCA

Editors

Dr. CSONGOR HERKE
Dr. SILVIA SIGNORATO
Dr. VOICU PUŞCAŞU
Dr. MIHÁLY TÓTH
Dr. IOANA CELINA PAŞCA
Dr. ZOLTÁN ANDRÁS NAGY
Dr. LÁSZLÓ KŐHALMI
Dr. ZOLTÁN ANDRÁS NAGY
Dr. ANDREEA VERTES-OLTEAN
Dr. CSABA FENYVESI
Dr. ADRIAN FANU MOCA
Dr. RUXANDRA RĂDUCANU

SCIENTIFIC BOARD

Prof. dr. Ulrich Sieber, director Max Planck Institute for International Criminal Law; Prof. dr. Ye Qing. Chancellor Law Institute of SASS, Shanghai; Prof. dr. Zoran Stojanović, University of Belgrade, Faculty of Law; Prof. dr. Vid Jakulin, University Lublijana, Faculty of Law; Prof. dr. Roberto E. Kostoris, Ordinario di Diritto processuale penale nell'Università di Padova; Prof. dr. Zoran Pavlovic, Faculty of Law for Business and Judiciary; Prof. dr. Tudorel Toader, Chancellor University A.I. Cuza Iasi, Faculty of Law, Justice minister; Prof. dr. Florin Streteanu, University „Babes-Bolyai" Cluj-Napoca, Faculty of Law; Prof. dr. Valerian Cioclei, Bucharest University, Faculty of Law; Prof. dr. Elek Balazs, Debrecen University, Faculty of Law; Prof. dr. Silvio Riondato, Università degli Studi di Padova; Prof. dr. Yuri Pudovochkin, Russian State University of Justice; dr. sc. Matko Pajčić, assistant professor, Law Faculty, University of Split, Croatia, prof. dr. François Rousseau, Université de Nantes, dr. habil. István Resperger, Associate Professor, National University of Public Sevice Budapest; dr. habil. József Boda PhD, associate Professor National University of Public Sevice, Budapest; Gary Hill, Scientific Coordinator of the International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program (ISPAC), prof. dr. Ovidiu Predescu, General secretary of Academy of Legal Sciences of Romania.

The board of editors shall not take responsibility for the authors' opinions, therefore the authors are exclusively responsible for the former.

FOR CONTRIBUTORS

Journal of Eastern-European Criminal Law could stand out as a unique publication, at least in this part of the world, as an outcome of the partnership between specialists in Criminal law and Criminal Procedure law from the law faculties of the West University in Timisoara and the University in Pecs, who aimed at presenting, in a different language from their own, the serious amendments of criminal legislation that occurred in their countries in the post-communist era, an essential requirement for the rule of law. We envisage this journal, published semesterly, to be open to all researchers in the academic environment from the former communist countries, to professors, PhD students, but also, to magistrates and other professionals interested in the evolution of criminal legislation and in the more and more firm response to be given to the criminal phenomenon, while observing the fundamental human rights.

Our concerns aim at enlisting the Journal in additional databases, others than the ones in which the magazine is presently indexed, **namely Social Science Research Network (SSRN), EBSCO and HeinOnline.**

Any correspondence with the journal editors shall be sent with the mention „for the Journal of Eastern-European Criminal Law" at the following mail addresses:

laura.stanila@e-uvt.ro; flaviu.ciopec@e-uvt.ro; gal.istvan@ajk.pte.hu; zoran.pav@hotmail.com

For the time being, the journal cannot pay copyright compensation, any collaboration article shall therefore be voluntarily submitted.

Non-patrimonial copyright is protected, so any reproduction, representation, adaptation, translation and/or modification, partial or total, or transfer to a site of the articles, without consent of the authors, is prohibited.

The articles to be published shall be written in the following forma:

Title (capital letters, bold type, centred, 14)

Author(s)' name *(e.g. Sandra Marked[1], Werner Taylor[2], Roland G. Rowling[3]) (italics, bold type, centred, 12)*

Scientific degree, position (in order of the marking number), centred

Abstract and key words: Times New Roman font type, size 12.

The **text** shall be typed on A4 size (white copy paper), margins: left 3 cm, others 2.5 cm, Times New Roman font type, size 12.

Headings (chapter titles) shall be in capitals, with a blank line preceding and following them.

Within chapters, subheadings shall be italicized with a blank line preceding and following them.

References shall be listed **at the end of the paper, in alphabetical order.**

The recommended form of the list of references at the end of the paper: 1. Lippman, M: *Contemporary Criminal Law*, London: Sage Publications, 2007, p...

The paper shall be written exclusively in English and shall be accompanied by an abstract in English (10-15 lines).

The future issue of the magazine appears at the end of December 2018. The main topic of the future issue is: **Artificial Intelligence – Challenges for Criminal Law and Criminal Procedure Law.**

THE BOARD OF EDITORS

CONTENTS

ECONOMIC CRIMES

Dina Bajraktarević Pajević, Muamer Kavazović, Marija Lučić – Ćatić
Financial crime of legal persons in case law of the court of Bosnia and Herzegovina 9

Csaba SZILOVICS
On a new tool to combat tax evasion 34

László Kőhalmi
Some issues of criminal liability by reason of economic decisions 44

Zoran S. Pavlović, Nikola Paunović
Phenomenological forms of asset misappropriation fraud as the specific type of economic crime 53

Gál István László, Serbakov Márton Tibor
How acts of rerrorism are financed and orchestrated in secrecy today: criminal offenses, donations, legal businesses and smartphone applications 66

Shenkuo Wu
Cybersecurity Obligations of ICT Companies in P. R. China 77

Ákos Farkas, Judit Jacsó, Bence Udvarhelyi
Criminal law protection of the financial interests of the Eu results and conclusions of a Hercule III project 89

István László Gál
Economic policy, criminal policy and economic crimes 100

Aleksandar Stevanović
Lobbying and Corruption: comparative legal analysis of two notions 110

Endre Nyitrai
Criminal regulations on money laundering in Hungary 120

Aleksandar R. Ivanović
Criminal regulation and criminalistic aspects of money laundering with special focus on the criminal legislation of the Republic of Serbia 127

TU Longke
On an Internet Service Provider's Content Management Obligation and Criminal Liability 145

Dragan Jovašević
Computer crimes in republic of Serbia 159

VARIA

Laura Stănilă
Specific aspects on the right to a fair trial in the recent caselaw against

Dávid Tóth
The theories and regulation of criminal liability of legal persons in Hungary 178

Balázs Elek
The Relationship between *Habeas Corpus* and Robot Technology in Criminal Proceedings 189

Aleksandar B. Ivanović
Accreditation and standardization in forensic science – present and future of reliability of forensics examination and expertise 200

Osman Jašarević
Criminological and criminal legal aspects of discrimination, violence, abuse and neglect of school-age children 213

Viorel Pașca
Terrorism: between the need for funding and obtaining funding sourceS 227

Financial crime of legal persons in case law of the Court of Bosnia and Herzegovina

***Prof. dr. Dina Bajraktarević Pajević*[1]**
***Prof. dr. Muamer Kavazović*[2]**
***Prof. dr. Marija Lučić – Ćatić*[3]**

Abstract

With entry into force of new criminal legislation in 2003 the legal concept of liability of legal persons for criminal offences was introduced into the criminal law of Bosnia and Herzegovina (B&H). However, the general scientific indifference to this issue reflected in limited literary fund and the scarcity, disorganization and inaccessibility of relevant case law in different circuits of B&H's criminal justice system well as absence or unavailability of relevant statistical data have created difficult environment for scientific observation of the results of implementation of new legal solutions regarding the liability of legal persons for criminal offenses. Following the premise that liability of legal persons for criminal offenses had the greatest practical significance in the sphere of financial crime, the authors analyzed the available case law of the Court of B&H in order to gain some insight into the specifics of legal persons' crime prosecution in B&H.

Keywords: *liability of legal persons for criminal offences, financial crime of legal persons*

I. Introduction

Liability of legal persons and especially their criminal liability no longer represents controversial point in majority of contemporary legal systems and present standpoint on subjection of the legal persons to the authority of criminal law has been shaped throughout alterations in legal systems during the last century. Long tradition of continental legal systems' opposition to the attribution of liability to legal persons emphasized with the principle *societas delinquere non potest* and characterized by focus on imposing liability on the natural person within the legal persons (such as employees at the managerial level), was scrutinized and consequently abandoned in the light of social, economic and political changes[4]. Modifications of criminal law concerning the

[1] Faculty of Criminal Justice Science, Criminology and Security Studies, University of Sarajevo; e-mail: dbajraktarevic@fkn.unsa.ba.

[2] Faculty of Criminal Justice Science, Criminology and Security Studies, University of Sarajevo; |e-mail: mkavazovic@fkn.unsa.ba.

[3] Faculty of Criminal Justice Science, Criminology and Security Studies, University of Sarajevo; UNSA e-mail: mlucic@fkn.unsa.ba.

[4] See: Stanila, L. (2014), 'Criminal Liability of Legal Persons. History, Evolution and Trends in Romanian Criminal Law', *Journal of Eastern European Criminal Law*, No. 1/2014, pp. 109-121. Available at SSRN: https://ssrn.com/abstract=2462414.

introduction of liability of legal persons as additional layer of criminal liability, alongside the liability of individual perpetrator[5], were especially stimulated by developments such as intensive privatization processes, immersion of legal persons in every aspect of economy and creation of mega-multinational corporations as the result of acquisitions, mergers and takeovers[6]. This intervention in the criminal law systems has been rationalized as an endorsement of fundamental societal values and effective determent of undesirable activity[7] but also as a form of retribution toward the legal persons because of the possibility that they might profit from engaging in illegal activities[8]. Today, in literature and practice corporate[9] wrongdoing is largely acknowledged as „delinquency worthy of criminal sanction"[10] [11].

Establishment of liability of legal persons for criminal offences in continental legal systems was also encouraged by the regional and international organizations such as the Council of Europe, the European Economic Community/European Union, and the United Nations[12]. It is interesting that this process of alteration also instigated

---

[5] See: Pudovochkin Y. E. and Adrianov V.K. (2015), 'Principles of criminal law: Immersion in theory', *Journal of Eastern-European Criminal Law*, No. 1/2016, pp. 201-207.

[6] Lederman, E. (2000), 'Models for Imposing Corporate Criminal Liability: From Adaptation and Imitation Toward Aggregation and the Search for Self-Identity', *Buffalo Criminal Law Review*, Vol. 4 No. 1, p. 644.

[7] In a sense that it creates incentives for corporations to monitor the activities of its employees or to as well as for prevention of setting up corporations for illegal purposes, and to prevent existing corporations from doing harm in any way. According to: Godwin Muhwezi, M. (2016), The Case for Corporate Criminal Liability, pp. 4-5. Available at: https://www.researchgate.net/publication/309041784_THE_CASE_FOR_CORPORATE_CRIMINAL_LIABILITY. Various researches affirmed that sometimes corporate system itself generates criminal behavior. See: Foerschler, A. (1990) 'Corporate Criminal Intent: Toward a Better Understanding of Corporate Misconduct', *California Law Review*, Vol. 78, Iss. 5, pp. 1289-1290; available at: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4440&context=californialawreview; Clubb, A. C. (2014), The corporation as a city, Journal of Financial Crime, Vol. 21 Iss. 2 pp. 191 – 203; Hansen, L. L. (2009) 'Corporate financial crime: social diagnosis and treatment', *Journal of Financial Crime*, Vol. 16 Iss. 1, pp. 28-40; available at: https://doi.org/10.1108/13590790910924948; etc.

[8] Godwin Muhwezi (2016), pp. 4-5.

[9] Terms corporation and legal person/legal entity are often interchangeably used in relevant literature. See: Coffee, J. C. (1999), Corporate Criminal Liability: An Introduction and Comparative Survey, pp. 9-39. In: A. Eser, G. Heine and B. Huber (eds), Criminal responsibility of legal and collective entities: international colloquium. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht; Heine, G. (1998), *„Sanctions in the Field of Corporate Criminal Liability,"* Paper presented at the International Colloquium on Criminal Responsibility of Legal and Collective Entities. 4-6 May 1998. Berlin, Germany; OECD (2015), *Liability of Legal Persons for Corruption in Eastern Europe and Central Asia, a*vailable at: https://www.oecd.org/corruption/ACN-Liability-of-Legal-Persons-2015.pdf*;* Vermeulen et al. (2012), *Liability of legal persons for offences in the EU,* Principal European Commission DG Justice (JLS/2010/JPEN/PR/1009/E4). Antwerpen, Apeldoorn, Portland: Maklu-Publishers*;* available at: https://publications.europa.eu/en/publication-detail/-/publication/e6a11989-48d3-41a1-b4ee-8f7051d84253/language-en.

[10] Tiedemann, 1994, p. 14 according to Beale and Safwat, 2005:108) Beale, S.S. and Safwat, A (2004), 'What developments in Western Europe tell us about American critiques of corporate criminal liability', *Buffalo Criminal Law Review*, Vol. 8, No. 1, 2005, p. 108 *(*Duke Law School Legal Studies Paper No. 80.); available at SSRN: https://ssrn.com/abstract=800533.

[11] As Lederman states: „policy setters in various legislative and law enforcement bodies sensed that attaining effective, and mainly trouble-free, control of the economy through criminal law depends on a sweeping subordination of the legal bodies themselves, as far as possible, to criminal proceedings." See: Lederman, E. (2000), 'Models for Imposing Corporate Criminal Liability: From Adaptation and Imitation Toward Aggregation and the Search for Self-Identity', *Buffalo Criminal Law Review*, Vol. 4 No. 1, p. 644.

[12] For more information on specific instruments of those organizations see: Derenčinović, D. (2002), Odgovornost pravnih osoba u hrvatskom kaznenom pravu, *Hrvatska pravna revija*, pp. 1-22,

modifications in the common law systems in form of further development of established legal and theoretical concepts of liability of legal person.

Despite the differences between the criminal law regimes, most of them usually require establishment of certain level of guilt (culpability, criminal intent, *mens rea*) before an imposition of criminal liability on person[13]. In the criminal law, guilt as an element of the notion of punishable act (criminal offence) represents the entirety of awareness about offence and awareness about unlawfulness[14]. In the narrow interpretation, the guilt is perceived as psychological relationship between the act and the offender[15], which was key problem in creating concept of criminal liability of legal persons. Legal person as fiction cannot fulfill *mens rea* requirement. Since criminal law was constructed in the light of the specificity of human beings - their behavior and characteristics, thorough change was needed in criminal law theory in order to apply its key institutes on legal person.

Perception that culpability of legal person is the same as the culpability of the individuals associated with it (and thus liability of legal persons has derivative nature) is in the focus of the nominalist theory which resulted in two models: model of vicarious liability and identification doctrine (derivative model of corporate criminal liability). Both legal theories on the liability of legal persons for criminal offences were developed in common law as a modification of the law of torts' concept and focused on the adaptation and imitation of the imposition of criminal liability on human beings[16]. The theory of vicarious liability uses as a foundation concept of legal relationship between the employee and employer or agent and principal in manner that attributes the unlawful act of the employee or agent to the to the principal or the employer[17] [18]. The theory of vicarious liability[19] was further developed by the courts who applied it to the to the situations when the principal or employer is a legal person (for example in case: Tesco Stores Ltd. v. Brent London Borough Council)[20]; the *actus reus* and *mens rea* of the individuals who act on behalf of a corporation are automatically attributed to the

---

available at: https://www.pravo.unizg.hr/_download/repository/Derencinovic_D.%2C_Odgovornost_pravnih_osoba_u_hrvatskom_kaznenom_pravu.pdf; Filipović and Ikanović (2010), Krivični postupak protiv pravnih lica, available at: https://vstv.pravosudje.ba/vstv/faces/docservlet?p_id_doc=4859; Clifford Chance (2012), Corporate Liability in Europe, available at: https://www.cliffordchance.com/briefings/2012/02/_corporate_liabilityineuropetechnicalbrochure.html; Vermeulen et al., 2012; etc.

[13] Vermeulen *et al*., 2012, p. 49.

[14] Derenčinović, 2002, p. 11.

[15] Vermeulen *et al.,* 2012, p. 57.

[16] Lederman, 2000, p. 652.

[17] *Ibidem*.

[18] According to the Bassi, the most widely accepted rationale of vicarious liability is loss distribution – losses caused by organization's employees are to be positioned upon that organization itself because organization should bear the loss not the victim or innocent party and organization is better able to absorb the losses as a cost of doing business, see: Bassi, A. (2016), Corporate criminal liability an analytical study with special reference to penal laws in India, p. 86; available at: http://shodhganga.inflibnet.ac.in/handle/10603/200004. Moreover, vicarious liability motivates organization to be careful in selection and supervision of employees.

[19] For example, in the United States (both on the federal level and in some states), any actor (whether a corporate employee, officer or agent) who acts within his normal scope of responsibility and violates the criminal law with an intent to benefit the organization thereby creates liability, both for himself and his corporate employ (Coffee, 1999:9).

[20] Gazette 07-Apr-1993, Times 16-Feb-1993, [1993] 1 WLR 1037.

corporation[21]. However, this doctrine failed to offer a comprehensive solution to the issue of imposing criminal liability to legal persons[22] and as response federal courts in US improved vicarious criminal liability into doctrine of *respondeat superior*[23] which allowed imposition criminal liability on corporations for acts of its agents or employees under the following cumulative conditions: agent/employee acted within the capacity of employment/agency in furtherance of the corporation's business interests[24]. Sporadically, courts insisted on additional condition that criminal acts of agent/employee were authorized, tolerated or ratified by corporate management[25].

The model of identification doctrine[26] was created mainly by English law[27] as a response to limitations of the theory of vicarious liability regarding the criminal liability of corporations. Under this theory of liability behavior and knowledge of certain individuals within the corporation (corporate organs/bodies) who act within the scope of their authority and on behalf of the corporate bodies is recognized as the behavior of the legal body itself (individuals as the embodiment of the legal body). Based on the perception that corporation must act through its representatives – individuals (natural persons) who operate within the certain corporative bodies (managerial or supervisory), it identifies those corporative bodies with legal person itself. This model occurs especially in relation to the offences requiring *mens rea*, highest ranking members of personnel act as company itself, rather than on behalf of it[28]. While critics see vicarious liability simultaneously as too wide (in attributing the wrongdoings of any employee to the organization) as well as too narrow (there is no possibility to examine company policies), the identification theory was criticized as insensitive in relation to the organization, size[29] and functioning of large corporations[30].

Another model of liability – the aggregation model was created within the nominalist framework as an attempt to solve problems of attribution of fault[31] at the end of twentieth century under the influence of theories developed in sociology and management[32]. This model was also consequence of the modification of the theory of vicarious liability in the context of decentralized and complex structures of large modern corporations. The aggregation model theory aimed at identifying a collective responsibility of individuals within the legal person, rather than identifying an

---

[21] De Maglie, C. (2005), 'Models of Corporate Criminal Liability in Comparative Law', *Global Stud. L. Rev*. 547, p. 553; available at: http://openscholarship.wustl.edu/law_globalstudies/vol4/iss3/4.

[22] It was criticized for distorting the concept of fault, particularly regarding *mens rea* offences, see: Bassi, 2016, p. 88.

[23] Supreme Court in New York Central & Hudson River Railroad Co v United States [53 L. Ed. 613 (1909)].

[24] Vermeulen *et al.*, 2012, p. 49.

[25] Lederman, 2000, p. 655.

[26] Theory of direct liability or alter ego theory of liability.

[27] In contrast, in the United Kingdom and much of the British Commonwealth, an alternative approach has long governed under which only the acts of certain very high-ranking corporate executives can be attributed to the corporate for purposes of creating corporate criminal liability („alter ego theory" or „identification theory") has been the dominant approach for much of this century. See: Coffee, 1999, p. 9.

[28] Vermeulen *et al.,* 2012, p. 58.

[29] Wells C, (1999) 'The Millennium Bug and Corporate Criminal Liability', *The Journal of Information, Law and Technology (JILT)*, p. 121. Available at: http://elj.warwick.ac.uk/jilt/99-2/wells.html.

[30] See: Bassi, 2016, pp. 99-100.

[31] Godwin Muhwezi, 2016.

[32] Lederman, 2000, p. 661.

individual perpetrator, therefore aggregation could involve matching the conduct of one individual with the state of mind or culpability of another individual to achieve liability[33]. This theory provides that corporations can be held criminally liable based on the act of one employee and on the culpability of one or more other employees who, cumulatively, but not individually, met the requirements of *actus reus* and *mens rea* of the crime[34]. However, in judicial practice implementation of this model has been modest because of the acknowledged difference between corporate collective knowledge and collective criminal intent and standpoint of courts that attributing *mens rea* of intent or recklessness to a legal body depends, according to these courts, on the full development of this culpable state of mind in one of the corporation's employees[35]. Furthermore, it is often argued that the aggregation theory lacks consistency with the traditional pri.nciples of criminal law[36]. In ongoing discussions regarding the idea of „optimal theory of corporate criminal liability" focus is on three elements: the collective knowledge; alleged desirability of adequate care or non – negligence and alleged „perverse effects" of existing rules on corporate liability[37].

In addition to the above-mentioned theories on liability of legal persons, in literature is often mentioned model of separate self – identity[38]. Unlike aforementioned models, who were developed by the courts, this concept of criminal liability of legal persons has been created in American literature under the influence of specific social trends[39]. It is based on the assumption that legal persons have a mechanism for expressing their substance and self-identity, which can be located and established and thus legal person can be held liable for criminal offences without necessity to be linked to the behavior of individuals[40]. Identity of legal person is perceived as different and separate from the identity of the body or individual within the corporation, even if they all play a role and contribute significantly to the development and shaping of that identity[41]. The legal person is seen as whole, and its bodies shouldn't be observed as legal person nor manifestations of bodies should be seen as manifestations of the will of legal person[42]. Thus, views opposite to ones previously presented, created different concept of liability of legal persons – organizational model of criminal liability of legal persons[43]. Organizations function as real entities in ways that are not reducible to propositions about individuals. So, the corporation is something more than what is attained from the sum of all individual parts.

---

[33] Vermeulen *et al.,* 2012.

[34] Pop, A. I. (2006), Criminal Liability of Corporations—Comparative Jurisprudence, p. 4. Available at: https://digitalcommons.law.msu.edu/king/81.

[35] See: Lederman, 2000, p. 666.

[36] Pop, 2006, p. 4.

[37] Coffee,1999, p. 25

[38] See: Quaid, J. A. (1998), The assessment of corporate criminal liability on the basis of corporate identity: An analysis. McGill Law Journal Volume 43, pp. 67–114; Lederman, 2000; Wells, C. (1994), 'Corporate Liability and Consumer Protection: Tesco v Nattrass Revisited Celia Wells', *The Modern Law Review*, Vol. 57, No. 5, pp. 817-823.

[39] Such as: complexity of the corporate phenomenon; rising dominance of collective theories; and growth of interdisciplinary research. See: Lederman, 2000, pp. 683-685.

[40] Vermeulen *et al*., 2012, p. 59.

[41] Lederman, 2000, p. 678.

[42] See: Savić, V-I, (2011), Koncept autonomne odgovornosti pravne osobe i njegova primjena u kaznenom pravu, *Godišnjak Akademije pravnih znanosti Hrvatske*, Vol. II No. 1, str. 41-68.

[43] According to some authors (Godwin Muhwezi, 2016) this model is far superior to the derivative model of liability.

II. Financial crime of legal persons

Companies and corporations represent types of legal persons that are most often associated with contemporary criminal activities. Profit earning deeply rooted in the grounds of their establishment[44] makes them vulnerable to the criminal behaviors – often, they are used as cover up for various criminal activities, but also, they generate criminal activities because of their inclination to maximization of profits within short time and in the easiest manner, regardless to the consequences[45]. In research it was pointed out that the national criminal justice system's capacity to investigate and prosecute corporate crime is in practice very limited as well as its capacity to enforce effective sanctions[46]. If liability of legal persons for criminal offences is not adequately developed and identified in certain legal system, that creates a number of consequences: companies will continue to benefit from their criminal and dangerous practices by ensuring that individual employees plead guilty to the offence; crime remains very profitable for the corporation and carries few if any consequences for the company itself; and future offences are not effectively prevented[47]. However, not only that corporate misbehavior is often handled in civil rather than criminal court, it is also rarely publicized for mass consumption as conventional crime[48].

Ability of corporate and collective entities to evade liability or responsibility for their harmful conduct is supported by the limitations of an antiquated social control system based solely on national institutions implying that contemporary corporate crime has increasingly transnational nature[49]. Furthermore, absence of effective international regulations[50] has resulted that transnational corporations, with their complex and intricate structures of parent companies, holdings and subsidiaries, are easily able to exploit the weaknesses of the existing regulatory regime[51]. Even though criminal offences linked to the liability of legal persons are themes of various research

---

[44] As Dobbin states: „Without the state's strict enforcement of the obligations of citizenship, the corporation is exposed for what it is. It is not a citizen, or anything even vaguely resembling such a multifaceted and complex entity. The corporation is strictly one-dimensional, demonstrating only the narrowest of characteristics: greed.". See: Dobbin, M. (1998), The Myth of the Good Corporate Citizen, Stoddart Pub: Toronto, p. 24.

[45] Derenčinović, 2002, p. 20.

[46] See: Pontell, H. N., *et al*. (1994), Corporate crime and criminal justice system capacity: Government response to financial institution fraud, *Justice Quarterly*, Vol. 11, Iss. 3, pp. 383-410.

[47] Brenen, K.-D. (1999), Forms of Criminal Responsibility of Organisations and Reasons for their Development. A Description of the Legal Practice in Germany, p. 54. In: A. Eser, G. Heine and B. Huber (eds), Criminal responsibility of legal and collective entities: international colloquium. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

[48] See: Morris, B. (2008), „Corporate convicts: where are they now?", Fortune Magazine, Vol. 157 No. 12.

[49] Préfontain, D. (1999), Effective Criminal Sanctions Against Corporate Entities: Canada, p. 277. In: A. Eser, G. Heine and B. Huber (eds), Criminal responsibility of legal and collective entities: international colloquium. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

[50] See: Gerber and Jensen, (2000), 'Controlling Transnational Corporations: The Role of Governmental Entities and Grassroots Organizations in Combating White-Collar Crime', *International Journal of Offender Therapy and Comparative Criminology* Vol. 44 Iss. 6, pp. 692-713, available at: https://pdfs.semanticscholar.org/0551/bd8af2a8c0019980322720eb3018aa692e50.pdf

[51] Dandurand, Y. (1999), Entertaining Realistic Expectations About the Effect of Criminal Sanctions Imposed on Corporate Entities: Canada, pp. 269. In: A. Eser, G. Heine and B. Huber (eds), Criminal responsibility of legal and collective entities: international colloquium. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

for the last few decades they still represent, in criminological sense, an unknown phenomenon[52]. Generally, this is caused by absence of quantitative data on extent, development, structure and control of this type of crime and its varieties.

The essence of legal persons' crime (more often referred to as corporative crime) are criminal offences committed by employees on behalf or in favor of the legal person[53], which places this area of crime into white collar crime[54] or in much broader concepts such as financial crime. However, similarly to the corporate crime, most of the data on financial crime is produced without credible methodology[55]. According to the Levi financial crime represents one of the biggest business and social issues of our time[56]. In literature, financial crime is defined as crime that involves use of deception for illegal gain, normally involving breach of trust, and some concealment of the true nature of the activities[57] or as a financially driven non-violent crime committed by business and government professionals[58] [59]. Various categories of financial crime: fraud, theft, corruption and manipulation[60] include significant participation of legal persons, which is not surprise having in mind profound involvement of legal persons in every segment of the economy. Researches show that at least one domestic or foreign legal person is behind almost every serious financial criminal offence against budget of EU[61]. Even though no industry is immune to the various forms of financial crime such as tax evasion, antitrust crime, insider trading, accounting frauds, environmental, corruption crime, little is known about extent, structure and control of those criminal offences in context of liability of legal persons. One of the reasons is that in those types of crimes prosecution often focuses on the individual employee[62] not legal person itself, even

---

[52] Walburg, C. (2015), The measurement of corporate crime: an exercise in futility? p. 25. In: J.v. Erp, W. Huisman and G. V. Walle (Eds.), *The Routledge Handbook of White-Collar and Corporate Crime in Europe*. Oxon: Routledge.

[53] According to the Brenan there is no doubt that companies organize themselves in a way that minimizes the legal and financial consequences of the crimes that are committed on their behalf by their employees. See: Brenan, 1999, p. 55. And some authors point out that corporate organizational structure itself is criminogenic. See: Clubb, 2014.

[54] According to Friedrichs white collar criminality is financial delinquency of persons of reputable occupation and social status. See: Friedrichs, D. O. (2009), Trusted criminals: white collar crime in contemporary society Belmont, CA: Wadsworth Cengage Learning, p. 5. Clubb suggests there is a general consensus among modern definitions that white-collar crime involves delinquent and criminal acts committed in the course of one's occupational activities or otherwise facilitated by the trust and resources provided by one's occupational position; and even though white-collar crime occurs in a variety of occupational settings, one of the most complex environments in which white-collar crime flourishes is the corporate system. See: Clubb, 2014, p. 193.

[55] See: Economic & Social Research Council. (2012). Data on financial crime is not credible, UK research finds. ScienceDaily. Available at: www.sciencedaily.com/releases/2012/12/121213193137.htm.

[56] *Ibidem*.

[57] Picket, K. H. and Picket, J. (2002), Financial Crime Investigation and Control. New York: John Wiley and Sons, Inc., p. 3.

[58] Tupman, W. (2015), 'The characteristics of economic crime and criminals', p. 4. In: B. Rider (ed) Research Handbook on International Financial Crime. Cheltenham, Northampton: Edward Elgar Publishing Limited.

[59] The Financial Services and Markets Act (FSMA) 2000 s 6(3) determines financial crime as „any offence involving (a) fraud or dishonesty; (b) misconduct in, or misuse of information relating to, a financial market; or (c) handling the proceeds of crime".

[60] Gottschalk, (2010), 'Categories of financial crime', *Journal of Financial Crime*, Vol. 17 Iss: 4, p. 443.

[61] Derenčinović, 2002, p. 21.

[62] For a long time, it was known that many managers - 43 % - are prepared to do things in their professional life that they would reject in their private life. See: Brenner, S.N. and Molander, E.A. (1977), Is the ethics of business executives changing?, Harvard Business Review, Vol. 55, January-February, pp. 57-71.

though profit derived from criminal activities goes to the employer[63]. Hansen points out that corporate financial crime is additionally difficult to detect, due to elaborate conspiracies in the form of social networks, which are not restricted to members of the business community but extend themselves to include politicians and law enforcement officials[64]. Due to the complexity of criminal offences connected with business activities of legal persons it can be assumed that „registered criminal offences represent only the tip of a large iceberg"[65].

In Bosnia and Herzegovina (abbreviated as: B&H) is even less known about financial crime (as well as any other type of crime) connected with legal persons. Uncertainties regarding the liability of legal persons for financial and other criminal offences are present in B&H due to general scientific indifference towards this issue reflected in scarce literary fund[66], and the insufficiency, disorganization and inaccessibility of relevant case law in different circuits of B&H's criminal justice system. Furthermore, absence or unavailability of relevant statistical data on liability of legal persons for criminal offences was confirmed during our research when we contacted the competent authorities on every level of governmental organization of B&H, which, *inter alia,* collect, produce and disseminate statistics on crime within the segment of demography and social statistics: the Agency for statistics of Bosnia and Herzegovina at the level of the state, the Federal Office of Statistics for the Entity of Federation of B&H (abbreviated: FB&H) and the Institute of Statistics for the Entity of Republika Srpska (abbreviated: RS)[67]. However, the official response of all contacted competent authorities was that they don't have any statistics regarding the liability of legal persons for criminal offences.

Having in mind previously stated and testing the assumption that liability of legal persons for criminal offenses has the greatest practical significance in the sphere of financial crime, we conducted the analysis of only publicly available cases – cases that were heard before the Court of B&H. However, before examination of cases, the concept of liability of legal persons for criminal offences developed in legal system of B&H will be explained.

III. Liability of legal persons for criminal offences in legal system of B&H

As in other criminal law systems belonging to the continental legal tradition, strongly shaped by the Roman law, liability of legal persons for criminal offences in legal system of Bosnia and Herzegovina was introduced relatively late – in 2003 with the entry into force of the new criminal legislation. Primarily the result of influence of international documents (generated by the Council of Europe[68], the European Union[69],

---

[63] See: Eidam, G. (1999), Forms of Criminal Responsibility of Organisations: Aspects of Legal Practice in Germany, p. 65. In: A. Eser, G. Heine and B. Huber (eds), Criminal responsibility of legal and collective entities: international colloquium. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

[64] Hansen, 2009, p. 34,36.

[65] Gobert, J. and Punch, M. (2003), Rethinking Corporate Crime. Cambridge: Cambridge University Press; p. 12.

[66] During the writing of this paper we performed search of Cooperative online bibliographic system and services in B&H COBISS.BH (http://www.cobiss.ba/) that resulted with only four results.

[67] See: http://www.bhas.ba/?option=com_publikacija&id=1&lang=ba.

[68] The Recommendation No. R(88) 18 of the Committee of Ministers to Member States concerning liability of enterprises having legal personality for offences commuted in the exercise of their activities.

In the context of liability this document stipulates: 1) that enterprises should be able to be made liable for offences committed in the exercise of their activities, even where the offence is alien to the purposes of the enterprise; and 2) the enterprise should be so liable, whether a natural person who committed the acts or omissions constituting the offence can be identified or not. Furthermore, Recommendation No. R(88) 18 indicates that the enterprise should be exonerated from liability where its management is not implicated in the offence and has taken all the necessary steps to prevent its commission. Also, it clarifies that the imposition of liability upon the enterprise should not exonerate from liability a natural person implicated in the offence; and persons performing managerial functions should be made liable for breaches of duties which conduce to the commission of an offence. Recommendation No. R (88) 18 favors a negligence-based approach to corporate criminal liability. The Recommendation No. R(96) 8 of the Committee of Ministers to Member States on crime policy in Europe in a time of change suggested that provision should be made for the liability of corporate bodies for criminal offences. In literature it is often referred to another international instrument as influential in context of introduction of liability of legal persons in legal system of B&H (see Babić *et al.* [2005]), Komentari krivičnih/kaznenih zakona u Bosni i Hercegovini. Sarajevo: Evropska komisija, Vijeće Evrope): the Convention on the protection of the environment through criminal law (Strasbourg, 4.XI.1998). This Convention defines the concept of criminal liability of legal persons in Article 9, which prescribes adoption of appropriate measures that are necessary to enable imposition of criminal or administrative sanctions or measures on legal persons on whose behalf an offence referred to in Articles 2 and 3 of Convention (intentional and negligent offences) has been committed by their organs or by members thereof or another representative. It is further stipulated that corporate liability in context of this Convention doesn't exclude criminal proceedings against natural person. Unfortunately, B&H still has not signed this Convention. Another influential instrument was the Criminal Law Convention on Corruption (Strasbourg, 27/01/1999), which incorporates provisions on liability of legal persons. The term „legal person" in Article 1(d) this document is defined as a „any entity having such status under the applicable national law, except for States or other public bodies in the exercise of State authority and for public international organizations". In Article 18 of the Convention stipulates obligation to adopt legislative and other necessary measures in order to ensure that legal persons can be held liable for criminal offences of active bribery, trading in influence and money laundering established in accordance with Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on: power of representation of the legal person; or an authority to take decisions on behalf of the legal person; or an authority to exercise control within the legal person; as well as for involvement of such a natural person as accessory or instigator in the above-mentioned offences. Furthermore, States must take necessarry measures to ensure that legal person can be held liable where the lack of supervision or control by a natural person who has leading position (referred to in Art.18 (1)) has made possible the commission of the criminal offences previously mentioned for benefit of that legal person by a natural person under its authority (Art. 18(2) of the Convention). Similarly, to the Convention on the protection of the environment through criminal law, this Convention also prescribes that corporate liability previously elaborated shall not exclude criminal proceedings against natural persons who are perpetrators, instigators of, or accessories to the criminal offences referred to in the Art. 18(1). The Criminal Law Convention was signed by B&H on 1 March 2000, ratified it on 30 January 2002 and entry into force was 1 July 2002. Another relevant instrument for development of corporate liability the Convention on cybercrime (Budapest, 23.XI.2001) that requires establishment liability of legal persons for a criminal offence established in accordance with Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a power of representation of the legal person; an authority to take decisions on behalf of the legal person; an authority to exercise control within the legal person. Additionally, States must ensure hat a legal person can be held liable where the lack of supervision or control by a natural person on leading position within the legal person, has made possible the commission of a criminal offence for the benefit of that legal person by a natural person acting under its authority (Art. 12(2) of the Convention). However, Convention doesn't explicitly prescribe criminal liability of legal persons but it leaves to the States that in accordance with its legal system and established legal principles to chose type of liability (criminal, civil or administrative) (Art. 12(3) of the Convention). Such liability will be without prejudice to the criminal liability of the natural persons who have commited the offence (Art. 12(4) of the

OECD[70] and the UN[71]), created concept of liability needed to provide more comprehensive approach in the fight against the financial crime and other related areas of crime given the implications of the criminal offences that are committed in relation with the activities of the legal persons or its structure (utilizing it as an instrument or

---

Convention). B&H signed the Convention on Cybercrime on February 9 2005, ratified it on 19 of May 2006 and entry into force was 1 September 2006.

[69] Second Protocol to the Convention on the protection of the European Communities´ financial interest - Joint Declaration on Article 13 (2) - Commission Declaration on Article 7 (OJ C 221/12/97). This document in Article 3(1) prescribes that Member States must ensure that legal persons can be held liable for fraud, active corruption and money laundering committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on a power of representation of the legal person, or an authority to take decisions on behalf of the legal person, or an authority to exercise control within the legal person, as well as for involvement as accessories or instigators in such fraud, active corruption or money laundering or the attempted commission of such fraud. Also Member State must ensure that a legal person can be held liable where the lack of supervision or control by a person referred to in Art 3(1) has made possible the commission of a fraud or an act of active corruption or money laundering for the benefit of that legal person by a person under its authority. Liability of a legal person doesn't exclude criminal proceedings against natural persons who are perpetrators, instigators or accessories in the fraud, active corruption or money laundering.

[70] The Convention on combating bribery of foreign public officials in international business transactions (adopted on 21 November 1997) created concept of „responsibility of legal persons" for the bribery of a foreign public official (Art. 2), like the concepts in other international documents. In the Annex I: Good Practice Guidance on Implementing Specific Articles of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions it is prescribed that „Member States' systems for the liability of legal persons for the bribery of foreign public officials in international business transactions should not restrict the liability to cases where the natural person or persons who perpetrated the offence are prosecuted or convicted.". Two approaches are suggested for Member States' systems for the liability of legal persons. First approach provides that the level of authority of the person whose conduct triggers the liability of the legal person is flexible and reflects the wide variety of decision-making systems in legal persons. Second approach stipulates that liability of legal persons is only triggered by acts of persons with the highest-level managerial authority. Furthermore, Annex I provide that Member countries should ensure that, in accordance with Article 1 of the OECD Anti-bribery Convention, and the principle of functional equivalence in Commentary 2 to the OECD Anti-bribery Convention, a legal person cannot avoid responsibility by using intermediaries, including related legal persons, to offer, promise or give a bribe to a foreign public official on its behalf. flexible and reflects the wide variety of decision-making systems in legal persons. B&H is not party to the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. Significant influence for establishment of liability of legal persons also had FATF Recommendations that set out the essential measures that countries should have in place to enhance the transparency and availability of beneficial ownership information of legal persons and arrangements (See: FATF, 2012).

[71] The United Nations Convention against transnational organized crime (General Assembly Resolution 55/25 of 15 November 2000) in Article 10 prescribes liability of legal persons for participation in serious crimes involving an organized criminal group and for offences established in Arts. 5, 6, 8 and 23 of this Convention. Liability of legal persons may be criminal, civil or administrative, and such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences. B&H signed the Convention on 12 December 2000, and it was ratified on 24 April 2002. The United Nations have addressed the matter of liability of legal persons also in the International Convention for the suppression of the financing of terrorism in the Article 5 and in the Convention against corruption in the Article 26. In the former document it is stipulated that parties of this Convention shall take the necessary measures „to enable a legal entity located in its territory or organized under its laws to be held liable when a person responsible for the management or control of that legal entity has, in that capacity, committed an offence as set forth in Article 2.". Liability of legal entities may be criminal, civil or administrative; and such liability is incurred without prejudice to the criminal liability of individuals who have committed the offences - Art. 5(2). This instrument doesn't define the position of perpetrator within the legal person nor its connection to the *actus reus* of offence.

cover for committing criminal offences) and especially their resulting consequences: instigated damage and generated benefits for legal persons. Notwithstanding the incentives for its establishment, final concept of liability of legal persons for criminal offences differs from the conceptions of that liability set forth in the international documents (conventions of the Council of Europe and by the Second Protocol to the Convention on Protection of Financial Interests of European Communities) in a sense that liability of legal persons is not linked to specific criminal offences[72] nor its limited to offences committed on the behalf, for the account or in favor of the legal person by its high – ranking individuals[73] [74].

Thus, the Criminal Code of B&H (Abbreviated: CC B&H)[75] adopts broader concept of liability given that it's not limited only to the offences committed on behalf, for account or in favor of legal person by the individual (natural person) in the leadership positions within its hierarchy. However, existence of one or more alternative forms of contribution of the managerial or supervisory bodies of the legal person to commission of a criminal offence is necessary for establishment of legal person's liability for such criminal offences. The specificities of the regulation of the liability of legal persons for criminal offences in legal system of B&H regarding: concept of a legal person, concept of liability of a legal person, and types of criminal offences for which liability can be imposed to a legal person, will be further discussed in the subsequent parts of this paper.

IV. Concept of a legal person

Unlike other countries in the region who adopted specific legislation on liability of legal persons for criminal offences[76], B&H opted to regulate liability of legal persons for

---

[72] The Criminal Law Convention on Corruption ensures that legal persons can be held liable for criminal offences of active bribery, trading in influence and money laundering; the Convention on Cybercrime requires establishment of liability of legal persons for a criminal offence established in accordance with Convention (offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; and offences related to infringements of copyright and related rights); the Second Protocol to the Convention on the protection of the European Communities´ financial interest prescribes that Member States must ensure that legal persons can be held liable for fraud, active corruption and money laundering.

[73]Which was indicated in: The Recommendation No. R(88) 18 of the Committee of Ministers to Member States concerning liability of enterprises having legal personality for offences commuted in the exercise of their activities; the Recommendation No. R(96) 8 of the Committee of Ministers to Member States on crime policy in Europe; the Criminal Law Convention on Corruption; the Convention on cybercrime; the Second Protocol to the Convention on the protection of the European Communities´ financial interest; the Convention against transnational organized crime; and the Convention for the suppression of the financing of terrorism Convention against corruption.

[74] See: Babić *et al.* (2005), Komentari krivičnih/kaznenih zakona u Bosni i Hercegovini. Sarajevo: Evropska komisija, Vijeće Evrope.

[75] „Official Gazette of B&H", no. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14, 22/15, 40/15, 35/18.

[76] Croatia – The law on liability of legal persons for criminal offences („Official Gazette of Republic of Croatia", no. 151/03, 110/07, 45/11, 143/12); Serbia - The law on liability of legal persons for criminal offences („Official Gazette of Republic of Serbia", no. 97/2008); Montenegro - The law on liability of legal persons for criminal offences („Official Gazette of Republic of Montenegro", no. 2/2007, 13/2007, 30/2012.

criminal offences through provisions of the CC B&H[77]. More specifically, criminal legislation of B&H is applicable to the legal persons in accordance with provisions of Chapter XIV of the CCB&H (Arts. 122-144)[78], which are explicitly designed for regulation of liability of legal persons for criminal offences, but also in accordance with other relevant laws of B&H[79]. Provisions of Chapter XIV represent deviation from provisions of general part of the Law that regulates criminal liability of natural persons. The CCB&H doesn't use the term „criminal liability of legal persons" but the „liability of legal persons for criminal offences". In literature is suggested that this is reflection of intention to emphasize the differences in fundaments of liability of natural and legal persons for criminal offences i.e. to reserve the usage of the term „criminal liability" and all that it entails exclusively for natural persons as perpetrators of criminal offences[80]. Having in mind previously stated, legal framework on criminal liability of legal persons in B&H consists of: provisions of Chapter IV of the CC B&H; provisions of the general section of the CC B&H; and criminal law provisions possibly contained in other B&H's laws.

Criminal law of B&H recognizes a legal person as its subject[81]. Following the premise that notion of legal person is based on a legal fiction about social construct bestowed with legal personality by legal order, the criminal legislation in B&H uses mixed approach to define the notion of a legal person. Listing of forms of legal persons (B&H, Federation of B&H, Republika Srpska, the Brčko District of B&H, canton, city, municipality, local community, every organizational form of economic enterprises and all forms of association of economic enterprises, public institutions, institutions performing credit and other banking activities, institutions for insurance of property and persons and other financial institutions, fund, political organizations, associations of citizens) is not closed given its ending indication of „other forms of associations" that meet two conditions: capacity for acquisition and usage of assets in a same way as any other institution or state authority that acquires and uses assets and recognition by the law as a legal person[82]. The „recognition by the law" refers to the concept of legal personality and whether such personality is granted to the certain associations or groupings[83]. However, substance and meaning of the legal personality is not derived from the positive law but is defined by legal theory as the ability of being holder of rights and obligations in legal transactions[84]. Furthermore, it is important to highlight that in B&H's legal system legal persons, unlike natural persons, have so called „special legal personality", which means that legal person may be holder only of those rights and obligations that are within the scope of activity for which legal person was established[85]. Limitations of special legal personality are defined through provisions of specific laws.

---

[77] And other relevant criminal laws in force: the Criminal Code of Federation of B&H (Abbreviated: CC FB&H) („Official Gazette of FB&H", no. 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16, 75/17), the Criminal Code of Republika of Srpska (Abbreviated: CCRS) („Official Gazette of RS", no. 64/17) and Criminal Code of Brcko District B&H (Abbreviated: CC BD B&H) („Official Gazette of BD B&H", no. 33/13).

[78] Arts. 126 – 148 of the CC FB&H; Arts. 103 – 122 of the CC RS and Arts. 126 – 148 of the CC BD B&H.

[79] Article 11 of the CC B&H.

[80] Babić *et al.*, 2005, p. 466.

[81] See Arts. 11 and 122-144 of the CC B&H. See also: Arts. 126 – 148 of the CC FB&H; Arts. 103 – 122 of the CC RS and Arts. 126 – 148 of the CC BD B&H.

[82] Article 1(15) of the CC B&H. Identical provision is contained in the Article 2 (11) of the CC FB&H and Article of the Article 2(13) CC BD B&H.

[83] See: Vermeulen *et al.*, 2014, p. 19.

[84] Čović, Š. (2003), *Poslovno pravo*. Sarajevo: Pravni Fakultet Univerziteta u Sarajevu, p. 41.

[85] Savremena administracija (1964), Pravni leksikon. Beograd: Savremena administracija, p. 691.

For example, the Law on companies of the Federation of B&H[86] stipulates in Article 2(2) that company is legal person that independently preforms activity of production and sale of goods and provision of services in the market for the purpose of gaining profit. The methods and moment of acquisition of legal personality are defined by the law regulating certain type of legal person, but in general, legal persons referred to in the Article 1(15) of the CCB&H obtain legal personality at the moment of their registration in appropriate record maintained by competent state authority[87]. Thus, in B&H's law entry of legal person into the specific register has a constitutive effect in regard of their capacity to be liable for criminal offences.

Nevertheless, the CC B&H narrows the circle of legal persons to which provisions on liability for criminal offences can be applied. According to the Article 122(1) of the CCB&H provisions of Chapter XIV on liability of the legal persons for a criminal offence committed by the perpetrator in the name, for the account or in favor of the legal person don't apply to the B&H, the FB&H, the RS, the BD B&H, canton, city, municipality and local community[88]. This exclusion of the legal persons of public law (i.e. prescribing their immunity) from the liability for criminal offences regardless of whether or not they acted *iure imperii* or *iure gestionis*[89] is based on the understanding that those legal persons are holders of *ius puniendi* as well as budget users, and therefore subjecting them to the liability for criminal offences would create situations of self-punishment and spilling of budget funds[90] [91].

From the abovementioned provisions of Articles 1(15) and 122 of the CC B&H it is evident that in criminal law of the B&H, notwithstanding the exclusions, both public and private entities qualify as legal persons. Even though the CC B&H doesn't directly define the notion of a legal person[92] it gives the catalogue of social structures, which are considered to be legal persons.

---

[86] „Official Gazette of Federation of B&H", no. 81/15. Similar provisions are contained in the Law on the company in the RS („Official gazette of the RS" no. 127/08, 58/09, 100/11 and 67/13) which stipulate that companies are legal persons established for performing activities for the purpose of gaining profit (Art. 2(1)).

[87] The Law on banks in the Federation of B&H („Official gazette of Federation of B&H" no 27/17); and the Law on banks in the RS („Official gazette of RS", no. 3/16).

[88] Identical solution is provided in: Art. 126 of the CC FB&H; Art. 126 of the CC BD B&H; and Art. 103 of the CC RS.

[89] This solution is encouraged by international instruments such as the Criminal Law Convention on Corruption (Strasbourg, 27/01/1999), in which term „legal person" in Article 1(d) this document is defined as a „any entity having such status under the applicable national law, except for States or other public bodies in the exercise of State authority and for public international organizations.".

[90] Filipović and Ikanović, 2010, p. 18.

[91] See also: Ilić, G. P. (2010) Marginalije uz Zakon o odgovornosti pravnih lica za krivična dela, *CRIMEN* (I) 2/2010 str. 246–256.

[92] It is interesting that also other relevant laws even though they use notion of a legal person don't define it. For example, the Law on Companies of the Federation of B&H („Official Gazette of Federation of B&H", no. 81/15) stipulates in Article 2(2) that company is legal person that independently preforms activity of production and sale of goods and provision of services in the market for the purpose of gaining profit. In the Article 4 the Law on Companies in FB&H titled legal capacity stipulates that company acquires capacity of legal person by the day of entry into the register kept by court indicated by the Law on registration of business subjects in Federation of B&H. Similar provisions are contained in the Law on the Company in the RS („Official gazette of the RS" no. 127/08, 58/09, 100/11 and 67/13) which stipulate that companies are legal persons established for performing activities for the purpose of gaining profit - Article 2(1). Also, company/business enterprise acquires status of legal person upon entering into register off business subject in a manner prescribed by law regulating the registration. Entities' laws on registration of business subjects refer to business subjects as a legal person: the Law on Registration of Business Subjects in FB&H („Official gazette of FB&H", no. 27/05, 68/05, 43/09 and 63/14) and the Law on Registration of Business Subjects in RS („Official gazette of RS", no. 67/13 and 15/16).

V. Concept of liability of a legal person

Attribution of liability for criminal offences to the legal person represents complex legal issue. In B&H, grounds of liability of legal person are stipulated in the Article 124 of the CC B&H: „Legal person will be liable for criminal offence that perpetrator committed on behalf, for account or benefit of that legal person: a) when purpose of the committed criminal offence stems from conclusion, order or permission of managerial or supervisory bodies of legal person; or b) when managerial or supervisory bodies of legal person have influenced perpetrator or enabled him/her to commit a criminal offence; or c) when legal person disposes with illegally acquired financial gain or uses objects obtained by the criminal offence; or d) when managerial or supervisory bodies of legal person failed to perform due supervision over the legality of employees' work"[93]. Established concept provides liability of legal person for criminal offences under the following two conditions: 1. perpetrator committed criminal offence on behalf, for account or benefit of the legal person; and 2. presence of one or more legally prescribed forms of contribution of legal person (i.e. its managerial or supervisory bodies) to committing criminal offence by perpetrator. Having in mind previously stated, it is evident that the CC B&H adopts one form of derivative model of liability of legal person for criminal offence. In OECD study on liability of legal persons for corruption in Eastern Europe and Central Asia[94] it was stated that B&H adopted „expanded identification model" i.e. model of liability of legal person „where the liability of a legal person can be triggered by management's failure to supervise its employees ('lack of supervision rule')", which is not entirely accurate. Namely, adopted model is more extensive than suggested because it encompasses liability of a legal person not only for the offence committed by person on leading position i.e. the person belonging to company's top management or having representative powers but also for offence committed by any employee acting within the scope of his employment and with the intent to benefit the legal person. Additionally, liability of legal person exits when it disposes with illegally acquired financial gain or uses objects obtained by the criminal offence. Established model of liability will be in more detail elaborated in the following sections of this paper.

The first condition for establishment of liability of legal person refers to actions of the perpetrator of the criminal offence and second to the actions of managerial or supervisory bodies of legal person. From the phrasing used in Article 124 of the CC B&H is evident that legal person is not perpetrator of criminal offence because the acts of criminal offence refer exclusively to the natural person, and perpetrator could only be natural person[95]. Moreover, according to the relevant provision position of perpetrator within the legal person is irrelevant, i.e. it is irrelevant whether that person has leading position within the legal person or has status of employee or a member. Furthermore, the CC B&H doesn't even require existence of any formal legal relationship between perpetrator and legal person in order to impose liability for committed criminal offence.

First condition for liability of legal person is that perpetrator committed criminal offence on behalf, for account or benefit of that legal person[96]. Consequently, there must

---

[93] Identical solution is provided in: Art. 128 of the CC FB&H; Art. 128 of the CC BD B&H; and Art. 105 of the CC RS.

[94] OECD, 2015, p. 21.

[95] See: Babić *et al*., 2005, p. 466.

[96] Art. 124 of the CC B&H. Identical provision is contained in: Art. 128 of the CC FB&H; Art. 128 of the CC BD B&H; and Art. 105 of the CC RS.

be circumstance that links committed criminal offence of perpetrator with particular legal person in a manner which allows legal attribution of his/hers acts to the legal person. That circumstance is the authority of perpetrator to act on behalf, for account or benefit of the legal person. This authorization of perpetrator may result from law or another legal act such as individual act of legal person (i.e. is its managerial bodies) or contract[97]. Having in mind this, legal person may be liable for criminal offence perpetrated not only by individual on leadership position within the legal person but also by non-member of legal person if he/she committed criminal offence acting on the some kind of legal basis on behalf, for account or benefit of legal person. This first condition will be fulfilled also when act of perpetrator which represents element of criminal offence represents abuse of given authority even in the form of their overstepping. However, according to the Babić *et al*[98]. and Filipović and Ikanović[99] in that case action will be considered as action taken on behalf, for account or benefit of legal person only if overstepping relates to manner of taking of activity or on existence of requirements necessary for its performance but not when overstepping is done in a sense that act by which criminal offence was committed went outside the circle of activities to which his/hers activity relates.

Second stipulated condition further limits liability of legal person by requesting the presence of one or more alternatively prescribed forms of contribution of a legal person (i.e. its managerial or supervisory bodies) to committing criminal offence by perpetrator. The notion of „managerial or supervisory bodies" refers to the individual or collective bodies within a legal person that have authority to: represent legal person; make decisions for the legal person; and perform control within the legal person. Which bodies within the legal person have beforementioned powers is more precisely defined by provisions of specific laws regulating that form of legal person as well as by provisions of subordinate regulations created by the legal person itself (such as statute of the legal person). However, it should be noted that is argued by some authors that formal establishment of those bodies isn't required, which means inclusion of informal bodies that conduct business activities of legal person and direct its actions[100].

Actions of managerial or supervisory bodies must represent contribution to commission of criminal offence in a sense that criminal offence wouldn't be perpetrated or wouldn't be perpetrated in such manner or intent of perpetrator wouldn't be realized if there were no acts of managerial or supervisory bodies of the legal person[101]. Intensity of that contribution is relevant for decision of the prosecutor whether he/she will require initiation of criminal proceeding against legal person and if circumstances of the case indicate that contribution was of no consequence for perpetrating criminal offence prosecutor might decide not to instigate criminal proceeding[102]. It is important to note that in case when legal person operated primarily for a criminal purpose (e.g. a front for a scheme that was designed to commit fraud; or was established to participate in the illegal manufacture, importation, or distribution of a controlled substance) or operated primarily by criminal means (e.g. a hazardous waste disposal business that had no

---

[97] Babić *et al*., 2005, p. 469; Filipović and Ikanović, 2010, p. 18.
[98] Babić *et al*., 2005, p. 470.
[99] Filipović and Ikanović, 2010, p. 18.
[100] *Ibidem*, p. 33.
[101] Babić *et al*., 2005, p. 472.
[102] See: Art. 367 of the CCB&H.

legitimate means of disposing of hazardous waste) in literature and judicial practice this legal person is recognized as „criminal purpose organization"[103].

First stipulated form of contribution of the managerial or supervisory bodies requires that purpose of the committed criminal offence stems from conclusion, order or permission of managerial or supervisory bodies of legal person[104]. Conclusion, order or permission represent different types of decision making of vital bodies within the legal person who govern its operations. According to the Filipović and Ikanović, it is not necessary that they have certain official form[105].

Second form of legal person's contribution to commission of criminal offence is prescribed as influence or enabling of perpetrator to commit a criminal offence by managerial or supervisory bodies of legal person[106]. Managerial or supervisory bodies of legal person could influence perpetrator with their actions to make decision or reinforce already made decision to commit criminal offence on behalf, for account or in favor of legal person. On the other hand, enabling perpetrator to commit criminal offence entails creation of conditions for him/her to commit criminal offence or facilitation of its commission[107].

Third form of contribution of legal person to commission of a criminal offence entails specific activities of its managerial or supervisory bodies: using the illegally acquired financial gain or objects obtained by the criminal offence[108]. This behavior of managerial and supervisory bodies of legal person should be understood as confirmation of knowledge of managerial and supervisory bodies that financial gain was obtained through criminal offence as well as acceptance and approval of criminal offence and continuation of violation of protected goods and maintenance of illegal state created with that criminal offence[109].

Finally, legal person will be liable for criminal offence committed by perpetrator on behalf, for account or in favor of legal person when managerial or supervisory bodies of legal person failed to perform due supervision of legality of employees' work[110]. This contribution of legal person to commission of a criminal offence is consisted in violation of its legal duties to perform control over employees' work in terms of its compliance with relevant laws and to correct identified errors and omissions.

If requirements stipulated in Article 124 of the CC B&H are met, legal person will be liable for criminal offence even when perpetrator of the criminal offence is not guilty[111]. This indicates that criminal law of B&H doesn't tie liability of legal person for criminal offence to establishment of guilt of the natural person as perpetrator. Consequently, even in situations when grounds for exclusion of perpetrator's guilt for criminal offence, which is committed on behalf, for account or in favor of legal person, are present,

---

[103] United States Sentencing Commission (2018), Guidelines Manual, §3E1.1 (Nov. 2018), p. 523. Available at: https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2018/GLMFull.pdf;

[104] Article 124(1) (a) of the CC B&H. Identical provision is contained in: Art. 128(1)(a) of the CC FB&H; Art. 128(1)(a) of the CC BD B&H; and Art. 105(1)of the CC RS.

[105] Filipović and Ikanović, 2010., p. 35.

[106]Article 124(1)(b) of the CC B&H. Identical provision is contained in: Art. 128(1)(b) of the CC FB&H; Art. 128(1)(b) of the CC BD B&H; and Art. 105(2) of the CC RS.

[107] See: Babić *et al*., 2005.

[108] Article 124 (1) (c) of the CC B&H. Identical provision is contained in: Art. 128(1)(c) of the CC FB&H; Art. 128(1)(c) of the CC BD B&H; and Art. 105(3) of the CC RS.

[109] See: Filipović and Ikanović, 2010, p. 36; and Babić *et al*., 2005.

[110] Article 124 (1) (d) of the CC B&H. Identical provision is contained in: Art. 128(1)(d) of the CC FB&H; Art. 128(1)(d) of the CC BD B&H; and Art. 105(4) of the CC RS.

[111] Article 125(1) of the CC B&H. Identical provision is contained in the: Art. 129(1) f the CC FB&H; Art. 129(1) of the CC BD B&H; and 106(1) of the CC RS.

liability of legal person for criminal offence still can be established if one of the forms of contribution of managerial or supervisory bodies to committing criminal offence exists. Furthermore, CPC B&H in Article 375(2) stipulates that criminal proceedings against legal person can be conducted and its liability for criminal offence established even when it is not possible to initiate or conduct proceeding against the perpetrator because of the reasons provided by the law (such as: death of perpetrator, amnesty etc.). According to the Filipović and Ikanović even when actual impediment for instigating criminal proceeding exists, such as lack of evidence on reasonable doubt that identified person is perpetrator of a criminal offence, it is possible to indict legal person for that criminal offence of unidentified perpetrator and after conducting criminal proceeding to deliver a verdict that legal person is liable for criminal offence[112].

Liability of legal person for criminal offence doesn't preclude guilt of natural persons i.e. accountable persons for committed criminal offence[113].

Conditions for imposing liability to a legal person stipulated in Article 124 of the CC B&H can hint towards the *mens rea* element, however they are only criteria for the attribution of liability to the legal person, not for the establishment of the criminal offence as such. First three forms of contribution of legal person to committing criminal offence assume premeditated actions given their content. Legal person can be liable for criminal offence committed by negligence only when last form of contribution of legal person exist[114], and under these circumstances legal person can be punished les severely[115].

In case when there is no other person or bodies within the legal person beside perpetrator, which could direct or supervise perpetrator[116], the legal person will be liable for perpetrated criminal offence within the limits of the perpetrator's liability[117]. This means that when there is complete personal overlap between perpetrator and legal person i.e. between perpetrator and managerial or supervisory bodies of legal person, it is not possible to establish contribution of legal person to committing criminal offence separately from actions of perpetrator which represent criminal offence. Thus, for establishing of liability of legal person for criminal offence it is not necessary to determine some form of contribution of managerial or supervisory bodies of legal person prescribed in Article 124 of the CC B&H[118] because liability of legal person is directly related to criminal liability of perpetrator. Consequently, if guilt of perpetrator is excluded for some reason, liability of legal person for that criminal offence will be excluded as well[119].

When it comes to the impact of changes in status of a legal persons on its liability for criminal offences, the CCB&H regulates the liability of an insolvent legal person for

---

[112] Filipović and Ikanović, 2010, p. 43.

[113] Article 125(2) of the CC B&H. Identical provision is contained in the: Art. 129(2) of the CC FB&H; Art. 129(2) of the CC BD B&H; and 106(2) of the CC RS.

[114] Article 125(3) of the CC B&H. Identical provision is contained in the: Art. 129(3) of the CC FB&H; Art. 129(3) of the CC BD B&H; and 106(3) of the CC RS.

[115] *Ibidem*.

[116] This provision refers to two types of legal persons: legal persons who have no other person in their membership other than a perpetrator and a legal person who, besides the perpetrator, have no bodies to direct or control the perpetrator (a legal person in its structure has other members other than a perpetrator, but there is no body personally different from the perpetrator that could oversee or direct the perpetrator (Babić, *et al.* 2005:474).

[117] Article 125(4) of the CC B&H. Identical provision is contained in the: Art. 129(4) of the CC FB&H; Art. 129(4) of the CC BD B&H; and 106(4) of the CC RS.

[118] Also: Art. 128 of the CC FB&H; Art. 128 of the CC BD B&H; and Art. 105 of the CC RS.

[119] (See: Filipović and Ikanović, 2010:44; Babić *et al.,* 2005).

criminal offences, i.e. influence of insolvency on the liability for criminal offences, and the effects of the termination of the legal person on its liability for criminal offences. In first case, position taken by law is that a legal person in insolvency can be liable for a criminal offence regardless of whether the criminal offence was perpetrated before the beginning of insolvency proceedings or in meantime[120]. However, on a legal person in insolvency can't be imposed sanction, but only the security measure of confiscation of financial gain or objects acquired by criminal offence[121]. In case when legal entity had ceased to exist before the criminal proceeding has been completed, and a liability of the legal person is established in criminal proceedings, fines and other sanctions will be imposed on the legal entity which is legal successor of the liable legal person, if its managerial or supervisory bodies had knowledge of the perpetrated criminal offence, before the cessation of existence of the legal person[122]. The security measure of confiscation of the financial gain or objects acquired by criminal offence can be imposed on the legal person - legal successor only if its managerial or supervisory bodies had knowledge of the perpetrated criminal offence[123]. If the legal person has ceased to exist after completion of the criminal proceedings, the criminal sanction will be executed over legal successor as above mentioned ceases[124].

VI. Criminal offences

Important aspect of the concept of liability of legal persons refers to the criminal offences which can give rise to liability of legal persons. Generally, most countries in EU have opted for enumeration strategy selecting either families of offences or single offences for which a legal person can be held liable[125]. Quite opposite of that, B&H chose to establish liability of legal persons for all criminal offences entailed in the CC B&H as well as for other criminal offences prescribed by the other laws of B&H[126], meaning that all-inclusive criminal liability of legal persons was introduced in the legal system of B&H and no distinction is made between natural and legal persons in the sense that legal persons can be liable only for certain criminal offences. Hence, legal persons may be liable for any criminal offence prescribed by the criminal legislation of B&H. However, it should be noted that there are certain groups of criminal offences in regard to which liability of legal persons will have primacy in relation to others - such as criminal offences against economy, business and security of money transfers, corruption criminal offences, tax criminal offences against environment etc.[127]

---

[120] Article 126(1) of the CC B&H. Identical provision is contained in the: Art. 130(1) of the CC FB&H; Art. 130(1) of the CC BD B&H; and 107(1) of the CC RS.

[121] *Ibidem*.

[122] Article 126(2) of the CC B&H. Identical provision is contained in the: Art. 130(2) of the CC FB&H; Art. 130(2) of the CC BD B&H; and 107(2) of the CC RS.

[123] Article 126(3) of the CC B&H. Identical provision is contained in the: Art. 130(3) of the CC FB&H; Art. 130(3) of the CC BD B&H; and 107(3) of the CC RS.

[124] Article 126(4) of the CC B&H. Identical provision is contained in the: Art. 130(4) of the CC FB&H; Art. 130(4) of the CC BD B&H; and 107(4) of the CC RS.

[125] Vermeulen *et al*., 2012, p. 11.

[126] Article 143 of the CC B&H. Identical provision is contained in the Article 147 of the CC FB&H, Article 122 of the CC RS and Article 147 of the CC BD B&H.

[127] Filipović and Ikanović, 2010, p. 26.

VII. Methods

Beside the methods of content analysis, description and comparison, in this paper are also used methods of classification and specialization, as well as statistical method. Namely, in order to determine characteristic of liability of legal persons for criminal offences in legal system of B&H we analyzed all cases relating to legal persons (38), which are available on the official web site of the Court of B&H: http://www.sudbih.gov.ba/. Namely, research included total of 29 cases categorized as finalized. However, it is necessary to point out that very fact that our sample is consisted of published cases generates the first limitation of this research since there is a possibility that this is not definite number of cases on liability of legal persons for criminal offences heard before this judicial body. Second limitation of this research results from specific competence of the Court of B&H and exclusivity in selection of cases[128].

VIII. Findings and discussion

In our sample size out of 38 analyzed cases published on the official web site of the Court of B&H, 29 cases were categorized as finalized while 9 of cases are still in proceedings (appellate proceedings before second instance court). Thus, our critical analysis only focused on finalized cases. In our sample 93% of cases resulted with judgement that established liability of the accused legal person for certain criminal offence, and only 6,9 % of the cases resulted with acquittal.

A previously stated, criminal law of B&H recognizes a legal person as its subject. Even though the CC B&H doesn't directly define the notion of a legal person it gives the catalogue of social structures, which are considered to be legal persons. However, the CC B&H through exclusion of the legal persons of public law (the B&H, the FB&H, the RS, the BD B&H, canton, city, municipality and local community) from the liability for criminal offences narrows the circle of legal persons to which provisions on liability for criminal offences can be applied. According to the Article 122(1) of the CCB&H provisions of Chapter XIV on liability of the legal persons for a criminal offence committed by the perpetrator in the name, for the account or in favor of the legal person only applies to private legal persons: all organizational form of economic enterprises and all forms of association of economic enterprises /companies, public institutions, institutions performing credit and other banking activities, institutions for insurance of property and persons and other financial institutions, fund, political organizations, associations of citizens and other forms of associations that meet two conditions: capacity for acquisition and usage of assets in a same way as any other institution or

[128] In accordance with the provisions contained in Art. 7(1) of the Law on Court of B&H, the Court has jurisdiction over criminal offences defined in the Criminal Code of Bosnia and Herzegovina and other laws of Bosnia and Herzegovina. The following provision in Art. 7(2) of the Law on Court of B&H stipulates that the Court has further jurisdiction over criminal offences prescribed in the laws of the Federation of Bosnia and Herzegovina, the Republika Srpska and the Brčko District of Bosnia and Herzegovina when such criminal offences: a) endanger the sovereignty, territorial integrity, political independence, national security or international personality of Bosnia and Herzegovina; b) may have serious repercussions or detrimental consequences to the economy of Bosnia and Herzegovina or may have other detrimental consequences to Bosnia and Herzegovina or may cause serious economic damage or other detrimental consequences beyond the territory of an Entity or the Brčko District of Bosnia and Herzegovina.

state authority that acquires and uses assets and recognition by the law as a legal person. All cases from our sample relate to private legal persons - economic enterprises in organizational form of limited liability company. This is not unexpected, given that this type of organizational form of economic enterprises is prevalent is in B&H's business practice because it is suitable structure for family business ventures or for joint business of founders who are closely connected. Furthermore, in B&H limited liability company is not only appropriate form for small entrepreneurial capital owned by one or fewer number of founders (members) but it often appears as a form of aggregation of large entrepreneurial capital with a small number of founders - members, which is the result of the legal flexibility because in the management and regulation of internal relations dispositive norms are more applicable (unlike joint stock companies)[129].

Even though majority of countries in Europe opted for introduction of criminal liability of legal persons only for certain criminal offences or families of criminal offences[130] in legal system of B&H liability of legal persons is established as all-inclusive criminal liability of legal persons, meaning that legal persons can be liable for all criminal offences prescribed by criminal legislation and other laws. In literature it was suggested that liability of legal persons has special significance in relation to financial criminal offences[131]. Because of significant presence of legal persons in every segment of the economy, it is no surprise that at least one legal person is behind almost every serious financial criminal offence[132]. In literature, financial crime is defined as crime that involves use of deception for illegal gain, normally involving breach of trust, and some concealment of the true nature of the activities[133] or as a financially driven non-violent crime committed by business and government professionals[134]. In our sample limited liability companies were found liable in 77.8%, cases for criminal offence of tax evasion or fraud, in 11,11% of cases for organized crime in relation to money laundering; 3,7% case for organized crime in relation to tax evasion or fraud, and in 7,4% cases for customs fraud. This result is in accordance with other research[135], which established the most common motive – tax evasion for the use of creative accounting techniques with the aim to present a lower financial result than was achieved, i.e. attempt to pay less on the name of tax obligations.

However, the legal opinions on specifics of criminal liability of legal person in B&H legal framework, i.e. accepted approach that legal person cannot be guilty but only liable for criminal offence, which was committed by natural person on the behalf, for the account and in favor of legal person, were neglected in certain cases in our sample. Namely, in 26% cases in our sample was incorrectly and contrary to law indicated that legal person is guilty for criminal offence.

In criminal law of B&H is adopted concept of derivative model of liability of legal person for criminal offence, that provides liability of legal person for criminal offences under the following two conditions: 1. perpetrator committed criminal offence on behalf, for account or benefit of the legal person; and 2. presence of one or more legally prescribed forms of contribution of legal person (i.e. its managerial or supervisory

---

[129] Čović,2003, p. 292.
[130] Vermeulen et al. 2012, p. 11.
[131] See: Filipović and Ikanović, 2010, p. 26.
[132] See: Derenčinović, 2002.
[133] Picket and Picket, 2002, p. 3.
[134] Tupman, 2015, p. 4.
[135] Isaković-Kaplan, Š. (2016), Forenzičko računovodstvo. Fojnica: Štamparija Fojnica, p. 285.

bodies) to committing criminal offence by perpetrator. As previously noted, the first condition for establishment of liability of legal person refers to actions of the perpetrator of the criminal offence and second to the actions of managerial or supervisory bodies of legal person. In B&H law position of perpetrator within the legal person is immaterial, i.e. it is irrelevant whether that person has leading position within the legal person or has status of employee or a member or a non-member. In all cases in our sample, perpetrator was within the structure of limited liability company: in 90, 5% cases in our sample perpetrator was director without limitation of powers, and in 9,5 % cases it was employee of the company.

First condition for liability of legal person is that perpetrator committed criminal offence on behalf, for account or benefit of that legal person. Consequently, there must be circumstance that links committed criminal offence of perpetrator with particular legal person in a manner which allows legal attribution of his/her acts to the legal person. That circumstance is the authority of perpetrator to act on behalf, for account or benefit of the legal person on some legal basis. In our sample in 74% of the cases was just indicated that first condition is fulfilled but without any elaboration.

Second stipulated condition further limits liability of legal person by requesting the presence of one or more alternatively prescribed forms of contribution of a legal person (i.e. its managerial or supervisory bodies) to committing criminal offence by perpetrator) when purpose of the committed criminal offence stems from conclusion, order or permission of managerial or supervisory bodies of legal person; or b) when managerial or supervisory bodies of legal person have influenced perpetrator or enabled him/her to commit a criminal offence; or c) when legal person disposes with illegally acquired financial gain or uses objects obtained by the criminal offence; or d) when managerial or supervisory bodies of legal person failed to perform due supervision over the legality of employees' work". In regard to the second requirement for establishment of liability of legal person for criminal offence, in 96,3% of cases in our sample it was indicated that contribution of managerial or supervisory bodies of legal persons was determined – in 80% cases limited liability company disposed with illegally acquired financial gain; and in 20% of cases court did not offer clarification which form of contribution exist in relevant case but it was noted that the activity of the legal person was used for the commission of the criminal offense (legal person acted as criminal organization).

Criminal law of B&H doesn't tie liability of legal person for criminal offence to establishment of guilt of the natural person as perpetrator. Consequently, even in situations when grounds for exclusion of perpetrator's guilt for criminal offence, which is committed on behalf, for account or in favor of legal person, are present, liability of legal person for criminal offence still can be established if one of the forms of contribution of managerial or supervisory bodies to committing criminal offence exists. In our sample in 7,4% of cases legal person was found liable for criminal offence although guilt of the perpetrator was not established. In one case criminal proceedings couldn't be instigated due to death of perpetrator.

In two cases from our sample it was established that beside perpetrator, within the companies no other person or bodies existed that could direct or supervise perpetrator. In such situation, when complete personal overlap exists between perpetrator and legal person i.e. between perpetrator and managerial or supervisory bodies of legal person, it is not possible to establish contribution of legal person to committing criminal offence separately from actions of perpetrator which represent criminal offence. Thus, for establishing of liability of legal person for criminal offence it is not necessary to

determine some form of contribution of managerial or supervisory bodies of legal person prescribed in Article 124 of the CC B&H because liability of legal person is directly related to criminal liability of perpetrator. According to this approach, both companies in our sample were found liable for perpetrated criminal offence within the limits of the perpetrator's liability.

IX. Concluding remarks

Criminal law transformation initiated by the introduction of a new layer of criminal liability – liability of legal persons or entities is evident in many national systems and current discussion is focused on its further development with focus on concepts such as corporate negligence and corporate culture in context of global economy. B&H adopted the concept of extensive derivative model of liability of legal person in 2003 and after more than decade of its implementation it is time for evaluation of its results. One of the areas where is expected that introduction of liability of legal persons had significant impact was financial crime, due to involvement of legal persons in every segment of the economy and consequently in serious financial criminal offences. However, it is little is known about extent, structure and control of those criminal offences in context of liability of legal persons in B&H. In attempt to fill that void, we conducted research of legal framework and available case law. Results of the research described in this paper should improve knowledge on liability of legal persons for financial criminal offences, and reveal specificities of implementation of new legal solutions in practice in B&H. However, this research represents only small insight in case law of one judicial body - the Court of B&H, and thus it shouldn't be used for generalization.

References

1. Babić *et al.* (2005), Komentari krivičnih/kaznenih zakona u Bosni i Hercegovini. Sarajevo: Evropska komisija, Vijeće Evrope.

2. Bassi, A. (2016), Corporate criminal liability an analytical study with special reference to penal laws in India, pp. 69-113. Available at: http://shodhganga.inflibnet.ac.in/handle/10603/200004.

3. Brenen, K.-D. (1999), Forms of Criminal Responsibility of Organisations and Reasons for their Development. A Description of the Legal Practice in Germany, pp. 53-58. In: A. Eser, G. Heine and B. Huber (eds), *Criminal responsibility of legal and collective entities: international colloquium*. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

4. Brenner, S.N. and Molander, E.A. (1977), Is the ethics of business executives changing?, Harvard Business Review, Vol. 55, January-February, pp. 57-71.

5. Clifford Chance (2012), Corporate Liability in Europe. Available at: https://www.cliffordchance.com/briefings/2012/02/_corporate_liabilityineuropetechnicalbrochure.html.

6. Clubb, A. C. (2014),'The corporation as a city', *Journal of Financial Crime*, Vol. 21 Iss 2, pp. 191 – 203;

7. Coffee, J. C. (1999), 'Corporate Criminal Liability: An Introduction and Comparative Survey', pp. 9-39. In: A. Eser, G. Heine and B. Huber (eds), *Criminal responsibility of legal and collective entities: international colloquium*. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

8. Čović, Š. (2003), Poslovno pravo. Sarajevo: Pravni Fakultet Univerziteta u Sarajevu.

9. Dandurand, Y. (1999), Entertaining Realistic Expectations About the Effect of Criminal Sanctions Imposed on Corporate Entities: Canada, pp. 267- 276. In: A. Eser, G. Heine and B. Huber (eds), *Criminal responsibility of legal and collective entities: international colloquium*. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

10. De Maglie, C. (2005), 'Models of Corporate Criminal Liability in Comparative Law', *Global Stud. L. Rev.* 547, pp. 547-566. Available at: http://openscholarship.wustl.edu/law_globalstudies/vol4/iss3/4.

11. Derenčinović, D. 2002, 'Odgovornost pravnih osoba u hrvatskom kaznenom pravu', *Hrvatska pravna revija*, pp. 1-22. Available at: https://www.pravo.unizg.hr/_download/repository/Derencinovic_D.%2C_Odgovornost_pravnih_osoba_u_hrvatskom_kaznenom_pravu.pdf.

12. Dobbin, M. (1998), *The Myth of the Good Corporate Citizen*, Stoddart Pub: Toronto.

13. Economic & Social Research Council. (2012, December 13). Data on financial crime is not credible, UK research finds. *Science Daily*. Available at: www.sciencedaily.com/releases/2012/12/121213193137.htm.

14. Eidam, G. (1999), Forms of Criminal Responsibility of Organisations: Aspects of Legal Practice in Germany, pp. 59-66. In: A. Eser, G. Heine and B. Huber (eds), *Criminal responsibility of legal and collective entities: international colloquium*. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht;

15. Eisenberg, P. (2017) „Financial crime – is there any way out of the theoretical deadlock*?", Journal of Financial Crime*, Vol. 24 Issue: 4, pp. 529-540.

16. Friedrichs, D.O. (2009), *Trusted criminals: white collar crime in contemporary society*. Belmont, CA: Wadsworth Cengage Learning.

17. Filipović and Ikanović (2010), *Krivični postupak protiv pravnih lica.* Available at: https://vstv.pravosudje.ba/vstv/faces/docservlet?p_id_doc=4859.

18. Foerschler, A. (1990) 'Corporate Criminal Intent: Toward a Better Understanding of Corporate Misconduct', *California Law Review*, Vol. 78, Iss. 5, pp. 1289-1290; available at: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4440&context=californialawreview

19. Godwin Muhwezi, M. (2016), *The Case for Corporate Criminal Liability*, pp. 1-47. Available at: https://www.researchgate.net/publication/309041784_THE_CASE_FOR_CORPORATE_CRIMINAL_LIABILITY.

20. Gobert, J. and Punch, M. (2003), *Rethinking Corporate Crime*. Cambridge: Cambridge University Press.

21. Gottschalk, (2010), 'Categories of financial crime', *Journal of Financial Crime*, Vol. 17 Iss: 4, pp. 441 – 458.

22. Gerber, J. and Jensen E. L. (2000), 'Controlling Transnational Corporations: The Role of Governmental Entities and Grassroots Organizations in Combating White-Collar Crime', *International Journal of Offender Therapy and Comparative Criminology*, Vol. 44, Iss. 6, pp. 692-713, available at: https://pdfs.semanticscholar.org/0551/bd8af2a8c0019980322720eb3018aa692e50.pdf.

23. Ilić, G. P. (2010) Marginalije uz Zakon o odgovornosti pravnih lica za krivična dela, CRIMEN (I) 2/2010 str. 246–256.

24. Isaković-Kaplan, Š. (2016), Forenzičko računovodstvo. Fojnica: Štamparija Fojnica.

25. Heine, G. (1998), *„Sanctions in the Field of Corporate Criminal Liability".* Paper presented at the International Colloquium on Criminal Responsibility of Legal and Collective Entities. 4-6 May 1998. Berlin, Germany.

26. Hansen, L. L. (2009) „Corporate financial crime: social diagnosis and treatment", *Journal of Financial Crime*, Vol. 16 Issue: 1, pp. 28-40, available at: https://doi.org/10.1108/13590790910924948.

27. Lederman, E. (2000), Models for Imposing Corporate Criminal Liability: From Adaptation and Imitation Toward Aggregation and the Search for Self-Identity *Buffalo Criminal Law Review*, Vol. 4 No. 1; pp. 641-708.

28. Morris, B. (2008), „Corporate convicts: where are they now?", *Fortune Magazine*, Vol. 157 No. 12.

29. OECD (2015), *Liability of Legal Persons for Corruption in Eastern Europe and Central Asia*. Available at: https://www.oecd.org/corruption/ACN-Liability-of-Legal-Persons-2015.pdf.

30. Picket, K. H. and Picket, J. (2002), Financial Crime Investigation and Control. New York: John Wiley and Sons, Inc.

31. Pontell, H. N., *et al*. (1994), Corporate crime and criminal justice system capacity: Government response to financial institution fraud, *Justice Quarterly*, Vol. 11, Iss. 3, pp. 383-410.

32. Pop, A. I. (2006), *Criminal Liability of Corporations—Comparative Jurisprudence*. Available at: https://digitalcommons.law.msu.edu/king/81.

33. Préfontain, D. (1999), Effective Criminal Sanctions Against Corporate Entities: Canada, pp. 277- 284. In: A. Eser, G. Heine and B. Huber (eds), *Criminal responsibility of legal and collective entities: international colloquium*. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

34. Pudovochkin Yu. E. and Adrianov V.K. (2015), 'Principles of criminal law: Immersion in theory', Journal of Easstern-European Criminal Law, no. 1/2016, pp 201-207.

35. Quaid, J. A. (1998), The assessment of corporate criminal liability on the basis of corporate identity: An analysis. *McGill Law Journal* Volume 43, pp. 67–114.

36. Savić, V-I, (2011), Koncept autonomne odgovornosti pravne osobe i njegova primjena u kaznenom pravu, *Godišnjak Akademije pravnih znanosti Hrvatske*, Vol. II No. 1, 2011, pp. 41-68.

37. Savremena administracija (1964), Pravni leksikon. Beograd: Savremena administracija.

38. Stanila, L. (2014), Criminal Liability of Legal Persons. History, Evolution and Trends in Romanian Criminal Law, Journal of Eastern European Criminal Law issue 1/2014. Available at SSRN: https://ssrn.com/abstract=2462414.

39. Sun Beale, S. and Safwat, A. (2004) What Developments in Western Europe Tell Us About American Critiques of Corporate Criminal Liability, 8 *Buffalo Criminal Law Review* 89-163. Available at: https://scholarship.law.duke.edu/faculty_scholarship/ 1241.

40. Tupman, W. (2015), 'The characteristics of economic crime and criminals', pp-3-14. In: B. Rider (ed) *Research Handbook on International Financial Crime*. Cheltenham, Northampton: Edward Elgar Publishing Limited.

41. United States Sentencing Commission (2018), Guidelines Manual, §3E1.1 (Nov. 2018). Available at: https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/ 2018/GLMFull.pdf.

42. Vermeulen *et al*. (2012), Liability of legal persons for offences in the EU, Principal European Commission DG Justice (JLS/2010/JPEN/PR/1009/E4). Antwerpen, Apeldoorn,

Portland: Maklu-Publishers. Available at: https://publications.europa.eu/ en/publication-detail/-/publication/e6a11989-48d3-41a1-b4ee-8f7051d84253/language-en.

43. Walburg, C. (2015) The measurement of corporate crime: an exercise in futility?, pp. 25-38. In: J.v. Erp, W. Huisman and Vwalle (Eds.),*The Routledge Handbook of White-Collar and Corporate Crime in Europe.* Oxon: Routledge.

44. Wells, C. (1994), 'Corporate Liability and Consumer Protection: Tesco v Nattrass Revisited', *The Modern Law Review* Vol. 57, No. 5, pp. 817-823.

45. Wells, C. (1999) 'The Millennium Bug and Corporate Criminal Liability', *The Journal of Information, Law and Technology (JILT)*, Available at: https://warwick.ac.uk/ fac/soc/law/elj/jilt/1999_2/wells.

On a new tool to combat tax evasion

Prof. Dr. Csaba Szilovics*
University of Pécs, Faculty of law
Department of Financial Law

Abstract

In these days the Hungarian government accommodating the new tools in the fight against the tax fraud, and tax avoidance. These new appliances mostly use the digital world elements, like Online cash register, Electronic Public Road Trade Control System (EKÁER), digital billing system and HU-GO network system. Therefore, in the last few years the Hungarian central budgeting proceeds dynamically increased, and strongly reduced the moonlight economy. This essay introduces some aspects of this process.

Keywords*: tax fraud, tax administration, digital government, VAT, central budgeting, transport, billing, HU-GO, EKÁER.*

I. Introduction

The functioning of the state partly depends on the efficient and fair tax system that essentially influences the functioning of the public finance system, the state and the economy, and the quality of life of the citizens. There has been quite a lively discourse on this subject in the past decade, in domestic and international academic and political discourse[1]. Criticisms and professional statements expressed have sometimes had a strong impact on national tax laws, tax laws, tax incentives, tax rates, and the relationship between clients and the tax office. Nonetheless, the fact that all countries apply and shape their tax policies[2], depending on their fiscal position and economic-policy goals, and quite often create substantial differences between the public-finance duties of natural persons and companies thereby, remains unchanged[3]. Several researches have pointed out that a tax situation has emerged in some states in Asia and Central and Eastern Europe that is disadvantageous for natural persons, and as a consequence of their excessive taxation, they have to pay more public expenses than necessary[4].

The players of corporate sector benefit from a significant tax advantage in several countries, including Hungary, Croatia, Romania, Vietnam and China, in order to increase

---

* Email: *szilovics.csaba@ajk.pte.hu*

[1] As far as foreign publications are concerned T. Pikkety, J. Stiglitz,G. Tullock are relevant, while, in terms of domestic literature, authors like Cs. Szilovics, Z.Pogátcsa, T. Erdős, and Cs. Leitner. Cs should be taken into considerations

[2] See in more detail at P. Elek and Á. Scharle: *Optimális adózáselméletek és az empirikus mérés lehetőségei*, Közpénzügyek adópolitika és adórendszer 2008. 3.szám, pp. 442-450

[3] István Muzslay: *Gazdaság és erkölcs, Studia Theologica Budapestinensia*, Márton Áron Kiadó, 1993.; T. Erdős.: *Adóztatás, hatékonyság és gazdasági növekedés*, Közgazdasági szemle, LXI., January 2014. pp. 1-26.

[4] R. S. Avi. Yohan, N. Sartori, O. Marian: *Global Perspectives on Income Taxation Law*, Oxford University Press 2011; J. Martinez – Vazquez, M.Rider, S. Wallace- *Tax Reform in Russia*, Chelthenham UK, 2008; Z. Pogátsa: *A skandináv modell Magyarországi esélyeiről*, 2016; Cs. Szilovics, *Néhány közép-európai ország adóváltozásainak tapasztalatai az elmúlt két évtizedben*, Jura 2018/ 1.; Vito Tanzi: *Adóreformok a piacgazdaságba való átmenet során: a fő kérdések*, Szociálpolitikai Értesítő, 1993.

investment and employment. These allowances may come in the shape of tax exemptions, individual or normative state subsidies or in the form of providing premises at a discounted rate. As a result of these measures, as in many other countries, the specific budget contribution of the large-corporation sector fell in Hungary as well. In this country, the 11 largest companies in the country produced 25% of GDP in 2015, but only 2% of the corporate tax burden was paid by them. At the same time, it also must be noted that the Hungarian Tax Office and several independent investigations have found that the rate of VAT fraud and tax evasion are also significant in this sector[5].

According to the experience of the authorities, abuses most frequently occur in the transactions between member states involving a large amount of bulk goods difficult to identify (sugar, edible oil, chocolate, flour). Some of the entrepreneurs abuse the rules of tax-free sales between EU Member States. It is a common practice to abuse tax-exempt status of export activity by using fictitious transport documents to sell products in Hungary, which have not actually been exported from the country, without paying public debts. The inspectors of the tax national authorities have also revealed that ex-post inspection of commercial transaction of goods based solely on documents are not sufficiently effective. In the course of the inspections, it was also a challenge fact that fraudulent taxpayers produced unlimited number of copies of the international transport documents and used them as they were not subject to strict accounting regulations. Well-prepared and organized criminal groups could produce and use a large number of fictitious invoices and rely heavily on a large-scale network of companies and dormant firms. These perpetrators could exchange shipping documents and invoices, misleading the authority, and frequently changing their contributing companies, bank accounts, and headquarters. Some of the members of the chain of suppliers have often disappeared during the audit or involved cross-border companies both on the seller's and on the customer side, making it even more difficult to control them.

In order to fight back the challenge posed by the unlawful steps of these fraudulent companies, causing significant damage to the state budget and the society, a control system had to be established which could enable the tax administration to overview and keep track of the economic activities continuously and in real-time. Although natural persons are also involved in sales without invoices and the grey economy, it is clear that different tax groups require the use of different control techniques in practice. Only segmented tax administration, which is perfectly aware of and responsive to taxation activity characteristics of taxpayers, can only be effective.

This kind of targeted toolkit for improving legal control and compliance for Hungarian companies was developed and implemented by the Hungarian government between 2012 and 2018, a. This package included the obligation to use online cash registers[6], the introduction of reverse VAT, the targeted reduction of VAT rates, the introduction of the Electronic Public Road Trade Control System (EKÁER) and the provision of online invoicing.

---

[5] For the topic of tax evasion, see also R. W. McGee, The Philosophy Of taxation And Public Finance, Kluwer Academic Publishers London, 2004, pp. 75-79; A. Semjén, Z. Szántó, I.J. Tóth., *Adócsalás és adóigazgatás*,Tárki Bp 2001, p. 120; The Challenge of Tax Administration Until The End Of The 20th Century, International Bureau Of Fiscal Documentation Amsterdam No.35, 1984.

[6] Az online kasszákhoz kapcsolódó szabályozás 2017-ben, Adó Online, 2017 https://ado.hu/rovatok/ado/az-online-kasszakhoz-kapcsolodo-szabalyozas-2017-ben Bevált és tervezett eszközök az áfacsalások elleni harcban,A XVII. Európai ÁFA Konferencia anyaga, https://www.kkvhaz.hu/cikk/2307-bevalt-es-tervezett-eszkozok-az-afacsalasok-elleni-harcban.

II. Objectives and functional features of new anti-tax fraud tools

This complex package of measures partly intended to broaden the tax base without raising taxes, while other elements wanted to reduce the size of the black economy, reducing the extent of unlawful benefits. The common feature of each step in the change is that it is counts on the increased cooperation of taxpayers and either reduces the paperwork included in taxation or broadens the database of control with technical means without putting significant extra burden on the customers. In other words, most elements of the package of measures were designed to provide a more accurate and real-time overview, and by developing a new database to provide information about the real processes of the economy. An efficient operation is primary based on the condition that the activity of the business sphere should not become a baffling puzzle for the tax office. It can be stated that any means that improve transparency will increase the efficiency of the tax office at the same time. However, this new approach should not only cover the development of digital devices, but also the development of a cooperative tax-office model. Digitalisation should also be used to improve keeping contact with customers, as well as to get a feedback regarding the opinion of taxpayers, for media monitoring, and for processing information received from domestic and international partner organisations.

Electronic development is likely to be the most effective tool for monitoring. Although voluntary compliance is an important element in the functioning of every tax system, it bears at least the same importance for taxpayers to continuously perceive the presence of state's control[7]. One of the least disturbing ways of it for taxpayers can be the enforcement of mandatory electronic steps incorporated into electronic communication, control and taxation process[8]. The use of them can reduce the time spent on monitoring and increase its effectiveness as the available official database can have a significant probative role in the proceedings. The level of compliance can increase because control is continuous, the risk of being caught is high, and the legal compliance does not require a great deal of intellectual effort or financial expense from the taxpayer either. These tools help to build good tax and public finance practices with state involvement and a small willingness to cooperate by the taxpayers. Studies on lawful conduct of taxpayers have demonstrated that compliance with tax obligations has been transformed into routine procedures for the vast majority of cases and taxpayers follow the same correct or incorrect tax pattern until it is changed by an audit[9]. The development of a good practice can help build a control system that is operated as a part of day-to-day work, and continuously informs the taxpayer and the tax office about the tasks and their fulfilment. Since VAT account for the majority of budget revenues, that is 20% or 25% of it[10], it is advisable to incorporate the new means of control into the system of VAT management of companies. In my study, I am presenting the operation the most important and effective element of these tools in Hungary that is the EKÁER system.

---

[7] Adó Online, Adóelkerülés: indulnak az akciótervek https://ado.hu/rovatok/ado/adoelkerules-indulnak-az-akciotervek

[8] Cs. Kriskó, B. Locskai: *Elektronikus ügyintézés az adóhivatalban*. Budapest, Saldo Kiadó, 2008; I. Futó.: *Az elektronikus adóhivatal*, Adóvilág 2002/9

[9] *See also*: Csa. Szilovics, *Csalás és jogkövetés az adójogban*, Gondolat Könyvkiadó, 2003.

[10] J. McGee, *The Philosophy Of taxation And Public Finance*, Kluwer Academic Publishers London, 2004, pp. 75-79.

III. What is the essence of Electronic Public Road Trade Control System (EÁKER)?

EKÁER was established and operated by the Hungarian National Tax and Customs Administration, as a technical system for monitoring, checking and registering the movement of goods, with the primary aim to reduce the number of abuses related to the shipment of goods and to reduce the number of fraudulent VAT transactions. The system covers transactions between Member States and movements of goods for sale to the first domestic non-end user, as well as the electronic recording of the data specified by the law by the tax authorities in advance, and the notification of the carriage. This can indirectly result in the whitening of the black economy, as by mapping the actual movement of goods, the legal history of the products delivered can be traced back by the joint application of NAV and HU-GO[11]. With these two digital systems, it is possible to significantly reduce the volume of untaxed merchandise, since it can only be legally marketed by means of road transport which has been duly announced in advance. This tool indirectly protects fair market participants, bona fide buyers, and improves the level of equal contribution to public burden, and helps to establish the soundness of government statistics and economic-policy plans.

IV. The legal background of the control system

This area of law is governed directly by three legal norms. First of all, the Act XCII of 2003 on the Order of Taxation and the CLI and CLII Laws of 2017, which have been in force since 2015, set out the detailed conditions for the operation of the system, the obligation to announce and provide guarantee. Secondly, the decree No. 5/2015 (II.27.) by the Ministry of National Economy on the operation of Electronic Public Road Trade Control System can be considered whereby partial rules not mentioned in the Act on the Order of Taxation are defined. Thirdly, the Decree of the Ministry of National Economy of 51/2014 (XII.31.) can be mentioned, which defines the entire scope of risky products.

V. Practical functioning of the EKÁER system

The most important element of the operation of the new system is that road transport by road vehicles with a total mass of 3.5 tonnes or more will have been subject to tolling from 1 January 2015 and before the commencement of the journey the person or company responsible for the carriage must report the planned transport to the tax office and request an EKÁER number. Those belong under the scope defined above can carry out transport activities with a valid EKÁER number only. This includes the sale of goods to and from Hungary from other Member States of the European Union and the sale or export of other products from Hungary to the Member States of the European Union or domestic imports, if it is not meant directly to the end user, and the first delivery to Hungary if the goods concerned are subject to VAT. It should also be noted that the export activity outside the EU or the imports from the same territory is also subject to permission, thus these rules apply to them either.

[11] HU-GO is a traffic monitoring camera system installed on the Hungarian public road system, which has been checking the movement of vehicles subject to toll, and generating a database of the information obtained since 2013.

The law specifies that stricter procedural rules have to be applied for so-called risky products. The range of risky products mainly include foods, such as meat, milk, butter, cheese, flour, sugar, cooking oil. In the case of products belonging to this range, consignments even under 3.5 tons of total weight, which are otherwise exempted from toll, must be announced and have them authorized in the following cases:

– If the total gross mass of the delivered product reaches 200kg for a recipient or the net value of the goods is at least of net HUF 250,000.

– In the case of more than one recipient, the total weight of the goods must reach 500kg and its net value should be of 1000,000 HUF.

The operation of the system is linked to the HU-GO national network of cameras, the operating rules of which are governed by Act LXVII 2013. Accordingly, from 1 January 2015 NAV is authorized to take over and use the digital traffic information collected by the HU-GO system. With the use of out-of-road traffic control cameras, the movement of consignments across the national road network can be accurately tracked and the data collected can be compared with the data obtained by the NAV, including the information based on EKÁER announcements. The system is also complemented by a financial guarantee scheme provided by carriers. The amount is determined based on the 45-day traffic data of the announcing company or sole proprietor, similarly to the guarantee system for excise duties.

VI. Scope of exemptions provided by law

Similarly to other financial legal standards, the legislative body concerned has also provided exempt status to a considerable group of forwarders.

The following legal entities and their means of delivery are provided with exempt status.

- Hungarian Armed Forces, Military National Security Service, Law Enforcement Bodies, Parliamentary Guard
- Official military service units (NATO) crossing Hungary for military service purpose and official and service vehicles of foreign military commanders performing official service in Hungary, in accordance with international treaties or, in the absence thereof, based on the principle of reciprocity
- Disaster management vehicles
- motor vehicles receiving exempt status based on international contracts or treaties
- humanitarian aid consignments
- vehicles carrying excisable goods or waste
- motor vehicles transporting goods subject to customs supervision under the Customs Act in force
- motor vehicles transporting mails, medicines and vehicles supplying goods covered by the law on metal trade

VII. Terms and means of notification of the carriage

Notification of the commencement of transport is one of the most important obligations of taxable subjects, even though the Act on the Rules of Taxation (hereinafter ART.) Did not include it in the taxation list of tax liabilities. The practical implementation of this has been done electronically through the „client gate" online electronic system of

state administration since its introduction with the user name and password of the notifying person. Taxpayers concerned must get these digital means before the first shipment. Otherwise, this obligation cannot be lawfully fulfilled.

The notification must be made by the taxpayer himself or by his legal representative or by his permanent agent. Section o(8) of § 22 of the Act regulates specifically the scope of the details the taxpayer or his representative must always state in full. The details requested include: the details of the dispatcher of the consignment (company name, tax ID), the exact address of loading, the details of the consignee (company name, tax ID) the address of unloading. In the case of a risky products, this scope is expanded. In this case, the exact details of the companies or businesses legitimately using the property found at the address of unloading should also be provided if it they are not the same as the details of the consignee. In addition, the taxpayer must also communicate control data with the tax office in order to check the loading and unloading (telephone number, house number, other contact details). An important element of the notification is that the type, weight, value and origin of the products of a certain ID number thus delivered should be specified and registered according to the current nomenclature in force. Besides, the purpose the entitlement and reason of transporting the product (sales, labor, storage) are also have to be specified. Carriers must also declare details of the transport vehicle (registration number, type, shipping capacity).

The most important element of the reporting process is the unique EKÁER number issued on a single occasion. This is a digital signal generated by the tax authorities, which only indicates a single consignment and expires after the transaction was completed. One shipment refers to a one-time shipping of a single shipment to a consignee shipped by one carrier, shipped by the same vehicle! However, in the case where the dispatcher have the same motor vehicle subjected to toll carried different types of goods (for example, has a consignment carried to one and the same consignee potatoes and sunflower at the same time) then in this case the different products can be declared simultaneously and the tax authorities can set one EKÁER number based on the notification.

In the case where a single dispatcher has a vehicle subject to toll carry a consignment of one or more types of products to several consignee, the number of notifications to determine the EKÁER number is based on the number of recipients. Accordingly, in the case of transport to five consignees, five EKÁER numbers must be requested before the commencement of road transport. The number acquired shall be valid for 15 days from the date of its issue and during this period the carriage shall be reported and implemented in practice and the date of loading, shipping, as well as the date of arrival (unloading) at the place of receipt shall also be reported.

Following the announcement, NAV assigns the ECÁRE number allocated to the carrier and the freight and the notified data to the product unit and quantity to be delivered, thus creating a unique digital data unit easy to be tracked. Thereby, both the legal and the actual track of this artificially created figure can be traced and monitored.

VIII. Verification of the notification obligation and legal consequences of failure

The most important consequence of breaching the the notification rules is that the unauthorized product is considered to be of arguable origin and the owner of it may be subject to a default fine of up to 40% of the value of the product. In addition, illegally

shipped products can be confiscated, unless the goods are perishable. These sanctions have been applied by the Authorities since 15 January 2015. NAV published a report on EKÁER's fining practice in 2018[12]. According to their experiences, failures are usually due to intentional human omission or lack of information. Most common mistakes include the failure to report or to meet deadlines, the use of incorrect data, and the incorrect determination of the value of the goods. According to the report the tax authorities are acting fairly in case of minor errors and imposing fines ranging from 0 to 100,000 forints regardless of the value of the goods. It is relatively rare that the highest i.e. 40% fine specified by law is imposed. This is only applied in the practices of business associations that are systemic and recurring in the practice of circumventing the tax administration system. However, the average fine does not usually exceed 15% of the value of the goods even in these cases. In other cases, when detecting minor errors not based on intentional fraud, the usual extent of fines is 4-5% of the value of the goods.

In order to ensure effective public control of freight forwarders, carriers are obliged to keep all documents accompanying the consignment with them, and to present them at the request of the authorities. Consequently, commercial quantities of products can only be legally delivered with supporting documents (bill of lading, invoice). In addition, natural persons or contractors performing carrier activity must declare the owner and the origin of the goods delivered and must provide the relevant supporting documents. If a carrier refuses to declare, does not fully support the facts included in his or her statement or makes false statements, he or she may face severe legal consequences.

One of the biggest legal deficiencies in the system's practical operation is that this procedure is lacking the option of self-audit. Thus, the business entity cannot improve its mistakes, as is the case with other areas of tax administration. In order to demonstrate its good faith, it may only record a protocol similar to a self-audit record, and it may refer to it later during a possible legal procedure. The legal procedure to be applied in this area is the same as those used for the inspection of other tax liabilities and the minutes of the agents of the tax office can be commented on and an appeal may be filed against the decision[13].

IX. First results of the application of new tools

Prior to the introduction of the new legal-technical tool, a number of Hungarian logistics and commercial professional organizations have formulated a negative opinion. One of the leaders of the Association of Hungarian Logistic Service Centres and the head of the Hungarian Association of Transportation and Logistics said[14] that the introduction of the control of goods would cause significant damage, and in the first four to five months after the introduction it might cause a chaos as it had not been tested in practice. They agreed that this device could be capable of detecting fraud on general sales tax and real-time tracking of goods to bleach the economy. They also stated that this could cause

---

[12] 5percAdó: *EKÁER bírságolási tapasztalatok, jogorvoslati lehetőségek*, https://5percado.hu/ekaer-birsagolasi-tapasztalatok-jogorvoslati-lehetosegek/

[13] 5percAdó: *EKÁER bírságolási tapasztalatok, jogorvoslati lehetőségek*, https://5percado.hu/ekaer-birsagolasi-tapasztalatok-jogorvoslati-lehetosegek/

[14] További két hónapos türelmi időszakot kér az MLSZKSZ, http://www.mlszksz.hu/hireink/41-ekaer-tovabbi-ket-honapos-turelmi-idoszakot-ker-az-mlszksz, Magyar Nemzet (on-line newspaper): Meglepően könnyen kijátszható az EKÁER, https://mno.hu/gazdasag/nagyon-konnyen-kijatszhato-ez-ekaer-1307638

some decline in the Hungarian logistics industry and that companies and investors carrying out forwarding activities might avoid the country and we would not be able to take advantage of the logistically favourable location of the country. As a result of these negative effects, the amount of VAT and corporate taxes, as well as the amount of customs revenues and employment might be reduced. According to the chairman of the Hungarian Vegetables and Fruit Inter-professional and Product Association[15], the control system can easily be circumvented by using vehicles of the 3.5 tonnes of or by falsifying freight data.

In contrast to the negative expectations that had arisen, the experts of the National Tax and Customs Administration and the Ministry of National Economy were optimistic. According to Zoltán Pankucsi, State Secretary for Tax Affairs of the Ministry of National Economy, the new system will increase tax revenues[16] in that the government does not levy new taxes, but rather would be able to collect the existing ones more efficiently. Ágnes Sinkóné Csendes[17], Taxation Director-General of NAV, says EKÁER's goal is to improve the position of lawful taxpayers, i.e. to eliminate the competitive advantage of contractors of unlawfully conduct and to help enforce the law and improve the efficiency of tax administration. This latter goal is achieved through the establishment of risk profiles created by controlling affiliated companies and the data of the notifying entities, as well as through mapping the customers' economic activities. The information gathered during the operation of the system could be used successfully in other tax audit procedures. As far as the actual budget results of the package of measures are concerned, the anticipated positive expectations have been fulfilled. As early as in the first year of the implementation, NAV and commercial organizations reported significant gains, increased sales revenue and an increased lawful economic activity, hence the grey economy declined. Companies of lawful conduct experienced a 15-20% increase in their turnover as early as in 2015. In the same year, the VAT gap, i.e. the unpaid portion of the tax, decreased by 3%. This resulted in a presumed proportion of tax evasion being reduced to 13.7% compared to the regional average of 25.5%[18]. The results of the new Hungarian system have also been recognized by the European Commission. In its 2017 report, the Commission described it as a good tool for combating tax evasion when, in 2015, the EU estimated a total of € 152 billion of tax evasion losses in the member countries[19] [20].

---

[15] További két hónapos türelmi időszakot kér az MLSZKSZ, http://www.mlszksz.hu/hireink/41-ekaer-tovabbi-ket-honapos-turelmi-idoszakot-ker-az-mlszksz, Magyar Nemzet: Meglepően könnyen kijátszható az EKÁER, https://mno.hu/gazdasag/nagyon-konnyen-kijatszhato-ez-ekaer-1307638.

[16] Előnyös hatást gyakorol az áfabevételre az ekáer, http://elelmiszer.hu/gazdasag/cikk/elonyos_hatast_gyakorol_az_afabevetelre_az_ekaer.

[17] Előnyös hatást gyakorol az áfabevételre az ekáer, http://elelmiszer.hu/gazdasag/cikk/elonyos_hatast_gyakorol_az_afabevetelre_az_ekaer.

[18] Az Európai Bizottság az EKÁER (elektronikus közútiáruforgalom – ellenőrző rendszer) szabályozási problémái miatt kötelezettségszegési eljárást indított Magyarország ellen, https://hirlevel.egov.hu/2017/10/04/az-europai-bizottsag-az-ekaer-elektronikus-kozutiaruforgalom-ellenorzo-rendszer-szabalyozasi-problemai-miatt-kotelezettsegszegesi-eljarast-inditott-magyarorszag-ellen/.

[19] It should be noted that for the application of the Hungarian EKÁER system, the European Commission called on the Hungarian government in 2017 to harmonize its national regulations with EU standards in accordance with the provisions of Council Directive 2006/112 / EC.

[20] J. Swinkels, *The Phenomeon of VAT Groups under EU Law and Their VAT – Saving Aspects* in International VAT Monitor January/ February 2010.p. 39; A.M. Jimenez, *Towards a Homogeneous Theory of Abuse in EU* (*Direct)Tax Law*, in Bulletin for International Taxation April/May 2012, p. 275.

„Fulfillment of the tax obligations related to the EKÁER system were investigated in about 25,000 cases in the first two years, and in more than 15,000 cases customs-related audits were carried out as well. As a consequence, the authorities imposed a default penalty of HUF 160 million. Due to the delivery of the goods of unproven origin, an additional HUF 230 million fines were imposed"[21]. „It may also be established that as early as in the fiscal year 2016, the expectations regarding VAT revenue increase, as well as concerning the decline in tax evasion and the black economy were met. Mihály Varga Minister of National Economy also reported similar experiences „Deployment of online cash registers and the road traffic control system, i.e. the introduction of EKÁER, yielded HUF 300-400 billion in the past two years. This is how much was paid to the state by economic operators who had previously been operating illegally or half illegally"[22]. As an indirect effect of the operation of the system, more than HUF 5.7 billion of other tax debts were settled until 30 June 2017 by companies using[23].

X. Conclusion

There is no doubt about the fact that these positive revenue outcomes and the whitening of the economy are due to these simple technical tools that had long been used in other countries. The changes were not brought about by the internal consolidation of the level of compliance or significant tax cuts, but by „only" a well thought-out electronic development of the tax office's control. Based on the positive experience in Hungary, two countries have introduced similar electronic devices. In Poland, following the Hungarian model, a road monitoring system called SENT has been operating since May 1, 2017[24]. Slovakia has been applying this technique since 2018- In addition, several countries have indicated that they are observing the experience of system operated in Hungary and are interested in its introduction. They includes Great Britain, Finland, Belgium. Fortunately, negative forecasts have not been proven, and Hungary has not lost its attraction to capital investments or logistical benefits due to EKÁER either. EKÁER seems to have become a technical means of combating tax evasion, which has repeatedly confirmed that every unit of development resources spent on fiscal control resulted in seriously increased budget revenues and thus could be a good investment even for taxpayers.

References

1. Elek, P., Scharle, Á., *Optimális adózáselméletek és az empirikus mérés lehetőségei*, Közpénzügyek adópolitika és adórendszer 2008. 3.szám.

2. Erdős T.,*Adóztatás, hatékonyság és gazdasági növekedés*, Közgazdasági szemle, LXI., January 2014.

---

[21] L. Varga: *Az EKÁER helyszíni ellenőrzésének tapasztalatai*, Adóvilág XX. 2016/7 pp. 29-31.

[22] Magyar Idők: Százmilliárdos adócsökkentés jövőre VM interview, 2017 https://magyaridok.hu/gazdasag/szazmilliardos-adocsokkentes-jovore-2456239/.

[23] Az Európai Bizottság az EKÁER (elektronikus közútiáruforgalom – ellenőrző rendszer) szabályozási problémái miatt kötelezettségszegési eljárást indított Magyarország ellen, https://hirlevel.egov.hu/2017/10/04/az-europai-bizottsag-az-ekaer-elektronikus-kozutiaruforgalom-ellenorzo-rendszer-szabalyozasi-problemai-miatt-kotelezettsegszegesi-eljarast-inditott-magyarorszag-ellen/.

[24] Lengyelország bevezette a SENT nevű rendszert, a magyar EKÁER mintájára, http://www.mkfe.hu/hu/mediamenu/hirek/aktualis-hrek/148-kulfoldi-hrek/8173-lengyelorsz%C3% A1g-bevezeti-a-sent-nev%C5%B1-rendszert,-a-magyar-ekaer-mint%C3%A1j%C3%A1ra.html

3. http://elelmiszer.hu/gazdasag/cikk/elonyos_hatast_gyakorol_az_afabevetelre_az_ekaer.

4. http://www.mkfe.hu/hu/mediamenu/hirek/aktualis-hrek/148-kulfoldi-hrek/8173-lengyelorsz%C3%A1g-bevezeti-a-sent-nev%C5%B1-rendszert,-a-magyar-ekaer-mint%C3%A1j%C3%A1ra.html

5. https://5percado.hu/ekaer-birsagolasi-tapasztalatok-jogorvoslati-lehetosegek/

6. https://ado.hu/rovatok/ado/adoelkerules-indulnak-az-akciotervek

7. https://ado.hu/rovatok/ado/az-online-kasszakhoz-kapcsolodo-szabalyozas-2017-ben https://www.kkvhaz.hu/cikk/2307-bevalt-es-tervezett-eszkozok-az-afacsalasok-elleni-harcban.

8. https://hirlevel.egov.hu/2017/10/04/az-europai-bizottsag-az-ekaer-elektronikus-kozutiaruforgalom-ellenorzo-rendszer-szabalyozasi-problemai-miatt-kotelezettsegszegesi-eljarast-inditott-magyarorszag-ellen/.

9. https://hirlevel.egov.hu/2017/10/04/az-europai-bizottsag-az-ekaer-elektronikus-kozutiaruforgalom-ellenorzo-rendszer-szabalyozasi-problemai-miatt-kotelezettsegszegesi-eljarast-inditott-magyarorszag-ellen/.

10. https://magyaridok.hu/gazdasag/szazmilliardos-adocsokkentes-jovore-2456239/.

11. Jimenez, A.M., *Towards a Homogeneous Theory of Abuse in EU* (*Direct)Tax Law*, in Bulletin for International Taxation April/May 2012.

12. Kriskó, Cs., Locskai, *Elektronikus ügyintézés az adóhivatalban*. Budapest, Saldo Kiadó, 2008; I. Futó.: *Az elektronikus adóhivatal*, Adóvilág 2002/9.

13. Magyar Nemzet (on-line newspaper): https://mno.hu/gazdasag/nagyon-konnyen-kijatszhato-ez-ekaer-1307638

14. Martinez–Vazquez, J., Rider, M., Wallace, S., *Tax Reform in Russia*, Chelthenham UK, 2008; Pogátsa, Z., *A skandináv modell Magyarországi esélyeiről*, 2016.

15. McGee, J., *The Philosophy Of taxation And Public Finance*, Kluwer Academic Publishers London, 2004.

16. McGee, R. W., *The Philosophy Of taxation And Public Finance*, Kluwer Academic Publishers London, 2004.

17. MLSZKSZ, http://www.mlszksz.hu/hireink/41-ekaer-tovabbi-ket-honapos-turelmi-idoszakot-ker-az-mlszksz.

18. Muzslay, I., *Gazdaság és erkölcs, Studia Theologica Budapestinensia*, Márton Áron Kiadó, 1993.

19. Semjén, A., Szántó, Z., Tóth, I.J., *Adócsalás és adóigazgatás*,Tárki Bp 2001, The Challenge of Tax Administration Until The End Of The 20th Century, International Bureau Of Fiscal Documentation Amsterdam No.35, 1984.

20. Swinkels, J., *The Phenomeon of VAT Groups under EU Law and Their VAT – Saving Aspects* in International VAT Monitor January/ February 2010.

21. Szilovics, Cs., *Néhány közép- európai ország adóváltozásainak tapasztalatai az elmúlt két évtizedben*, Jura 2018/ 1.

22. Szilovics, Csa., *Csalás és jogkövetés az adójogban*, Gondolat Könyvkiadó, 2003.

23. Tanzi, V., *Adóreformok a piacgazdaságba való átmenet során: a fő kérdések*, Szociálpolitikai Értesítő, 1993.

24. Varga, L., *Az EKÁER helyszíni ellenőrzésének tapasztalatai*, Adóvilág XX. 2016/7.

25. Yohan, R. S. Avi., Sartori, N., Marian O., *Global Perspectives on Income Taxation Law*, Oxford University Press 2011.

Some issues of criminal liability by reason of economic decisions

Prof. Dr. László Kőhalmi*
Head of Department of Criminology and Penal Law
Faculty of Law, University of Pécs

Abstract

Traditionally several levels of the conceptual approach to economic criminality obtains. The ordinary „average citizen" construes economic criminality as all crimes, offences or unethical conducts as a consequence of which the actors of everyday economic life gain unlawful pecuniary advantage according to public opinion

According to the approach of the broad scope of criminal law economic criminality includes not only the conducts expressly qualified as economic crime in the penal code of the particular country, but also certain crimes against property, certain official crimes, certain corruptions and certain breaches of confidentiality.

A basic difference obtains between risk and risking. The risky economic decisions of economic actors does not entail holding responsible under criminal law, if the assumed risk is permitted. Permitted risk is a kind of negative condition of culpability, which precludes criminal liability for the injury of the interest protected by criminal law via activity (assumption of risk).

Keywords: *criminal liability, economic crime, permitted risk.*

I. The concept of economic crime

According to some views economic crime is a necessary concomitant of the market economy: For prosecuting authorities of the states with socialist social establishment orientation amongst the entangled threads of economic crime implied novelty to some extent. Prosecution and law-makers equally needed time to become familiar with the operational methods of economic crime emerging along the logic of the market economy. The clarification of criminal liability is many times not unproblematic in case of economic delinquencies with a far-reaching scope of perpetrators in several cases.

In criminal sciences the status of economy is peculiar, since economic criminality is a criminological, whereas economic crime is a concept of criminal law[1].

---

* Email: *kohalmi.laszlo@ajk.pte.hu*

[1] Wiener, A. Imre, *A gazdasági bűncselekmények fogalmáról* [About definition of economic crime]. Állam-és Jogtudomány 1979/1. pp. 42-47. See: Dharma Raj Bhusal: *Economic Crime Law and Legal Practice in the context of Nepal*. Inaugural dissertation for getting a doctoral degree (doctor juris) from the Faculty of Economics and Business Administration of Chemnitz University of Technology, Germany, 2009. p. 12.: *„Economic crime including money laundering today is a part of the major transnational organized crime. It is really difficult to give an exact definition of economic crime. A person is acquiring easy money in his life in different ways which do not respect the socially accepted norms. When activities are outside of the accepted social norms, the law tries to prevent them, and then the activities are illegal and ultimately a crime. There are various motivating factors for a person to commit a crime. Those factors may be classified in various ways. A financial criminal not only attempts to accumulate money from illegal sources but its activity is also threatening the economic order and creates a hurdle for national development."*

The concept of economic criminality is necessarily broader than that of economic crime, since upon the analysis of criminality criminology according to its own viewpoints examines not only economic crime but other crime (against property and corruption[2]) as well. The legal subject of economic crime[3] is the intervention of the state, i.e., the economic management by the state construed in a broader scope into economic life[4].

We can assert that traditionally several levels of the conceptual approach to economic criminality obtains. We can frequently encounter a more or less unified ordinary concept, we can also coin a criminological definition as well as a criminal legal concept encompassing a broader, finally a narrower area of positive law. The discourse may be aggravated or misguided if we don't know at which level the opinion-maker joins the debate.

According to Mihály Tóth, the conceptual approach to economic criminality is viable at a so-called ordinary level, the criminological definition as well as the criminal legal concept of economic criminality in a broader or a narrower sense are also justified.

The ordinary „average citizen" construes economic criminality as all crimes, offences or unethical conducts as a consequence of which the actors of everyday economic life gain unlawful pecuniary advantage according to public opinion[5]. Thus, beyond the scope of actual criminals, public opinion construes as economic criminals the millionaire „businessman" or the vendor selling beer for the multiple amount of the purchase price at the beach, both of whom exploit the legal regulatory gaps, although neither of them can be held responsible in a criminal legal sense since neither of them are criminals[6]. The before-mentioned definition attached to the name of László Pusztai is undoubtedly the most general, at the same time the most imprecise and pliable by reason of its emotional touch. Ordinary economic delinquencies are marked by negative social judgement, though legal responsibility cannot be attached to these conducts[7] as Mihály Tóth assumes[8]. In such cases even the prosecuting authorities are in a difficult situation since in these conducts legal and illegal elements mingle and it is problematic to justify the culpability of the perpetrator before the penal courts.

According to the criminological approach criminality related to business management includes crimes related to economic activity[9], which may encompass corruption[10], crime against property and expressly economic crimes[11]. The Achilles heel of this definition is the formulation of conceptual content of „economic activity," since

---

[2] Tóth, Dávid, *A korrupciós bűncselekmények szabályozásának története Magyarországon* [The history of the regulation of corruption crimes in Hungary]. Büntetőjogi Szemle 2015.3. pp. 107-112.

[3] Gál, László István, *The criminal law protection of the stock market in Hungary*. Journal of Eastern-European Criminal Law 2015.2. pp. 44-46.

[4] Fehér, Lenke, *Gazdasági bűnözés, gazdasági bűncselekmények* [Economic criminality, economic crime], Jogtudományi Közlöny 1981/1. p. 74.

[5] Pusztai, László, *A gazdasági bűnözés* [Economic criminality]. In: Gönczöl Katalin – Korinek László –Lévai Miklós: Kriminológiai ismeretek – bűnözés – bűnözéskontroll [Criminological knowledge – criminality – control of criminality], Corvina Kiadó. Budapest, 1999. pp. 186 – 188.

[6] Tóth, Mihály, *A gazdasági bűnözés és bűncselekmények néhány aktuális kérdése* [Some Topical Issues of Economic Criminality and Crime], MTA Law Working Papers, 2015/4. p. 2.

[7] A so-called consensus prevails concerning the fact that company cars and company mobiles are used by the employees for private purposes or a professional training justifies a luxurious cruise.

[8] Tóth, M.. *op. cit.*, p. 3.

[9] Szilovics, Csaba: *About the Causes of Corruption in the Hungarian Public Procurement System*. Journal of Eastern-European Criminal Law 2014.2. pp. 104-106.

[10] Gál, László István, *Economic Bribery as a Part of Economic Criminal Law and a Concomitant of Political Corruption*. Journal of Eastern-European Criminal Law 2014.1. pp. 24-26.

[11] Pusztai, L., *op. cit.* It is worth noting the problems related to the taxonomic placement of money laundering.

the definition may become boundless. A further difficulty consists in the fact that the economic activity may at many times convey a meaning related to economics[12].

Furthermore, conceptual overlaps appear concerning the essential differentiae specifica of „white-collar criminality", „grey economy" and „black economy."

It is rightful to pose the question whether the broker committing a brokerage fraud of billions is a white-collar criminal, an economic criminal, fraudster, embezzler or none of these.

According to Mihály Tóth in criminological terms economic criminality is deemed to be accomplished in the process of business management or a form of criminality closely related to it, which with respect to the method of commission (frequently via using or abusing the legal forms and framework of business management) or its result is suitable to injure or jeopardise primarily and typically the order and obligations of business management as well as the framework of honest and lawful management beyond injuring contingent individual interests[13].

According to the approach of the broad scope of criminal law[14] economic criminality includes not only the conducts expressly qualified as economic crime in the penal code of the particular country, but also certain crimes against property (e.g., fraudulence, negligence, fraud, embezzlement), certain official crimes (e.g., abuse of office), certain corruptions (e.g., bribery) and certain breaches of confidentiality (e.g., the breach of trade secret)[15].

According to the approach of the narrow scope of criminal law economic criminality consists in the totality of prohibited conducts enumerated in the chapter of „economic crime" in the penal code of the particular country.

Antal Fonyó draws our attention to the fact that the demarcation of economic crime, the method of the establishment of the relevant legal facts of the cases pose a unique and difficult task to makers of criminal law both from legal political and legal technical viewpoints, because the changing criteria via which crime against property and economic crime can be distinguished are based on rather „relative values"[16]. According to Mihály Tóth, no really unequivocal demarcation can be accomplished owing to the equivalence of the forms of ownership and the mingling of property and management relations. What can be established is that both economic criminality and crime against property injure property

---

[12] Tóth. M., *op. cit.*, p. 4. E.g., The author who intends to describe the conceptual differences and the sameness of „black economy," „grey economy" or „white-collar criminality" takes on a rather difficult scientific task of legal interpretation.

[13] Tóth, M., *op. cit.*, p. 5.

[14] It is only a peculiarity that Imre A. Wiener, who had a definitive ideological role in Hungarian economic criminal law for a long time distinguished the so-called internal and external economic crimes. I do not agree with this typology. According to Tamás Sárközy internal economic crimes do not directly injure economic and production relations (only indirectly), but they do injure the external component of the economic system, the form of business management entangled with political, legal and other elements. The activity of the direction of the economy by the state is only one component of the forms of business management. Internal economic crime is basically designed to protect the totality of the forms of business management via criminal law. See more amply, Sárközy, Tamás, *A „belső" gazdasági bűncselekmények alapvető anyagi jogi kérdései* [Basic substantive legal issues of „internal" economic crime], Jogtudományi Közlöny 1968/1. pp. 25 -26.

[15] Of course, it is difficult to present an exact basis for the enumeration.

[16] Fonyó, Antal, *A gazdálkodási kötelességeket sértő bűncselekmények* [Crimes Violating the Obligations of Business Management] in Bodgál-Bodrogi-Erdősy-Fonyó-Gál-Gáspár-Kovács-Pintér-Wéber: Magyar büntetőjog - Különös Rész [Hungarian Criminal Law. The Special Part], BM Könyvkiadó, Budapest, 1981, pp. 116-117.; See further, Fonyó, Antal, *A gazdasági bűncselekmények fogalma* [The concept of economic crime], Kandidátusi értekezés tézisei [Thesis of candidate dissertations]. Szeged. 1961. p. 10.

relations, however, economic criminality is peculiarly related to the process of business management (production, manufacturing, distribution, circulation), whereas crime against property manifests itself not in these processes, but in the violation of the property and ownership relations topical at the time of commission.

According to Tóth we can establish that economic criminality injures or jeopardises legal interests always in certain dynamic, mobile systems of relations necessarily attached to these, whereas crime against property is generally static and violates a certain situation, a state, property relations independent of processes.

II. The conception of the so-called socialist criminal law on economic criminal liability

In socialist states under the totalitarian nightmare of the Marxist ideology the predominant view was that in the state of socialism, or in its superior social conformation, i.e., in communism criminality simply withers and ceases. If and so far as criminality sustains in socialism, its cause is the infiltration of retrograde, bourgeois elements into the countries of the socialist block. Namely, the socialist human being is superior to the „Western" human being, that is, the citizens of capitalist states. The morality of the socialist man is more developed than that of their western counterparts, therefore, they do not commit crimes. If somebody does commit crimes, they are apparently insane, because they do not recognise the superiority of socialism, consequently, they need to be confined to mental hospitals (or in a better case to prison).

This encompasses the conception of the official politics about criminality. This was supported by several „scientific" mercenary pen-pushers, who elaborated plenty of pseudo-scientific theories, on the basis of which the so-called Marxist foundation of criminal liability was concocted. The predominance of the conformity of scientific logics to the rules was not important, but a striking, relevant quotation from the classicists of Marxism (Marx, Engels or Lenin) needed to be found and explicated and in the end the given problem was covered with a pseudo-scientific, seemingly criminal legal sauce.

There were few scientists who took the courage and escaped this Marxist and pseudo-scientific play, by risking their existence they intended to fulfil the requirements of penology instead of the ideological expectations of the state party.

According to my opinion one of the most significant figures of the modern Hungarian science of criminal law, Emil Erdősy did not conform to socialist expectations, but in case of economic crime he endeavoured to determine the essential criteria of criminal liability in terms of the aspects of the bourgeois science of law.

III. Risk manifest in economic life and criminal liability

The expression of risk has a fairly broad scope of meaning, however, the science of law including criminal law can exploit only a narrow scope of its meaning.

First of all, we need to set forth that neither the professional, nor the everyday usage makes a sharp distinction between the concepts of risk and risking (assumption of risk), although they should.

Risk has a dual meaning: on the one hand, it means the main feature of the given conduct, in particular, uncertainty, the possibility of the occurrence of drawback, on the

other hand, it implies the human activity itself[17], which occurs on the basis of a conscious decision under circumstances with uncertain outcome as Emil Erdősy formulates[18].

A basic difference obtains between risk and risking. According to Emil Erdősy risk is inseparable from human conduct, since „it emerges via the conduct, although we do not identify it with the conduct as phenomenon since risk in itself is not a phenomenon, but it is a feature which marks the conduct with peculiar nature." Risk is merely a feature of the given conduct, the possibility of hazard, damage, trouble or inconvenience incurred by the activity or undertaking[19].

Risking (the assumption of risk)[20], however, means human conduct, „subordination or conscious subjugation with a view to a definite objective..." In the course of this either the intended consequence or some detrimental outcome (the destruction of a property) may occur. According to Emil Erdősy risking is a purposeful conduct with uncertain outcome[21].

Risk in terms of criminal law postulates culpability, because it may be mentioned only related to conducts which qualify as crime[22]. The criminal legal relevance of risk crops up when it is unsuccessful. The unsuccessful assumption of risk and crime belong to the same group of phenomena[23].

The objective feature of risking is the uncertainty of the activity, that is, the risking person does not know all conditions of the conduct, namely, (s)he commences a process of activity which involves the possibility of inauspicious consequence[24], e.g., the managing director of a property renovating company purchases a property at a very favourable price without having seen it first. Criminal law designates this as a hazardous situation.

The subjective substantial element of risking is purposefulness. The condition of the enforceability of criminal liability is jeopardising or the actual injury of values protected by criminal law[25].

The risky economic decisions of economic actors (e.g., managing director) does not entail holding responsible under criminal law, if the assumed risk is permitted. According to Emil Erdősy permitted risk is a kind of negative condition of culpability,

---

[17] It is worth paying attention to the extraordinarily pithy thoughts of Ferenc Irk published in this topic: *„(…) Risk is closely related to human behaviour, to an activity, doing or not doing. In my opinion risk may become what it is when man has recognised or could have recognised the hazards of some phenomenon or activity. We generally do not speak of the risk of high tide, at most only with respect to those countries where we have recognised that this physical phenomenon may incur danger or do damage to man. Risk not recognised by man does not fall under the concept of risk even if according to a later realisation it really incurred danger. We have mentioned the risk entailed by certain pesticides or insecticides since we had recognised their harmful effect to health. Thence only from this time on is man capable of risking as a form of action."* See more amply, Irk, Ferenc: *A rizikó és a gondatlan bűncselekmények* [Risk and Negligent Crimes)], Jogtudományi Közlöny 1980/3. pp. 180-181.

[18] Erdősy, Emil, *A megengedett kockázat a büntetőjogban* [Permitted Risk in Criminal Law], Akadémiai Kiadó, Budapest, 1988. p. 12.

[19] Interpretational Dictionary of Hungarian Language.

[20] *See* Wiener A. Imre: *Kockázat és bűnösség* [Risk and culpability]. Állam-és Jogtudomány 1972/1. pp. 93-99.

[21] Erdősy, E., *op. cit.*, p. 13.

[22] Erdőy, E., *op. cit.*, p. 32.

[23] Erdősy, E., *op. cit.*, p. 65.

[24] Erdősy, E., *op. cit.*, p. 66.

[25] See further, Wiener, A. Imre, *A gazdasági vezetőknek a beosztottak bűncselekményéhez kapcsolódó büntetőjogi felelőssége* [The criminal liability of managers for the crimes of their subordinates], Magyar Jog 2003/12. pp. 706-708.

which precludes criminal liability for the injury of the interest protected by criminal law via activity (assumption of risk)[26].

In his monography titled *„permitted risk"* Emil Erdősy expounds that the differentiae specifica of the concept are as follows:

- The basis of risking is some specific social necessity.
- The hazard incurred by risking is proportionate to the expected social benefit.
- The risk contains the necessary safety conditions.
- The risky decision is realistically founded.
- The risky decision is directed by socially useful objective[27].

Upon making decisions on criminal liability, criminal courts should proceed with due respect to the aspects above. However, practice unfortunately indicates that decisions by the magistrates often lack this conceptual scheme.

IV. Permitted economic risk

The regrettable concomitant of economic life is risk. Economic risk proceeds fundamentally from the uncertainty related to economic activity since economic life, the operational mechanisms of the economy are extraordinarily complex and unpredictable. The consequences of economic decisions, their overall effects cannot be determined with complete accuracy[28].

So far as we accept the statements above, we may rightfully pose the question: on what basis is criminal legal consequence attached to an unforeseeable and unpredictable process?

In economic life the purchase of valueless shares may qualify as a totally faulty decision. However, after some weeks when it turns out that valuable and easily exploitable gold deposits can be found on the territory of the shareholding, the price of the shares soars. Of course, the opposite may also be true: a seemingly shell-proof investment may become complete bankruptcy, since the estates of the company are radioactively contaminated.

Economic risk differs from other kinds of risk (transport risk, medical risk, sports risk, technical risk) inasmuch as in its emergence and formation concrete political, social, economic and legal factors are determining. In our days, unfortunately, the profitable operation of a company may be promptly devastated by politics, whereas political support may create billionaires out of unworthy entrepreneurs.

Erdősy defines the particular features of economic risk as follows:

- the object of risk: financial value or pecuniary relationship[29]
- in the majority of given cases the interaction of series of conducts shapes the final consequence
- in some cases it can be measured, while in other cases it cannot[30]

---

[26] Erdősy, E., *op. cit.*, p. 71.

[27] Erdősy, E., *op. cit.*, p. 73.

[28] Erdősy, E., *op. cit.*, p. 122.

[29] According to Erdősy unsuccessful risk with respect to financial value manifests itself in the form of pecuniary disadvantage.

[30] According to Erdősy *„measurability means primarily the possibility of calculation, secondly the calculability of the reciprocal effects of the assumption of risk. It often emerges in economic life that the non-commission agent sells the product below the level of the purchase price (e.g. in the scope of the discount sales of clothes). In such a case it may also occur that the company stores the seasonal product (swimming costumes) and intends to sell it next year. This incurs storing expenses and it is uncertain what will be fashionable next year and whether the company can sell the old-fashioned clothes. The decision on either of the options (discount sales or storage) by the manager incurs risk".*

● decision-making situations are partly typifyable and thereby partially can be regulated by law

● unsuccessful risk manifests itself as pecuniary disadvantage[31]

V. The criminal legal evaluation of permitted economic risk

One type of legal responsibility is criminal liability. Criminal liability differs from other manifestations of legal responsibility in general terms[32] (under civil law or labour law) with respect to the conditions of responsibility.

The prerequisite of criminal liability is the commission of crime[33]. Consequently, economic risk becomes a criminal legal issue, if the specific economic activity is circumscribed by a legal facts of the case under the Special Part of the Penal Code, but this activity is marked by features of risk, owing to which criminal legal consequences are not applicable versus the conduct[34].

In accordance with Emil Erdősy risk needs to be construed in a differentiated manner, that is, the general effect of permitted risk, the preclusion of criminal liability need to be examined in relation to its certain concrete forms of manifestation.

According to its criminal legal taxonomi[35] „and" function of permitted risk is not characterised by an either-or relation, namely, permitted risk precludes either culpability or the unlawfulness of the act. The right construction is the both-and approach, that is, permitted risk is a precluding circumstance in some cases in re the disposition-like character of the act, in other cases in re the culpability of the perpetrator.

According to Erdősy the essence of the assumption of risk is not „*whether the conduct injures interests protected by criminal law, but whether the hazardous act with uncertain outcome fully complies with the specific professional rules or in the absence of specific professional rules (or in case of the breach of prevalent professional rules) whether the detrimental consequence of the decision on the assumption of risk is imputable to the person assuming the risk on grounds of wilful or negligent commission"*[36].

VI. Closing remarks

The proof of the commission of economic crimes is problematic since the prosecuting organs often do not dispose of proper economic knowledge. Therefore, recourse to an expert (professional counsellor) is required for passing meritorious decisions in all the phases of the criminal procedure. In a significant part of the cases even the decision whether lodging a criminal procedure is justified requires economic expertise[37].

---

[31] Erdősy, E., *op. cit.*, p. 128.

[32] See further, Wiener, A. Imre, *A gazdasági tevékenységgel kapcsolatos büntető szankciók* [Criminal sanctions related to economic activity], Jogtudományi Közlöny 1984/ pp. 301-303.

[33] Földvári, József: *A büntetés tana* [The Doctrine of Punishment], Közgazdasági és Jogi Könyvkiadó, Budapest, 1970. pp. 72-75.

[34] Erdősy, Emil, *A termelési kockázat és büntetőjogi felelősség* [The risk of production and criminal liability], Jogtudományi Közlöny 1971/7. p. 366.

[35] *See* Stănilă, Laura, *The legal person and the tax evasion offenses. From theory to practice*, Journal of Eastern European Criminal Law 2015.2. pp. 157-161.

[36] Erdősy, E., *op. cit.*, p. 159.

[37] Pusztai László: *A gazdálkodás menetében elkövetett bűncselekmények bizonyításáról* [On proving crimes committed in the course of business management], Magyar Jog 1977/2. p. 114.

During investigation the lack of economic knowledge is crucial, since the knowledge and interpretation of rules of law referred to in a framework disposition imply difficulty for the members of the authority[38].

According to Tamás Sárközy the inconceivably complicated mesh of the conglomerate of economic and production relations lies at the heart of the difficulties of holding criminally liable for economic activity. The recognition of the real direction of economic processes is an extraordinarily difficult task, since the implicit element of economic decisions is risk, in particular, the outcome of purposeful economic activity diverges from the intended.

Several objective circumstances interfere with economic processes. economic output emerges as the resultant of several human activities. Economic conducts are influenced by a mass of super-structural elements, they are affected by various impetuses[39].

The continual change, dynamics (and cycles) of economic circumstances perforce lead to criminal legal problems on the one hand in relation to the establishment of culpability, on the other hand in relation to the economic process and to the „selection" of the person requiring actual criminal penalisation.

Holding criminally liable may be detrimentally affected by the detachment of the economic law-making of the given country from the specific economic circumstances, by inflexibility and over-complicatedness, e.g., the continuous change of the rules of taxation.

Criminal law is on familiar grounds if life or physical integrity is injured, since in these cases the establishment of crime is not problematic. In economic criminality, however, the real objects are business management and the order of the direction of the economy.

Several times criminal law is inclined to retreat instead of the resolution of problems of economic criminal law, because it turns out that it is unable to penetrate into this area. Frequently a long time passes between the accomplishment of the act and the recognition of its being an economic crime. Generally during this time the punishability[40] of the act expires. The retreat of criminal law from certain areas of economic criminality is unjustified. Although both the responsible person and the person who could decide who is responsible are really difficult to find. Cutting the Gordian knot of the situation would be by all means supported by making the decision mechanism more regulated, transparent and clearer.

A typical contradiction of our days is on the one hand the promotion of risk and creativity, on the other hand the policy of enhancing personal responsibility. In this area of tension the golden mean should be found, which could by all means be supported by the serious consideration of general and professional ethical norms along with legal provisions.

References:

1. Bhusal, Dharma Raj, *Economic Crime Law and Legal Practice in the context of Nepal*. Inaugural dissertation for getting a doctoral degree (doctor juris) from the Faculty of Economics and Business Administration of Chemnitz University of Technology, Germany. 2009.

2. Erdősy, Emil, *A megengedett kockázat a büntetőjogban* [Permitted Risk in Criminal Law], Akadémiai Kiadó, Budapest, 1988.

---

[38] Pusztai, L., *op. cit.*, p. 117.

[39] Sárközy, T., *op. cit.*, p. 26.

[40] See: Stănilă, Laura: *To punish or to torture? About inhuman treatment in the recent view of the Strassbourg Court*, Journal of Eastern European Criminal Law 2017.2. pp. 256-259.

3. Erdősy, Emil, *A termelési kockázat és büntetőjogi felelősség* [The risk of production and criminal liability], Jogtudományi Közlöny 1971/7. pp. 365-371.

4. Fehér, Lenke, *Gazdasági bűnözés, gazdasági bűncselekmények* [Economic criminality, economic crime], Jogtudományi Közlöny 1981/1. pp. 73-78.

5. Földvári, József, *A büntetés tana* [The Doctrine of Punishment], Közgazdasági és Jogi Könyvkiadó, Budapest, 1970.

6. Fonyó, Antal, *A gazdálkodási kötelességeket sértő bűncselekmények* [Crimes Violating the Obligations of Business Management]. In: Bodgál-Bodrogi-Erdősy-Fonyó-Gál-Gáspár-Kovács-Pintér-Wéber, Magyar büntetőjog - Különös Rész [Hungarian Criminal Law. The Special Part], BM Könyvkiadó, Budapest, 1981.

7. Fonyó, Antal, *A gazdasági bűncselekmények fogalma* [The concept of economic crime], Kandidátusi értekezés tézisei [Thesis of candidate dissertations]. Szeged. 1960.

8. Gál, László István, *Economic Bribery as a Part of Economic Criminal Law and a Concomitant of Political Corruption*. Journal of Eastern-European Criminal Law 2014.1. pp. 22-32.

9. Gál, László István, *The criminal law protection of the stock market in Hungary*. Journal of Eastern-European Criminal Law 2015.2. pp. 43-49.

10. Irk, Ferenc: *A rizikó és a gondatlan bűncselekmények* [Risk and Negligent Crimes)], Jogtudományi Közlöny 1980/3. pp. 178-186.

11. Pusztai László, *A gazdálkodás menetében elkövetett bűncselekmények bizonyításáról* [On proving crimes committed in the course of business management], Magyar Jog 1977/2. pp. 113-120.

12. Pusztai, László, *A gazdasági bűnözés* [Economic criminality]. In: Gönczöl Katalin – Korinek László –Lévai Miklós: Kriminológiai ismeretek – bűnözés – bűnözéskontroll [Criminological knowledge – criminality – control of criminality], Corvina Kiadó. Budapest, 1999. pp. 186 – 197.

13. Sárközy, Tamás, *A „belső" gazdasági bűncselekmények alapvető anyagi jogi kérdései* [Basic substantive legal issues of „internal" economic crime], Jogtudományi Közlöny 1968/1. pp. 25 -34.

14. Stănilă, Laura, *The legal person and the tax evasion offenses. From theory to practice*, Journal of Eastern European Criminal Law 2015.2. pp. 153-164.

15. Stănilă, Laura, *To punish or to torture? About inhuman treatment in the recent view of the Strassbourg Court*, Journal of Eastern European Criminal Law 2017.2. pp. 256-268.

16. Szilovics, Csaba, *About the causes of corruption in the hungarian public procurement system*. Journal of Eastern-European Criminal Law 2014.2. pp. 101-109.

17. Tóth, Dávid: *A korrupciós bűncselekmények szabályozásának története* [The history of the regulation of corruption crimes in Hungary]. Büntetőjogi Szemle 2015.3. pp. 107-112.

18. Tóth, Mihály, *A gazdasági bűnözés és bűncselekmények néhány aktuális kérdése* [Some Topical Issues of Economic Criminality and Crime], MTA Law Working Papers, 2015/4. pp. 1-21.

19. Wiener A. Imre, *Kockázat és bűnösség* [Risk and culpability] Állam-és Jogtudomány 1972/1. pp. 91-106.

20. Wiener, A. Imre, *A gazdasági bűncselekmények fogalmáról* [About definition of economic crime]. Állam-és Jogtudomány 1979/1. pp. 42-63.

21. Wiener, A. Imre, *A gazdasági tevékenységgel kapcsolatos büntető szankciók* [Criminal sanctions related to economic activity], Jogtudományi Közlöny 1984/ pp. 301-305.

22. Wiener, A. Imre, *A gazdasági vezetőknek a beosztottak bűncselekményéhez kapcsolódó büntetőjogi felelőssége* [The criminal liability of managers for the crimes of their subordinates], Magyar Jog 2003/12. pp. 705-710.

Phenomenological forms of asset misappropriation fraud as the specific type of economic crime

Prof. dr Zoran S. Pavlović*
Full time Professor of Criminal law,
Chairman of the Department for Criminal Law
Faculty of Law, University of Business Academy Novi Sad,
Ombudsman of the Autonomous Province of Vojvodina,
Republic of Serbia

MA Nikola Paunović*
Research Asistant
Assistant at Ministry of Foreign Affairs
PhD Student, University of Belgrade, Faculty of law

Abstract

One of the typical phenomenological forms of economic crime in the modern world that represents a worrying threat is the asset misappropriation as the specific type of fraud. Asset misappropriation means the theft of company assets by the perpetrator for their own benefit and it can include a lot of fraud schemes committed by anyone who possesses the relevant information concerning the financial data of the target company. Bearing in mind that the consequences could affect very seriously the financial sector of the targeted company, the article deals with the phenomenological forms of this phenomenon. Precisely, since there are numerous forms, in this paper, it will be analyzed only the following phenomenological types of fraud: 1) Cash schemes; 2) Accounts receivable schemes and 3) Inventory and Fixed asset schemes. First of all, when it comes to the cash schemes, the focus will be on the forms of fraud depending on whether misappropriation of assets occurs before they are recorded in the books and records of an organization, or while assets are currently held by the organization or during the process of purchasing goods or services: a) Skimming; b) Cash larceny; and c) Fraudulent disbursements. Secondly, in the context of accounts receivable schemes, the attention will be dedicated to the following types of fraud: a) Lapping; b) Fictitious receivables. Moreover, regarding the inventory and fixed asset schemes the analysis will have consisted of the following types of fraud: 1) Simple larceny; 2) Asset requisition and transfers; 3) Purchasing and receiving schemes; and 4) False shipments of inventory. Finally, concerning the fixed asset schemes the article deals with: 1) Misappropriation of assets; 2) Recognition of fictitious assets; 3) Misrepresentation of asset value and 4) Capitalisation of non-asset expenses. In concluding remarks, it is noted that the advancement of the application of a proactive approach should be the main objective in combating the analyzed type of fraud in order to detect the asset misappropriation schemes in a timely manner.

Keywords: *phenomenology, asset misappropriation, fraud, economic crime.*

---

* Contact: zoran.pav@hotmail.com.
* Contact: dzoni925@gmail.com.

I. Introduction

Fraud represents widespread issue within organizations and remains a significant and high-cost problem for nearly every type of organization everywhere in the world. Bearing in mind enlarged competitive markets, rapid developments in technology and periods of economic crisis, the risks of fraud may only be increasing. Although there is no worldwide accepted definition of fraud, it could be mentioned that it essentially involves using deception to make a personal financial gain for oneself and/or create an economic loss or damage for another[1]. Since various forms of fraud are occurring at uncontrollable levels nowadays fraud has received comprehensive attention in the scientific discussions and in public actions as well. In a general sense, fraud can be committed internally or externally from a company by employees, customers, vendors and other parties. When it comes to the internal fraud, it should be noted that it usually occurs within an organization and is committed by employees, while the external fraud is perpetrated by outsiders meaning that the suspect is not an employee, manager, officer, or owner of the victim company, thereby covering a broad range of schemes, from vendor and customer frauds that attack businesses to traditional consumer frauds and confidence schemes[2]. Furthermore, fraud can be committed knowingly by a consumer (first-party fraud), or consumers can be victimized by fraudsters operating within financial institutions or as part of criminal enterprises (third-party fraud)[3]. All in all, fraud schemes are classified into three categories: *asset misappropriation* involving, but not limited to, cash larceny, skimming, and billing schemes, *corruption* in which perpetrators misuse their authority for private gain and *fraudulent financial statements* including false presentation or concealment of facts concerning the organization's financial statements[4].

Asset misappropriation means the theft of company assets, including monetary assets, cash supplies or equipment, by company directors, others in fiduciary positions or an employee for their own gain[5]. Therefore, it should be noted that asset misappropriation includes stealing an asset of a company for personal use at the corporation's expense or misuse of resources accompanied by false or deceptive records or documents to conceal the theft[6]. Asset misappropriation frauds are generally divided into two main categories: 1) *the theft of cash* and 2) *the theft of non-cash* assets. Misappropriation of assets, concerning the theft of cash, may occur under different circumstances involving the following: 1) before assets are recorded in the books and registers of an organization (e.g. *skimming*), 2) during assets are conducted by the

---

[1] Chartered Institute of Management Accountants, *Fraud risk management*, pp. 5-7, 2009, https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf, accessed on 11.5.2019.

[2] Association of Certified Fraud Examiners-ACFE, *Introduction to Fraud Examination*, Association of Certified Fraud Examiners", Austin 2017, p. 75.

[3] T., Gates, K., Jacob, „Payments Fraud: Perception Versus Reality", *Economic Perspectives*, No. 1/2009, p. 7.

[4] M., Bekiaris, G., Papachristou, „*Corporate and accounting fraud: types, causes and fraudster's business profile"*, Corporate Ownership & Control, Vol. 15, No.1/2017, p. 468.

[5] K., Bussmann, *Economic crime: people, culture & controls*. PricewaterhouseCoopers, London, 2008, p. 8.

[6] R., Kassem „Detecting asset misappropriation: a framework for external auditors" *International Journal of Accounting, Auditing and Performance Evaluation*, Vol. 10, No. 1/2014, p. 3.

organization (e.g. *cash larceny*), or 3) at the time of purchasing goods or services (e.g. *billing, expense reimbursement or payroll schemes*)[7]. Finally, non-cash misappropriation of assets involves the schemes where perpetrator steal or misuse the non-cash assets of an organization, such as inventory or equipment, for own material gain[8]. In the following lines, the focus will be only to different types of internal fraud unified under the term of asset misappropriation.

II. Phenomenological forms of the asset misappropriation fraud

Majority of business-level financial crimes are consisted of stealing funds or assets over which perpetrators have control[9]. In that sense, the most common form of economic fraud is the misappropriation of assets, in which an employee, executive or owner of a company by taking advantage of his or her position steals a company's cash or non-cash assets from an organization for own personal use and gain. Therefore, it is worth mentioning that asset misappropriation falls under occupational fraud also known as the workplace, internal or employee fraud[10]. The above stated definition is pretty extensive since the majority of occupational types of theft could potentially be incorporated under the term of asset misappropriation fraud[11]. For that reason, in this paper it will be only analyzed the following phenomenological forms of asset misappropriation fraud: 1) Cash schemes, including: a) Skimming; b) Cash larceny; c) Fraudulent disbursements; 2) Accounts receivable schemes, involving: a) Lapping; b) Fictitious receivables; as well as 3) Inventory and Fixed asset schemes[12].

III. Cash schemes

1. Skimming

Skimming is known as an „*off-book*" fraud since the money is stolen before it is recorded in the books. Precisely, skimming occurs at any point where and any time when assets enter to company business, thereby anyone who deals with the process of receiving funds may be in a position to skim money (e.g. salespersons who receive assets directly from customers). In that regard, it should be pointed out that many skimming fraud schemes are committed by employees whose duties include receiving

---

[7] C., Albrecht, M., Kranacher S., Albrecht, *Asset Misappropriation Research White Paper for the Institute for Fraud Prevention*, 2010, pp. 1-2,
https://www.researchgate.net/publication/242597392_Asset_Misappropriation_Research_White_Paper_for_the_Institute_for_Fraud_Prevention, accessed on 11.5.2019.

[8] *Ibid*, pp. 3-4.

[9] P., Burgess, *The 3 most common corporate fraud schemes*, 2016,
https://www.microbilt.com/news/article/here-are-the-3-most-common-corporate-fraud-schemes, accessed on 6.5.2019.

[10] D., Gordon, *Understanding the 3 types of occupational fraud*, 2019,
https://www.cpacanada.ca/en/news/atwork/2019-01-10-types-of-occupational-fraud, accessed on 11.5.2019; See also E., Perdue, C. McDonald, Responding to Workplace Embezzlement and Asset Misappropriation, *Michigan Defense Quarterly*, 2010, p. 14.

[11] J., P. Kennedy, „Asset misappropriation in small businesses", *Journal of Financial Crime*, Vol. 25 No. 2/2018, p. 374.

[12] Association of Certified Fraud Examiners-ACFE, *Introduction to Fraud Examination*, Association of Certified Fraud Examiners, Austin, 2011, p. 62.

and recording customers' and donors' payments[13]. In that context, it should be emphasized that there are two main types of skimming: 1) sales skimming; and 2) receivables skimming. *Sales skimming* are especially prevalent in the cases when the perpetrator has access to incoming funds from an unexpected source, such as e.g. refunds that have not been accounted for by the victim organization, while, *receivables skimming* involve the situations when incoming receivables payments are foreseen[14]. More detailed, the skimming schemes involve the following types of fraud: 1) unrecorded sales; 2) understated sales; 3) revenue skimming and 4) skimming accounts receivable[15]. The skimming in the form of *unrecorded sales* represent those type of sales that never is documented in the company books at all and could be explained by the case of an employee in which he was selling goods and services to a customer, as well as collecting the customer's payment, but did not make any record of the sale in order to steal the money. On the other hand, in the context of *understated sale*s as the specific type of skimming, the transaction in question is registered in the accounting system, but for a lower amount than what the perpetrator exactly collected. For instance, understated sales could be understood by the example of a cashier who sold 10 combination hunting and fishing licenses at $100 each, but recorded 8 at $100 each and pocketed the $200[16]. Furthermore, the form of *revenue skimming* involves cases in which the perpetrator (e.g. an employee) accepts payment from a customer, but does not record the transaction and then pockets the money. In the case of revenue skimming, a county employee embezzled at least $84,193 over two years by skimming cash receipts collected at county parks, abusing its authority to receive, record, and deposit cash receipts[17]. By contrast, in the context of *skimming accounts receivable* form, an employee accepts payments on accounts and records that the customer made a payment on the account, but falsely records a charge to an expense account with the aim of pocketing the money[18].

2. Cash larceny

Although cash larceny and skimming are very similar forms of cash fraud schemes, there is a difference between them depending on the time when the cash is stolen. In that respect, cash larceny is the theft of money that has already recorded in the company's books, while skimming is the theft of cash that has not yet been registered in the accounting system. Therefore, the key element that differentiates skimming from cash skimming is that cash larceny is referred to the amount of stolen money that is recorded in the books while regarding the skimming it does not the matter. The most common form of committing cash larceny is through the cash register since the enormous number of transactions provides an excuse for perpetrators to manipulate with the records and steal some cash, finding his or her access as a mean to rob the

---

[13] J. Finlay, *How Cash May Be Stolen*, 2009 B, pp. 1-2, http://sectorsource.ca/sites/default/files/james_finlay_nov_2009.pdf, accessed on 11.5.2019.

[14] R., Kassem, *op. cit.,* pp. 4-5.

[15] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* pp. 62-63.

[16] Office of the Idaho State Controller, *Revenue Skimming*, 2017, p. 1, https://www.sco.idaho.gov/web/DSADoc.nsf/F3CA0DB6B2CD938187258136005243F4/$FILE/FFFF-June_2017.pdf, accessed on 11.5.2019.

[17] *Ibid.,* p. 2.

[18] Office of Auditor General, State of Arizona, *Fraud Alert— Skimming*, 2012, https://www.azauditor.gov/sites/default/files/Fraud_Alert_12-01.pdf, accessed on 11.5.2019.

company cash and remove transaction or understate it into the records[19]. An example of cash larceny is the case regarding a bookkeeping employee, responsible for posting donors receivable in a small nonprofit agency, which was stealing some of the cash receipts but nonetheless posting the transaction to the company's donors-receivable books, thus enabling that the amount of stolen money reaches more than $200,000. Eventually, a bank reconciliation revealed a major discrepancy between the donors-receivable details and received cash and the scheme was uncovered[20].

3. Fraudulent Disbursements

Fraudulent disbursements, as the type of „on-book frauds", are the most common form of asset misappropriation, and they occur when an employee uses his position of employment to make a payment for some inappropriate purpose. Fraudulent disbursement schemes are divided into the following types: 1) check tampering schemes; 2) register disbursement schemes; 3) billing schemes; 4) expense reimbursement schemes and 5) payroll schemes[21].

Check tampering is a type of fraudulent disbursement scheme whereby an employee either 1) prepares a fraudulent check for own benefit or 2) intercepts a check intended for a third-party and converts it to own gain. By contrast from the other fraudulent disbursement schemes, such as false billings or payroll fraud which tend to rely on false claims for payment, the perpetrator of a check tampering scheme takes physical control of a check and places false information on that instrument, forging a signature and/or an endorsement as well as altering a payee or the amount of the check. The key point is that the perpetrator places false information on a company check enabling the fraudster to illegally obtain funds from employer[22]. Furthermore, there are register disbursement schemes which represent a type of occupational fraud that is a hybrid between cash theft and fraudulent disbursements. However, since these schemes appear on the books as legitimate disbursements of funds from the cash register, they are classified as fraudulent disbursements, and therefore are very similar to cash larceny schemes. On the other side, billing schemes attack the purchasing function of an organization, causing the victim organization to buy goods or services that are non-existent, high-price or not needed by the organization. This type of scheme is accomplished in one of the following two ways, either by running a voucher for a personal purchase through the payables system, misrepresenting the nature of the purpose, claiming that the goods or services are being bought on the company‘s behalf, or by purchasing personal goods or services on the company‘s credit card or on a credit account[23].

An example of using company funds for personal use represents the case in which the perpetrator as the store manager was using some of the money orders sold in her store to pay her personal bills, including the rent on her house. The money orders were pre-numbered and are stored in the vault of the store. The missing money orders caused the cash register to be short which caused the corporate office to be suspicious, thereby

---

[19] Fraud Fighting, *Cash Larceny and its types*, Fraud Fighting, 2017, p. 1, https://fraudfighting.org/wp-content/uploads/2017/12/Cash-Larceny-and-its-Types.pdf, accessed on 6.5.2019.

[20] J. Finlay, *Fraud Schames*, 2009A, p. 3, http://sectorsource.ca/sites/default/files/james_finlay_oct_2009.pdf, accessed on 7.5.2019.

[21] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 63.

[22] *Ibid.,* pp. 63-64.

[23] *Ibid.,* pp. 64-65.

the corporate office started investigating perpetrator's paperwork and found the money orders she used to make rent and other credit card payments were cashed by a regional manager[24]. Therefore, it should be noted that a billing scheme has three major parts: a) the creation of a false entity to receive the payments by opening a bank account in the name of the false entity, or through cashing the cheques in some other manner causing that an account cannot be traced if the fraud is discovered; b) the creation of the false invoice submitted for payment; or c) the manipulation of the payments system so that the false invoice is approved and the payment is made. How this is done will depend on the position the employee has in the business and what influence he or she can have over the payment process. To conclude, all billing schemes have one common purpose regardless of their form to get the victim to voluntarily make a payment to and record the payment as a legitimate business expense[25].

Moreover, *expense reimbursement* schemes fall into four general categories: 1) mischaracterized expense reimbursements; 2) overstated expense reimbursements; 3) fictitious expense reimbursements; 4) multiple reimbursements. This type of scheme is most commonly perpetrated by sales personnel who overstate or create fictitious expenses in areas such as client entertainment and business travel. However, sales personnel are not the only employees who commit this type of fraud since any person who is in a position to incur travel or business entertainment expenses is potentially capable of committing expense reimbursement fraud[26].

Finally, there are *Payroll schemes* which occur when an employee fraudulently generates overcompensation on his or her behalf. These schemes are similar to billing schemes in a way that the perpetrator generally produces some false document or otherwise makes a false claim for distribution of funds by his employer. In other words, while in billing schemes, the false claim typically comes in the form of a fraudulent invoice, in payroll schemes, the false claim generally occurs when the fraudster falsifies payroll records, timekeeping records or some other document concerned with the payroll function. In that regard, the most common forms of payroll fraud are: 1) ghost employee schemes; 2) falsified hours and salary; 3) commission schemes[27]. Precisely, the payroll fraud includes the following examples: a) creating a ghost employee; b) claiming hours worked that were unrelated to business; c) claiming sick leave when not really sick; d) attending to personal business instead of attending professional training[28]. In that sense, for payroll forms, the following four things must take place. Firstly, the perpetrator must fabricate all the necessary personnel and payroll records for the ghost employee (false name, address, pay rate, etc.) and enter them into the payroll system. Another method used to create a ghost is to leave a terminated employee on the payroll, creating that the terminated employee becomes the ghost. Secondly, if the ghost employee is paid by the hour, the perpetrator must submit falsified timekeeping documentation to the payroll system. Thirdly, the falsified

---

[24] C., Lehmann, *„Asset Misappropriation Schemes: Short Cases for Use in the Classroom"*, Journal of Forensic & Investigative Accounting, Vol. 7, No.2/2015, pp. 343.

[25] Association of Certified Fraud Examiners-ACFE, *Billing Schemes – Cash Frauds*, ACFE Brisbane Chapter, 2019, https://brisbaneacfe.org/library/occupational-fraud/billing-schemes-cash-frauds/, accessed on 12.5.2019.

[26] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 65.

[27] *Ibidem.*

[28] Odgen-Weber Tech College, *Fraud prevention*, 2015, p. 2, https://www.otech.edu/site/wp-content/uploads/fraud-newsletter-02.pdf, accessed on 12.5.2019.

timekeeping information must be authorized. Lastly, the pay cheque must be cut and issued, and the perpetrator must gain access to it[29].

Since the payroll schemes are difficult to detect it is worth meaning that the potential indicators of these schemes could include the following: 1) employees with duplicate addresses and/or bank account information; 2) invalid social security or social insurance numbers; 3) employees without employee's files; 4) fluctuations in payroll expense as compared to prior periods, including inconsistencies between the level of payroll comparing with department productivity; 5) timesheets with notations in different handwriting or color; 6) extra pay stubs left over after distribution to employee; 7) changes to payroll from one pay period to the next that are unsupported or unauthorized; 8) expense reports with photocopied or altered receipts, calculation errors, and supporting documentation lacking details of expenses incurred[30]. Moreover, fraud indicators in payroll schemes might be recognized by the inconsistent overtime hours for a cost center, overtime charged during a slack period, overtime charged for employees who normally would not have overtime wages as well as budget variations for payroll by cost center[31].

An example of payroll scheme fraud is the case of a financial controller, who over the years had been progressing well in terms of promotions, and thereby decided with her spouse to purchase their dream home. However, she was stunned to find out that her long-deserved promotion was being deferred indefinitely as the result of a new responsible person for finance. For that reason, she started processing the weekly payroll, adding a new fictitious, or „ghost," employee to the payroll which is a person who is on the books but does not actually work for an organization as well as using an alias name and her own legitimate bank account to set up the new employee, believing that uncovering one ghost employee among 500 was going to be like finding a needle in haystack. Within weeks, the Payroll Administrator for details and strong checks and balances uncovered the Controller's payroll fraud scheme[32].

IV. Accounts receivable schemes

1. Lapping

In the context of skimming, it seems that concealing the fraud is the most important part of the crime, even more, important than obtaining the funds. In that sense, it is worth mentioning the method of lapping[33]. Lapping is not fraud itself. It is the method of using a new fraud to hide an old fraud, in the sense that one fraud laps over another. Before the next statement is issued, an amount needs to be credited against the original debtor to hide the theft of their receipt. For example, the money needed for debtor A's

---

[29] P., Munachewa, *Payroll Fraud*, 2015, https://www.icpak.com/wp-content/uploads/2015/09/Payroll-Fraud-Munachewa.pdf, accessed on 6.5.2019.

[30] E., Nagel, *Payroll Fraud: A Global Problem:Finding a Potential Needle in the Pay Stack*, Paytech, 2015, p. 4, http://nagel-forensics.com/wp-content/uploads/2015/07/Payroll-Fraud-A-Global-Problem-Finding-a-Potential-Needle-in-the-Pay-Stack.pdf, accessed on 12.5.2019.

[31] T. Di Napoli, *Red Flags for Fraud*, New York: State Of New York Office Of

The State Comptroller, 2010, p. 7, https://www.osc.state.ny.us/localgov/pubs/red_flags_fraud.pdf, accessed on 7.5.2019.

[32] E., Nagel*, op. cit.,* pp. 2-3.

[33] J. Finlay, 2009B, p. 2.

account is taken from a receipt from debtor B - usually a debtor who pays just before the issuance of these statements. Furthermore, the money from debtor B is recorded as being collected from debtor A, hiding the fraud with debtor A, but creating a new fraud with debtor B. At the end money from debtor C is used to solve the discrepancy with debtor B, and so on[34]. This type of scheme was described by the Missouri Court of Appeals in *State v. Brown* case. According to this Court, in the context of the implementation of lapping scheme, it is necessary that the perpetrator has access to substantial amounts of cash and also is able to arrange the credit of payments made by checks to cover the misappropriated cash. In other words, lapping is an operation recognized in accounting circles as a sophisticated type of embezzlement in the form of accepting checks and failing to account for the receipt thereof in the books. However, to make the books balance, the cash should be removed in an amount equal to the face value of the checks received. Since no record has been made of the checks having been received, there is no apparent loss when the checks are used to replace the same amount of cash in the bank deposit[35].

2. Fictitious receivables

Fictitious receivables accounts are usually set up to disguise fictitious sales. Once a sale is booked, the corresponding journal entry is to a receivable that is never collected and eventually written-off[36]. Although, accounts receivable frauds start with the basics of skimming and lapping more advanced accounts receivable frauds include *account identity theft*. With account identity theft, the perpetrator sets up a bank account in a name similar to that of the victim and then steals checks intended for the victim and deposits them in the criminal's bank account in order to withdraw the funds or wire out of the account. Furthermore, there are *reaging receivables* which represents a fraud perpetrated by management when the receivables are being used for collateral for a loan. It is also done when fake sales have been entered into the accounting system in order to conceal the fact that a payment has not been made. The reaging of receivables involves creating a new receivable and using the funds to pay off an aged receivable. Finally, there are receivables *dumping* which occurs when an employee, who normally has a connection with a collection company, writes off a collectable receivable and sends it out for collection. The collection company usually gets a third of the collection and the employee either has an undisclosed interest in the collection company or is receiving a kickback from the collection company[37]. Management engaging in fraud will have two choices if intends that such frauds are not to be revealed: to intervene in the confirmation process so that phony responses can be sent to the auditors or to create journal entries that effectively move the fictitious receivables into other balance sheet accounts that will not be subject to the same level of audit scrutiny. Regarding the arrangements designed to interfere with the auditors' attempts to confirm receivables, it should be noted that this avenue commonly requires that allies of the perpetrator serve as would-be customers, who will respond favorably to the auditors' inquiries regarding

---

[34] *Ibid.,* p. 3.

[35] D., Studler, D., Malcomb, *Stealing – Back To The Basics*, Fidelity Law Association New Jersey, 2008, p. 11,
https://sdccpa.com/wp-content/uploads/2013/09/STEALING_BACK_TO_BASICS.pdf,
Retrived from 12.5.2019.

[36] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 66.

[37] R., Minniti, *Fraud Review*, CCH Publications, Riverwoods, 2019, p. 14-15.

amounts ostensibly owed to the company. The other way, by which wholly fraudulent sales can be disguised and hidden from auditors, requires the corresponding amounts recorded as receivables be eliminated from the books before accounts are selected for confirmation. For example, receivables balances may be eliminated by means of recording fictitious returns or, more often, allowances, which are then explained as being non-cash credits to calm victimized customers[38].

V. Inventory fraud and fixed asset schemes

Inventory fraud schemes could be broken down into the following types: 1) misappropriating inventory for personal use, 2) stealing inventory and 3) theft of scrap proceeds. Phenomenological forms of inventory fraud, *misappropriating inventory for personal use* means that the inventory is being stolen for personal use under the excuse that it is being borrowed. By contrast, the inventory fraud type, *stealing inventory* involves situations when inventory is stolen for sale to outsiders, e. g. to unknowing purchasers or to co-conspirators[39]. Precisely, *inventory theft* is typically manifested by one of the following four methods: 1) simple larceny; 2) asset requisition and transfers; 3) purchasing and receiving scheme and 4) false shipments of inventory. *Simple larceny* scheme is comprised of acts in which an employee steals the company assets without any attempt to conceal it in the books. The examples of this scheme may include the following: a) theft of parts, materials, or tools used at workplaces; b) entering company premises during closed hours and stealing inventory; c) setting aside goods intended for delivery to customers or setting aside excess merchandise received. During the scheme of *asset requisition and transfers,* perpetrator moves the asset from one location to another in order to steal the inventory e.g. by requesting more material than is needed in order to steal the excess or convert it to personal gain. Furthermore, *purchasing and receiving* fraud schemes means falsifying incoming shipment records to cover up a theft and it could be perpetrated in the way that e. g. an employee who receives shipment stole some of the items, but marks the copy of the receiving document as a full shipment or marks the receiving shipment rejected since the quantity is below quality control standards. However, in fact, the rejected items do not return to the supplier, but instead sells. Finally, *false shipments of inventory* schemes include the situations which cause inventory to be shipped to a fictitious person as well as its accomplice or in some cases to a customer in order to cover up the false shipment[40]. To conclude, inventory theft can occur in many and varied forms. A common scheme involves collusion between delivery and receiving personnel, by signing for more items than were actually received in order to sell the difference to other parties and to split the money between the individuals. Another form of theft is the ordering of excess inventory items and then converting the excess to personal use. For example, in a case an employee of a motion picture company misappropriated $470,000 over a two-year period, by operating procedures which allowed him to arrange for outside script copying services, to receive script copies, and

---

[38] B., Epstein, *Fraudulent Revenue Schemes and How to Detect Them*, 2015, http://www.epsteinnach.com/commentary/fraudulent-revenue-schemes-detect/ accessed on 12.5.2019.

[39] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 67.

[40] Lowers Risk Group, *Inventory, Shipping, & Receiving Fraud- Hidden Dangers in Every Transaction*, 2019, pp. 2-3, https://www.lowersrisk.com/files/resources/Inventory-Shipping-Receiving-Fraud.pdf, accessed on 12.5.2019.

to approve payments. In that sense, the employee set up a fictitious corporation, submitted invoices for services never rendered, and charged the production of films shot at the studio that were never produced[41].

Theft of Scrap Proceeds is a common practice in the case of the amounts which are generally insignificant to the financial statements of the company, since the scrap sales are usually not well controlled and inventory documentation is not well kept, enabling individuals to underreport the amounts received through the sales[42]. In that sense is a case of sale director, in which the investigation discovered that a significant proportion of sales invoiced to particular suppliers had been falsely created, allowing the misappropriation of inventory from the warehouse. The fraudulent sales invoices were later credited by the sales director as 'non-inventory return credits'. The inventory itself had been collected by an associate of the sales director and the sale proceeds shared between them[43]. To conclude, fraud indicators in inventory schemes may include increasing number of complaints about products or service, increase in purchasing inventory but no increase in sales, abnormal inventory shrinkage, lack of physical security over assets/inventory, charges without shipping documents, payments to vendors who are not on an approved vendor list, high volume of purchases from new vendors, purchases that bypass the normal procedures, vendors without physical addresses, vendor addresses matching employee addresses, excess inventory and inventory that is slow to turnover and purchasing agents that pick up vendor payments rather than have it mailed[44].

Fixed assets are the company's property, plant, and equipment. Often, fixed assets are the targets of employee theft and unlicensed personal use. Fixed assets that are easily removed from the premises (such as tools and computers) are especially exposed to employee theft[45]. Assets can be stolen directly or they can be inappropriately scrapped and sold for salvage, with the perpetrator keeping the proceeds. Furthermore, assets which have been fully depreciated but still have economic value to the company may be eliminated from the records and then stolen[46]. Another common type of fixed asset scheme is the unauthorized personal use of fixed assets by employees. For example, the personal use of computers or company-owned vehicles can develop into fraud or an abuse situation if the subject is not licensed[47]. There are four most common types of fixed asset fraud schemes: 1) misappropriation of assets; 2) recognition of fictitious assets; 3) misrepresentation of asset value and 4) capitalization of non-asset expenses. First of all, the *misappropriation of assets* happens when employees abuse their position to steal from the company. On the other side, *recognition of fictitious assets* involves the action of producing fake documents (such as invoices or purchase orders) to support the fraudulent accounting entries. Furthermore, *the misrepresentation of*

---

[41] C. Greene, *Focus on Employee Fraud*, 2019, https://www.mcgoverngreene.com/archives/archive_articles/Craig_Greene_Archives/Focus-Employee_Frauds-Invent.html, accessed on 5.5.2019.

[42] *Ibidem.*

[43] Price waterhouse Coopers Fraud, *A guide to its prevention,detection and investigation*, 2008, p. 9, https://www.pwc.com.au/consulting/assets/risk-controls/fraud-control-jul08.pdf, accessed on 6.5.2019.

[44] T. Di Napoli, *op. cit.,* p. 7.

[45] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 67.

[46] B., Epstein, *Business And Accounting Fraud. Institute of Singapore Chartered Accountants*, Singapore, 2014, p. 29, https://isca.org.sg/media/775682/businessandaccountingfraud.pdf, Retrived fro accessed on 12.5.2019.

[47] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 67.

asset value has several types of execution. First of all, fixed asset misrepresentations include the case of misclassification of assets to meet budgetary or covenants requirements. Moreover, in the case of understatement of values, the asset is depreciated at a higher rate compared to the estimated useful life of the asset. Finally, in the case of overstatement of values, the asset is recorded in the financial statements with a value higher than the value allowed by the applicable accounting framework. Lastly, *capitalization of non-asset expenses* scheme consists in capitalizing costs which do not meet the requirements for capitalization under the applicable accounting standards in order to show a stronger company's performance[48].

VI. Conclusion

Taking into consideration the fact that investigators are constantly faced with a lot of challenges concerning the detection of asset misappropriation schemes due to the continuous development of technology that creates new possibility for perpetrators to commit new phenomenological forms of this type of fraud or to improve the existing ones, it can be concluded that it is impossible to imagine all the potential forms of asset misappropriation schemes. In addition, it can be noted that this crime is characterized by a dark figure mostly due to lack of expertise and knowledge of relevant actors to identify potential situations that may indicate that there has been occurred the asset misappropriation. Accordingly, bearing in mind the complex and covert manifestations of asset misappropriation, it seems that the application of reactive investigation, after the criminal complaint is filed, cannot provide adequate results in terms of suppression of this type of crime. Therefore, the basic goal should be the improvement of the proactive approach in the police teamwork and public prosecutors' offices in order to achieve the sustainable reduction of asset misappropriation fraud schemes. In order to fulfill the above stated goal and make the highest results in combating economic crime, all relevant actors involved in investigations should be part of the relevant training program. In addition, it is necessary to strengthen the cooperation of state bodies that possess data relevant for carrying out investigations concerning asset misappropriation with the police and the prosecutor's office. Therefore, it should be added that starting from the covert manifestation of asset misappropriation schemes, only through comprehensive cooperation both at the international and national level in the field of information exchange, this crime could be detected in a timely manner and the valid evidence could be collected as well as used in criminal proceedings.

In that sense, it is necessary to conduct transnational investigations based on operational and strategic assistance that would be focused on the exchange of criminal intelligence data and coordination of joint investigation teams. Additionally, since perpetrators constantly adjust their activities to the latest technologies, it is extremely important to constantly collect data on new trends for commitment the asset misappropriation schemes. Furthermore, it is necessary for policy investigation teams to participate constantly in thematic training programs in order to develop the capacities and skills as well as to enable them to be prepared for all methods and techniques used by the perpetrators. Moreover, in terms of prevention, taking into account the complex and covert manifestations of asset misappropriation in order to combat efficiently against this criminal activity, it is necessary to apply a multinational

[48] Fraud fence, *Fixed assets: popular frauds and how to prevent them*, Fraud fence, 2016, http://fraudfence.co.uk/fixed-asset-frauds/, accessed on 6.5.2019.

coordinated approach, because it is unrealistic to expect that only one or several countries, without others, will achieve any results at the level of prevention. In that sense, it is necessary that all relevant actors work together on strengthening cooperation between the internal affairs bodies of national states and international organizations and European agencies. This is why it should be kept in mind that asset misappropriation schemes cannot be eradicated as such, but it should be aware that, by working together much more could be achieved in controlling this phenomenon.

References

1. Albrecht, C., Kranacher M., Albrecht, S. (2010). *Asset Misappropriation Research White Paper for the Institute for Fraud Prevention*, accessed on 11.5.2019. https://www.researchgate.net/publication/242597392_Asset_Misappropriation_Research_White_Paper_for_the_Institute_for_Fraud_Prevention.

2. Association of Certified Fraud Examiners-ACFE (2011). *Introduction to Fraud Examination*. Association of Certified Fraud Examiners, Austin.

3. Association of Certified Fraud Examiners-ACFE (2017). *Introduction to Fraud Examination*. Association of Certified Fraud Examiners, Austin.

4. Association of Certified Fraud Examiners-ACFE (2019). Billing Schemes – Cash Frauds, ACFE Brisbane Chapter, https://brisbaneacfe.org/library/occupational-fraud/billing-schemes-cash-frauds/, accessed on 12.5.2019.

5. Bekiaris, M., Papachristou, G. (2017). „Corporate and accounting fraud: types, causes and fraudster's business profile", *Corporate Ownership & Control*, Vol. 15, No.1.

6. Burgess, P. (2016). The 3 most common corporate fraud schemes, https://www.microbilt.com/news/article/here-are-the-3-most-common-corporate-fraud-schemes, accessed on 6.5.2019.

7. Bussmann, K. (2008). *Economic crime: people, culture & controls*. Pricewaterhouse Coopers, London.

8. Chartered Institute of Management Accountants, (2009). Fraud risk management, https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf, accessed on 11.5.2019.

9. Di Napoli, T. (2010). *Red Flags for Fraud,* New York: State Of New York Office Of

10. Epstein, B., (2014). Business And Accounting Fraud. Institute of Singapore Chartered Accountants. Singapore. https://isca.org.sg/media/775682/businessandaccountingfraud.pdf, accessed on 12.5.2019.

11. Epstein, B., (2015). Fraudulent Revenue Schemes and How to Detect Them, http://www.epsteinnach.com/commentary/fraudulent-revenue-schemes-detect/, accessed on 12.5.2019.

12. Finlay, J. (2009A) Fraud Schames, http://sectorsource.ca/sites/default/files/james_finlay_oct_2009.pdf, accessed on 7.5.2019.

13. Finlay, J. (2009B) How Cash May Be Stolen, http://sectorsource.ca/sites/default/files/james_finlay_nov_2009.pdf, accessed on 11.5.2019.

14. Fraud fence (2016). Fixed assets: popular frauds and how to prevent them, Fraud fence http://fraudfence.co.uk/fixed-asset-frauds/, accessed on 6.5.2019.

15. Fraud Fighting (2017). *Cash Larceny and its types*, Fraud Fighting https://fraudfighting.org/wp-content/uploads/2017/12/Cash-Larceny-and-its-Types.pdf, accessed on 6.5.2019.

16. Gates, T., Jacob, K. (2009). „Payments Fraud: Perception Versus Reality", *Economic Perspectives*, No.1.

17. Gordon, D. (2019). Understanding the 3 types of occupational fraud, https://www.cpacanada.ca/en/news/atwork/2019-01-10-types-of-occupational-fraud, accessed on 11.5.2019.

18. Greene, C. (2019). *Focus on Employee Fraud,* https://www.mcgoverngreene.com/archives/archive_articles/Craig_Greene_Archives/Focus-Employee_Frauds-Invent.html, accessed on 5.5.2019.

19. Kassem, R. (2014). Detecting asset misappropriation: a framework for external auditors. Int. *International Journal of Accounting, Auditing and Performance Evaluation* Vol. 10, No. 1.

20. Kennedy, P. J. (2018) „Asset misappropriation in small businesses", *Journal of Financial Crime*, Vol. 25 Issue: 2, https://doi.org/10.1108/JFC-01-2017-0004, accessed on 5.5.2019.

21. Lehmann, C. (2015), „Asset Misappropriation Schemes: Short Cases for Use in the Classroom", *Journal of Forensic & Investigative Accounting*, Vol. 7, No.2.

22. Lowers Risk Group (2019). Inventory, Shipping, & Receiving Fraud- Hidden Dangers in Every Transaction, https://www.lowersrisk.com/files/resources/Inventory-Shipping-Receiving-Fraud.pdf, accessed on 12.5.2019.

23. Minniti, R. (2019). *Fraud Review.* CCH Publications, Riverwoods.

24. Munachewa, P. (2015). Payroll Fraud, https://www.icpak.com/wp-content/uploads/2015/09/Payroll-Fraud-Munachewa.pdf, accessed on 6.5.2019.

25. Nagel, E. (2015). „Payroll Fraud: A Global Problem: Finding a Potential Needle in the Pay Stack", Paytech, http://nagel-forensics.com/wp-content/uploads/2015/07/Payroll-Fraud-A-Global-Problem-Finding-a-Potential-Needle-in-the-Pay-Stack.pdf, accessed on 12.5.2019.

26. Odgen-Weber Tech College, (2015). Fraud prevention, https://www.otech.edu/site/wp-content/uploads/fraud-newsletter-02.pdf, accessed on 12.5.2019.

27. Office of Auditor General, State of Arizona, (2012). Fraud Alert— Skimming, https://www.azauditor.gov/sites/default/files/Fraud_Alert_12-01.pdf, accessed on 11.5.2019.

28. Office of the Idaho State Controller (2017). Revenue Skimming https:// www.sco.idaho.gov/web/DSADoc.nsf/F3CA0DB6B2CD938187258136005243F4/$FILE/FFFF-June_2017.pdf, accessed on 11.5.2019.

29. Perdue, E., McDonald, C. (2010). Responding to Workplace Embezzlement and Asset Misappropriation, Michigan Defense Quarterly, https://www.dickinsonwright.com/~/media/Files/News/2011/01/Responding%20to%20Workplace%20Embezzlement%20and%20Asset%20M__/Files/MDTCWin11_McDonald_mil_pdf/FileAttachment/MDTCWin11_McDonald_mil_pdf.pdf, accessed on 12.5.2019.

30. Price waterhouse Coopers (2008). Fraud, A guide to its prevention, detection and investigation, https://www.pwc.com.au/consulting/assets/risk-controls/fraud-control-jul08.pdf, accessed on 6.5.2019.

31. Studler, D., Malcomb, D. (2008). *Stealing – Back To The Basics*, Fidelity Law Association New Jersey, https://sdccpa.com/wp-content/uploads/2013/09/STEALING_BACK_TO_BASICS.pdf, accessed on 12.5.2019.

32. The State Comptroller https://www.osc.state.ny.us/localgov/pubs/red_flags_fraud.pdf, accessed on 7.5.2019.

How acts of terrorism are financed and orchestrated in secrecy today: criminal offenses, donations, legal businesses and smartphone applications

Prof. Dr. Gál István László
Professor, Head of department
University of Pécs, Faculty of Law
Department of Criminal Law

Dr. Serbakov Márton Tibor
Ph.D student
University of Pécs, Faculty of Law
Department of Criminal Law

Abstract

The aim of this study is to present how acts of terrorism are financed and orchestrated in secrecy today, by committing criminal offenses, through donations, and by legal businesses and by the use of smartphone applications. Terrorists abuse the anonymity of the internet, and constantly look for secure channels of communication, to further their goals and to stay one step ahead of law enforcement. Through encrypted channels, terrorists spread their propaganda, recruit new members, and try to reach potential financers etc.

In this paper, we introduce the categories of smartphone apps used by terrorists. We also examine the weak point of these apps, and methods for infiltration.

Keywords: *terrorist financing, intelligence, smartphone applications, terrorist groups, IRA, security, propaganda, ISIS*

I. Introduction

Terrorist groups exploit the widespread access and the anonymity of the internet, especially the rapid growth of social media, to raise funds from sympathetic individuals on a global scale. The phenomenon represents a growing terrorist financing threat. Terrorist organizations spread their propaganda by social network and reach out to sympathisers. Terrorists also use social networks for fundraising campaigns. Terrorists organizations are able to reach a wide audience trough peer-to-peer horizontal communication (such as Facebook, Twitter, Instagram etc.) and sometimes that continues through mobile messenger applications (such as WhatsApp or Viber) and even more secure communication networks (such as Surespot). Terrorists' use of organized crowdfunding is also a growing terrorist financing risk[1]. Terrorist financing on social media can take several forms, donors may sometimes not even realize, that they are financing terrorist activity, because terrorists also conduct fundraising under fake charities, where donors believe they donate for humanitarian purpose. Platforms of

[1] FATF REPORT Emerging Terrorist Financing Risks October 2015, pp. 30-31.
http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (5/12/2018.)

social media are mouthpieces for broadcasting explicit calls for financial support. Terrorist supporters direct potential funders to communication platforms. Terrorists encourage donors to use encrypted mobile applications, to hide from external surveillance. This means serious a difficulty for efforts against terrorist financing. For example, the Telegram application is being used used as a channel of communication regarding the exchange or transfer of funds and for recruitment purposes[2].

II. Sources and techniques of terrorist financing

1. Committing criminal offenses

Terrorism is a form of criminality, namely one of its most severe and dangerous form. Because of this, naturally terrorist organizations are not afraid to commit other criminal offenses. The risks of these other criminal offenses are usually lower than those of acts of terrorism, the sentences applicable are generally lower. Terrorists usually prefer such types of criminal offenses that generate a large income in a short amount of time. Out of these criminal offenses terrorists probably prefer drug-trafficking the most. Drug-trafficking generates 60-90% of the icome of Columbian paramilitary groups and guerilla fighters of Colombia[3]. Furthermore, some fatwas expressly authorise Islamic terrorist organizations to use drug-trafficking as a tool in their fight agains the decadent West[4].

In addition, kidnapping is also a significant source of income for terrorists. For example, The Islamic Movement of Uzbekistan (IMU)[5] earned 5 million USD by releasing 4 Japanese geologists, after kidnapping them in 1999 in Kyrgyzstan[6].

Illegal immigrant smuggling is also a profitable tool for terrorists. The difference of the quality of life between developed and underdeveloped regions of the world, and the desire for the security provided by the democratic states brought ecomonic and political migration into being. To get to Western Europe, a Bangladeshi or Chinese citizen should be prepared to sacrifice up to 20-25 thousand dollars[7].

On the one hand, money laundering is a lucrative activity for terrorists, thus, it is a tool of terrorist financing. On the other hand, considerable proportion of the literature also considers terrorist financing and money laundering related phenomena. Terrorist financing is probably also going to integrate into the wider-sense definition of money laundering, as „reverse money laundering" or „money dirtying", in a short time. Terrorist financing has the following different characteristics compared to money laundering[8]:

---

[2] Yuen Stacey, *It's not just Russia — terror financiers are also using social media propaganda*, available on https://www.cnbc.com/2017/12/18/social-media-propaganda-terror-financiers-operate-on-internet.html (accessed on 5/12/2018).

[3] L.V.Berry, G.E. Curtis, R.A. Hudson, N.A. Kollars, *A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups,* Library of Congress 2002, p. 52.

[4] R. Beers, F.X. Taylors, *Narco-Terror*, *The Worldwide Connection Between Drugs and Terror*, in Terrorsim and Goverment Information 2002, p. 322.

[5] The IMU is allied to the Islamic State, and considers itself part of it. Merhat Sharipzhan: IMU Declares It Is Now Part Of The Islamic State https://www.rferl.org/a/imu-islamic-state/27174567.html (accessed on 5/12/2018.)

[6] L. Napoleoni, *Modern Jihad. Tracing the Dollars Behind the Terror Networks*, Pluto Press, London, 2003, pp. 89.

[7] László Korinek, *A terrorizmus* in Katalin Gönczöl, Klára Kerezsi, László Korinek, *Kriminológia-Szakkriminológia Szerk*, Lévay Miklós CompLex kiadó, Budapest, 2006, p. 456.

[8] Steven Mark Levy, *Federal Money Laundering Regulation (Banking, Corporate, and Securities Compliance)* New York, 2003, Chapter 2, pp. 18-20.

– The motive is rather violent (intimidation) than financial (for financial gain). The aim of terrorists is mainly to coerce a government agency, another State or an international body into doing, not doing or countenancing something, to intimidate the general public, or to conspire to change or disrupte the constitutional, economic or social order of another State, or to disrupt the operation of an international organization. These aims that are specified by international documents can also be found in the Hungarian Act C of 2012 on the Criminal Code, under section 314, which is about acts of terrorism. So financial gain is the aim of terrorists only in the rarest cases, while money laundering is clearly „profit-oriented".

– Money from legal sources is also used for terrorist financing, as well as money from illegal sources. Significant portion of the money that terrorists get as financial support is from legal sorces, such as charitable organizations, philantropic donors, and legally operating companies. – The third distinguishing characteristic is the different in the amount of the sum involved. Larger acts of terrorism can also be organized and conducted by using relatively smaller sums of money. For example, the perpetrators of the aircraft hijackings of 2001 regularly withdrew humble amounts of financial support, disguised as foreign studensts, and none of the transfers reached the „magical" 10,000 dollars limit, without an exception.

There are other types of lucrative criminal offenses, which are used by terrorists to get money. The taxative listing of these is impossible. In 2002 the IRA allegedly gained 11 million USD by committing various criminal offenses. The largest portion of their income came from tobacco smuggling from Eastern Europe to England[9]. Large portion of the Al-Qaeda's European income came from credit card fraud; secret services estimated that this sum reached 1 million USD per month[10].

2. Donations

The donation is giving terrorists or terrorist organizations cash, commercial bank money, securities, precious metals, precious stones, or other marketable assets of value, free of charge, without remuneration. Its typical form is monetary support. Terrorists favor cash, which has the highest liquidity among all assets.

Terrorists can be supported by private individuals, organizations (even other terrorist organizations) and states. In the criminal law sense, „donation" in a broader sense can be considered terrorist financing, while in economic sense, the perpetration of the criminal offense and the legal business activity can also be considered as part of this activity.

In the narrow sense, the regulation of criminal law regarding terrorist financing focuses on the donations of private individuals, if states support terrorist aims, that often presents an insoluble problem for criminal law[11]. The state's donation's form (direct or indirect financial support), its cover (commercial deal, humanitarian aid etc.), and the military and economic power of the state (smaller or bigger country, or a

---

[9] L. Clarke, D. Leppard, *Photos link more IRA Men to Colombia,* Sunday Times, 28 April 2002.

[10] R. Gunaratna, *Inside Al Quaeda: Global Network of Terror,* Hurst&Company London, 2002, p. 65.

[11] Our far fetched and deliberately provocative example is the following. The radical armed Taliban are considered terrorists, today, and an international hunt was conducted against them in Afghanistan. The financial support of their activity is considered terrorist financing. The same Taliban attacked the Soviet troops with the same exact methods, they later used against the international forces. Does anybody think about it today to suggest the responsibility of the CIA, or in a broader sense, of the USA as state, beacause of committing terrorist financing 20+ plus years ago?! Of course not. According to today's Western standpoint, the Taliban attacking the Soviet forces were freedom fighters…

country with nuclear weapons, or maybe a superpower) makes a difference.

3. Legal businesses

Between 1991 and 1996, Osama bin Laden established 30 companies in Sudan, with 3000 employees altogether. Already in 1994-1995 Western and Israeli secret service sources talked about bin Laden as the key figure of terrorist financing.

Legal businesses have an iscreasingly larger role in terrorist financing, as it can also be stated in a general sense, that legal sources have an increasingly important role in terrorist financing. As we have already mentioned, mainly European jihadoist cells rely increasingly on legal sources of income, for example, on the salary, that they earn at their legal workplace. The attack of 9/11 was the last terrorist attack, which was wholly financed by Al-Qaeda, in 2002 gobal financing came to an end! Most of today's bomb attacks are acts of of self-financing cells. Thus, a process that is named *„privatization of terrorist financing"* by the literature started[12].

If terrorists as employees use part of their legal income for terrorist purposes, it can be regarded as part of legal business in a broader sense. If we go by past years' experiences of larger acts of terrorism, a sum of 8-10,000 USD is already enough to finance a serious attack, then our fear that a terrorist cell of 4-5 members is able to save this kind of money in 2-3 years in practically in any developed or moderately developed country[13], and able to strike, whithout the need of any additional sources may be realistic!

III. Terrorists' use of the internet and their search for secure platforms

As Róbert Bartkó states: *„The particular prevention methods evolve alongside terrorist acts, so the statment that can be regarded as a „chliché" today, that criminals are always one step ahead of law enforcement authorities, still seems to be confirmed"*[14].

Criminals and terrorist financers are constantly adjusting their techniques, to always stay one step ahead of law enforcement; they gladly use unique or experimental products and services to further their goals[15].

The biggest challenge for intelligence regarding counterterrorism is in the inherent difficulty of unearthing plots that involve a few people who do their planning and preparation covertly and take operational security very seriously[16]. Terrorism generates perceptible extra expenses in the sphere of law enforcement, justice and secret service. Out of these spheres, secret services' extra expenses are the most significant. The most effective tools against terrorism are in the hands of secret services. For example, the most severe economic criminal offenses and the fight agains terrorism are specifically among the scope of duties of the Polish secret services, which were reorganized in 2002, so the

---

[12] Sean S. Costigan, David Gold, *Terronomics*, ASHGATE, Printed in Great Britain, 2007, p. 14.

[13] If we count by a cell of 5 members, 2 years are enough to save 10,000 USD, if one member saves 1000 USD per year. This is barely more than 80 USD per month.

[14] Robert Bartkó, *A terrorizmus elleni küzdelem kriminálpolitikai kérdései*, Győr, UNIVERSITAS-GYŐR Nonprofit Kft., 2011, p. 68.

[15]Sean McCrossan, *Combating the Proliferation of Mobile and Internet Payment Systems as Money Laundering Vehicles*, CAMS-FCI, p. 15.

https://www.acams.org/wp-content/uploads/2015/08/Combating-the-Proliferation-of-Mobile-and-Internet-Payment-Systems-as-ML-Vehicles-S-McCrossan.pdf (5/12/2018.)

[16] Pillar Paul R., *Terrorism and Current Challenges for Intelligence*, GSSR Special Issue: What the New Administration Needs to Know About Terrorism and Counterterrorism, February 2017, p. 108.

http://georgetownsecuritystudiesreview.org/wp-content/uploads/2017/02/GSSR-What-the-New-Administration-Needs-to-Know-About-Terrorism-and-Counterterrorism.pdf (5/12/2018.)

conclusion can be clearly drawn that terrorist financing is also among their scope of authorities[17]. We can only have estimations about the increased expenses; they are among the most serious state secrets in every country[18]. The fight agains terrorism has presumably increased the budget of secret services by billions of dollars on a global scale.

„The Internet has revolutionized terrorism forever." Terrorists exploit possibilities provided by the cyberspace to further their goals in ways never before possible[19]. According to *Gabriel Weimann, terrorists the use the internet for psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, sharing information, planning and coordination*[20]*. Beacause of goverments' increased surveillance over telephone systems and social media, and because social media platforms' measures against them, terrorists are forced to find safer and more hidden alternatives to communicate to conduct transactions.* (Such as the Telegram app, this is known for its high level encryption[21]). They turned to the *dark web*[22], to supplement their activities conducted on other platforms. Terrorists use social media rather for propaganda and recruitment purposes, and the dark web for communication and transactions, because the latter has higly secure platforms. The encryptions of the dark web make it very difficult for law enforcement agencies to track down the IP addressess of the users. Beacause of its very high security and anonimity, the dark web is a home of many illegal activities[23].

IV. Smartphone applications used by terrorists for security, messaging, and propaganda

In Laith Alkhouri's and Alex Kassirer's report titled Dissecting Jihadists' Digital Toolbox Alkhouri and Kassier lists and examines the digital tools used by jihadists. These tools are the following: secure browsers, virtual private networks (VPNs) and proxy

---

[17] Emil Pływaczewski, Wojciech Filipkowski, *The Development of Organised Crime Policies in Poland: From Socialist Regime to Rechtsstaat* in *Organised Crime in Europe* Edited by Cyrille Fijnaut and Letizia Paoli, Springer, 2004, p. 918.

[18] Because if the exact portion of the budget of secret services of a given country that is spent on the fight against terrorism, and the way this sum increases, year by year (how it changes) was made public, terrorists could also draw significant conclusions from this data.

[19] Ariel Victoria Lieberman, *Terrorism, the Internet, and Propaganda: A Deadly Combination*, Journal of National Security Law and Policy, 2017, Volume 9, 122. http://jnslp.com/wp-content/uploads/2017/04/Terrorism_the_Internet_and_Propaganda_FINAL.pdf (accessed on 5/12/2018).

[20] Gabriel Weimann, www.terror.net *How Modern Terrorism Uses The Internet*, United States Institute Of Peace, Special Reoprt, 2004. 5-10.

https://www.usip.org/sites/default/files/sr116.pdf (5/12/2018.)

[21] Rebecca Tan, *Terrorists' love for Telegram, explained. It's become ISIS's „app of choice."*

https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter (accessed on 5/12/2018).

[22] *„The „dark web" is a part of the world wide web that requires special software to access. Once inside, web sites and other services can be accessed through a browser in much the same way as the normal web.*

However, some sites are effectively „hidden", in that they have not been indexed by a search engine and can only be accessed if you know the address of the site." https://www.iflscience.com/technology/what-dark-web/all/ (accessed on 5/12/2018)

[23] Erdal Ozkaya, (2017), *The Use of Social Media for Terrorism*, in NATO Defence Against Terrorisim Review. 9. 47, pp. 8-9.

https://www.researchgate.net/publication/322486831_The_Use_of_Social_Media_for_Terrorism (accessed on 5/12/2018.)

services, protected e-mail services, mobile security applications, encrypted messengers, and mobile propaganda applications[24]. In this article we follow Alkhouri's és Kassirer's categorization of applications[25], and examine mobile security applications, encrypted messengers, and mobile propaganda applications. Certain platforms, such as Facebook and Twitter have taken steps against terrorist's social media activity. Twitter in particular has taken serious measures against ISIS-supporter accounts. Tech-expert terrorists demonstrate their adaptive abilities by circumventing barriers set up against them by using the tools of digital technology. Todays terrorists are constantly looking for alternative possibilities to further their agenda and to communicate securely with each other[26].

Tech savvy terrorists realize, that the use of smartphone applications involves risks for their users, without proper precautions, third persons are able to access their sensivite information, such as their GPS location, IP address etc. To lessen the security risks, tech-expert supporters of terrorism recommend the use of several smartphone applications. The main use of these applications is to secure the location and the data of their users, to clean their devices and to delete their browser history. The folowing security applications are preferred by and recommended for jihadists: Locker, FAKE GPS, D-Vasive Pro, AMC Security, ESET Mobile Security, Battery Saver, Call/SMS Blocker, Privasy Locker, APP Manager, iSHREDDER PRO, Override DNS, DNSCrypt, Net Guard, AFWall, F-Secure Freedome, Hide.me, Tutanota. For example, FAKE GPShides the user's location, and provides fake GPS data[27].

To avoid surveillance, terrorists use messaging applications that implement *end-to-end encryption*, such as the Telegram or the Signal application[28].

Terrorits have been using encryted messaging applications for years. Terrorists prefer messaging applications, which use end-to-end encryption.

Terrorists use the following apps, during their daily operations: the Swiss Threema, which implements end-to-end encryption, and was praised by a pro-ISIS technology guide, for its high security, in April 2016. Telegram, which was created by Pavel Durov, the founder of the Russian VKontakte, seems to be the most preferred application of lone wolf terrorists and terrorist groups.

However advanced an application may be, sceptical jihadists do not fully trust any of them, because most of them are Western developments. In February 2013 a jihadist media logistics unit called the Global Islamic Media Front (GIMF) released the Asrar al-Darshah (Secrets of Chatting), which is an encryption plugin, compatible with several instant messaging platforms. This plugin enables users the encryption of live messaging on messaging platforms, such as Paltalk, Google Chat, Yahoo, MSN és Pidgin[29]. The Islamic State also developed its own encrypted chat app, called Alrawi[30].

---

[24] Laith Alkhouri, Alex Kassirer, *Tech for Jihad: Dissecting Jihadists' Digital Toolbox*, Flashpoint, July 2016, p. 1. https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf (accessed on 5/12/2018.)

[25] Ibid.

[26] Ibid., p. 1.

[27] Ibid., p. 6.

[28] Paganini, Pierluigi: The Role of Technology in Modern Terrorism
https://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/#gref (5/12/2018.)

[29] Alkhouri, Laith & Kassirer, Alex: Tech for Jihad: Dissecting Jihadists' Digital Toolbox, Flashpoint, July 2016, pp 7-8.
https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf (5/12/2018.)

[30] Constine, Josh: ISIS Has Its Own Encrypted Chat App

The Islamlic State used Telegram to recruit the perpetrators of the Christmas market attack in Berlin, 2016. The terrorist attack of Saint Petersburg in 2017, in which 15 people died, was planned by using the application. Telegram was ideal: it has very high level encryption, it has private chat rooms, self-destructing messages, it's easy to join, and to create new accounts[31].

Husnain Rashid, a British ISIS supporter urged his followers on the Telegram, to target the 4-year-old Prince George. Furthermore Rashid encouraged his followers to commit acts of terrorism, during the World Cup in Russia; he urged them to inject cyanide into fruit and vegetables in stores and to poison ice cream. Rashid's activities specialized in assisting lone wolf terrorists. He sent 360,000 (!) messages on 150 different chat threads on Telegram, between November 2016 and his arrest on 22 November 2017. Police could only access a handful of these messages. Sajid Javid, the Secretary of State for the Home Department accused Telegram of being a „mouthpiece for terror"[32].

In December 2015, FBI's Director James Comey called upon tech companies providing users with end-to-end encryption to review „their business model" and stop implementing it[33].

Russia and Iran tried to ban Telegram[34]. The ban had no success in Russia, so far[35], and it also failed in Iran[36].

ISIS and other jihadist groups developed their own propaganda applications. The A'maq Agency app provides news and warzone videos for ISIS supporters. The Al-Bayan Radio is the Islamic State's official radio station, and it is also available as an android application.

The app called Voice of Jihad was released by the Afghan Taliban in April 2016 was originally available on Google Play store, but after about 48 hours Google removed the application, which resurfaced in the Amazon app store, several days later. This application provided news, announcements, reports, articles, and videos.

ISIS's jihadist themed Alphabet application teaches the arabic alphabet to children37. The terrorist organization released the Alphabet (Huroof) app for children

---

https://techcrunch.com/2016/01/16/isis-app/?guccounter=2 (5/12/2018.)

[31] Tan, Rebecca: Terrorists' love for Telegram, explained. It's become ISIS's „app of choice."

https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter (5/12/2018.)

[32] Victoria Ward, Steven Swinford, Dominic Nicholls, *Telegram app is 'mouthpiece' for terror, Sajid Javid says as jihadi admits encouraging attack on Prince George*

https://www.telegraph.co.uk/news/2018/05/31/islamic-state-supporter-admits-encouraging-jihadis-attack-prince/ (accessed on 5/12/2018).

[33] Pierluigi Paganini, *Islamic State launches the Kybernetiq magazine for cyber jihadists* http://securityaffairs.co/wordpress/43435/hacking/kybernetiq-magazine-cyber-jihad.html (accessed on 5/12/2018.)

[34] Palko Karasz, *What Is Telegram and Why Are Iran and Russia Trying to Ban It?*

https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html (accessed on 5/12/2018).

[35] Maria Kolomychenko, *Russia tries more precise technology to block Telegram messenger*

https://www.reuters.com/article/us-russia-telegram/russia-tries-more-precise-technology-to-block-telegram-messenger-idUSKCN1LF1ZZ (accessed on 5/12/2018).

[36]Rohollah Faghihi, *Iran's conservatives return to Telegram after failed ban*

https://www.al-monitor.com/pulse/originals/2018/11/iran-telegram-ban-conservative-media-rejoin-tasnim-fars.html (accessed on 5/12/2018).

[37] Laith Alkhouri, Alex Kassirer,*Tech for Jihad: Dissecting Jihadists' Digital Toolbox*, Flashpoint, 2016. július, 7-9, available on

https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf (accessed on

on 10 May 2016, in which children can match arabic letters to jihadi themed images (such as rocket, rifle, tank etc.)[38]. The bizarre application was released by ISIS' Office of Zeal. According to the press release of the Office of Zeal, the app „teaches the cubs the alphabet letters"[39].

In 2013 ISIS released its Dawn of Glad Tidings app, which enabled terrorists of the Ismalic State to orchestrate their social media campaign on Twitter on a very high level. The app enabled the participant twitter accounts to post tens of thousands tweets[40]. According to Michael Weiss and Hassan Hassan the Islamic State also used Zello, a „free walkie-talkie app"[41] which is popular among the younger targets of ISIS. The application lets users listen to preachers discreetly[42].

V. Terrorists' risks of using smartphone applications and a way of infiltration for law enforcement

ISIS' use of smartphone applications is not without risks for the terrorist organization. On the 1st of June 2016 Amaq and later other social media sources reported of a fake version of the Amaq Agency and other fake ISIS related apps circulating online. The sources warned supporters to only download apps from official sources, and to verify with the officially released checksum, before installation.

All of the apps of ISIS are developed for Android Operating System. The main difference between iPhone and Android devices is that Android lets users develop and install new apps outside its designated app store. Android applications can be developed and installed independently as APK (Andoid application package) files, without ever entering Google Play Store. This technique is called „sideloading", the Islamic State's main method to circumvent Google's and Apple's rules. This technique makes it easier for law enforcement agencies and vigilantes to plant malwares into fake apps, and to infiltrate the community of terrorists. A common defense against this is veryfing the app by uniquely generated checksum files. The former warnings prove that not every ISIS supporter bothers with veryfing their apps. ISIS' official Nashir and Amaq channels are often removed, so ISIS supporters have to turn to secondary and less reliable media outlets and make more and more mistakes regarding veryfication[43].

Al-Khabir al-Taqni, a jihadist supporter and self-proclaimed security expert ranked 33 smartphone messaging apps on Twitter, by their level of security, as unsafe, moderately

---

5/12/2018).

[38] Rita Katz, *ISIS's Mobile App Developers Are in Crisis Mode,* available on https://motherboard.vice.com/en_us/article/qkj34q/isis-mobile-app-developers-are-in-crisis-mode (accessed on 5/12/2018).

[39]The Islamic State calls the children „cubs" its adult terrorists „lions". *See Don Reisinger, ISIS Has Launched A Mobile App For Children,* available on http://fortune.com/2016/05/11/isis-mobile-app-children/(accessed on 5/12/2018).

[40] Mohammad-Mahmoud Ould Mohamedou, *A Theory of ISIS: Political Violence and the Transformation of the Global Order*, Pluto Press, 2018, p. 205.

[41] Cortney Moore, *What Is Zello and How Do You Use It?,* available on https://www.tomsguide.com/us/zello-app-guide,news-25805.html (accessed on 5/12/2018).

[42] Weiss Michael, Hassan Hassan, *Az Iszlám Állam. A terror hadserege belülről*, Budapest, HVG Könyvek, 2015, pp. 205-206.

[43] Rita Katz, ISIS's Mobile App Developers Are in Crisis Mode, available on https://motherboard.vice.com/en_us/article/qkj34q/isis-mobile-app-developers-are-in-crisis-mode (accessed on 5/12/2018).

safe, safe, and safest. For example, WhatsApp got the lowest ranking, among 15 other applications, like Viber. Al-Khabir warned jihadist against using these applications because they are closed source apps, and or use very weak or no encryption[44].

VI. Conclusion

On the internet terrorists can be monitored, kept under observation, their activities can be studied; there are theories, that by this, terrorists's online presence works against them. Websites and message boards act as an early warning system, regarding acts of terrorism[45]*.* The anonomity of the internet is not just advantageous for terrorists, because the anonimity also gives covert agents opportunities for infiltration. In the USA, several FBI agents already managed to infiltrate terrorist organizations successfully, thus thwarting terrorist attacks[46].

An efficient fight against terrorism requires the knowledge and understanding of every aspect of terrorism, including terrorists' online activities and their use of smartphone applications.

Our stance is that smartphone apps are platforms, where terrorists activity can and must be studied, where covert agents can infiltrate terrorist organizations, and could also prevent terrorist financing, acts of terrorism, recruitment etc. Terrorist related smartphone apps should be traced and infiltrated, and fake terorist apps should be developed with surveillance malwares planted in them.

References

1. Alkhouri, L., Kassirer, A., *Tech for Jihad: Dissecting Jihadists' Digital Toolbox*, Flashpoint, July 2016, https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf (accessed on 5/12/2018).

2. Bartkó, R., *A terrorizmus elleni küzdelem kriminálpolitikai kérdései*, Győr, UNIVERSITAS-GYŐR Nonprofit Kft., 2011.

3. Beers, R., Taylors, F.X., *Narco-Terror: The Worldwide Connection Between Drugs and Terror*, in *Terrorsim and Goverment Information* 2002.

4. Berry, L.V., Curtis G.E., Hudson, R.A., Kollars, N.A., *A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups,* Library of Congress 2002.

5. Clarke, L., Leppard, D., *Photos link more IRA Men to Colombia*, Sunday Times, 28 April 2002.

6. Constine, J., *ISIS Has Its Own Encrypted Chat App* https://techcrunch.com/2016/01/16/isis-app/?guccounter=2 (accessed on 5/12/2018).

7. *Conway, M.,* TERRORIST 'USE' OF THE INTERNET AND FIGHTING BACK. Department of Political Science College Green Trinity College Dublin 2 Ireland, https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura_co

[44] Rita Katz, *Almost Any Messaging App Will Do—If You're ISIS,* available on https://motherboard.vice.com/en_us/article/kb7n4a/isis-messaging-apps (accessed on 5/12/2018).

[45] *Maura Conway, Terrorist „use" of the Internet and fighting back,* Department of Political Science College Green Trinity College Dublin 2 Ireland, p. 22., available on https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura_conway.pdf (accessed on 5/12/2018).

[46] József Kis-Benedek, *Dzsihadizmus, radikalizmus, terrorizmus*, Zrínyi Kiadó, 2016, pp. 195-196.

nway.pdf (accessed on 5/12/2018).

8. Costigan, S.S., Gold, D., *Terronomics,* ASHGATE, Printed in Great Britain, 2007.

9. Faghihi, R., *Iran's conservatives return to Telegram after failed ban* https://www.al-monitor.com/pulse/originals/2018/11/iran-telegram-ban-conservative-media-rejoin-tasnim-fars.html (accessed on 5/12/2018).

10. FATF REPORT Emerging Terrorist Financing Risks October 2015, http:// www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (accessed on 5/12/2018).

11. Gunaratna, R., *Inside Al Quaeda: Global Network of Terror*, Hurst&Company London, 2002.

12. Karasz, P., What Is Telegram, and Why Are Iran and Russia Trying to Ban It? https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html (accessed on 5/12/2018).

13. Katz, R., *Almost Any Messaging App Will Do. If You're ISIS* https://motherboard.vice.com/en_us/article/kb7n4a/isis-messaging-apps (accessed on 5/12/2018).

14. Katz, R., *ISIS's Mobile App Developers Are in Crisis Mode* https://motherboard.vice.com/en_us/article/qkj34q/isis-mobile-app-developers-are-in-crisis-mode (accessed on 5/12/2018).

15. Kis-Benedek, J., *Dzsihadizmus, radikalizmus, terrorizmus*, Zrínyi Kiadó, 2016.

16. Kolomychenko, M., *Russia tries more precise technology to block Telegram messenger*, https://www.reuters.com/article/us-russia-telegram/russia-tries-more-precise-technology-to-block-telegram-messenger-idUSKCN1LF1ZZ (accessed on 5/12/2018).

17. Korinek, L., *A terrorizmus* in Gönczöl K.– Kerezsi K., Korinek L., Lévay M. Kriminológia-Szakkriminológia Szerk, CompLex kiadó, Budapest, 2006.

18. Levy, S.M., *Federal Money Laundering Regulation (Banking, Corporate, and Securities Compliance)*, New York, 2003. 2. chapter.

19. Lieberman, A.V., *Terrorism, the Internet, and Propaganda: A Deadly Combination,* Journal of National Security Law and Policy, 2017, Volume 9, p. 122. http://jnslp.com/wp-content/uploads/2017/04/Terrorism_the_Internet_and_Propaganda_FINAL.pdf (accessed on 5/12/2018).

20. McCrossan, S., *Combating the Proliferation of Mobile and Internet Payment Systems as Money Laundering Vehicles*, CAMS-FCI, https://www.acams.org/wp-content/uploads/2015/08/Combating-the-Proliferation-of-Mobile-and-Internet-Payment-Systems-as-ML-Vehicles-S-McCrossan.pdf (accessed on 5/12/2018).

21. Mohamedou, M.-M.O., *A Theory of ISIS: Political Violence and the Transformation of the Global Order*, Pluto Press, 2018.

22. Moore, C., *What Is Zello and How Do You Use It?* https://www.tomsguide.com/us/zello-app-guide,news-25805.html (accessed on 5/12/2018).

23. Napoleoni L., *Modern Jihad: Tracing the Dollars Behind the Terror Networks*, Pluto Press, London, 2003.

24. Ozkaya, E., *The Use of Social Media for Terrorism*. NATO Defence Against Terrorism Review 2017, no. 9 issue 47. https://www.researchgate.net/publication/322486831_The_Use_of_Social_Media_for_Terrorism (accessed on 5/12/2018).

25. Paganini, P., *Islamic State launches the Kybernetiq magazine for cyber jihadists* http://securityaffairs.co/wordpress/43435/hacking/kybernetiq-magazine-cyber-jihad.html (accessed on 5/12/2018).

26. Paganini, P., *The Role of Technology in Modern Terrorism* https://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/#gref (accessed on

5/12/2018).

27. Pillar, P.R., *Terrorism and Current Challenges for Intelligence*, GSSR Special Issue: What the New Administration Needs to Know About Terrorism and Counterterrorism, February 2017. http://georgetownsecuritystudiesreview.org/wp-content/uploads/2017/02/GSSR-What-the-New-Administration-Needs-to-Know-About-Terrorism-and-Counterterrorism.pdf (accessed on 5/12/2018).

28. Pływaczewski, E., Filipkowski, W., *The Development of Organised Crime Policies in Poland: From Socialist Regime to Rechtsstaat* in *Organised Crime in Europe* Edited by Cy. Fijnaut, L. Paoli, Springer, 2004.

29. *Reisinger, D., ISIS Has Launched A Mobile App - For Children* http://fortune.com/2016/05/11/isis-mobile-app-children/ (accessed on 5/12/2018).

30. Sharipzhan, M., *IMU Declares It Is Now Part Of The Islamic State* https://www.rferl.org/a/imu-islamic-state/27174567.html (accessed on 5/12/2018).

31. Tan, R., *Terrorists' love for Telegram, explained. It's become ISIS's „app of choice."* https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter (accessed on 5/12/2018).

32. Ward, V., Swinford, S., Nicholls, D., *Telegram app is 'mouthpiece' for terror, Sajid Javid says as jihadi admits encouraging attack on Prince George* https://www.telegraph.co.uk/news/2018/05/31/islamic-state-supporter-admits-encouraging-jihadis-attack-prince/ (accessed on 5/12/2018).

33. Weimann, G., *www.terror.net How Modern Terrorism Uses The Internet, United States Institute Of Peace*, Special Report, 2004. https://www.usip.org/sites/default/files/sr116.pdf (accessed on 5/12/2018).

34. Weiss, M.H., *Az Iszlám Állam. A terror hadserege belülről*, ford.: Nagy Marcell, Takács Zoltán, Budapest, HVG Könyvek, 2015.

35. What Is The Dark Web? https://www.iflscience.com/technology/what-dark-web/all/ (accessed on 5/12/2018).

36. Yuen, S., *It's not just Russia - terror financiers are also using social media propaganda* https://www.cnbc.com/2017/12/18/social-media-propaganda-terror-financiers-operate-on- internet.html (accessed on 5/12/2018).

Cybersecurity obligations of ICT Companies in P. R. China

PhD Shenkuo Wu *

Abstract

With the fast development of new generation of ICT technologies, the entire Chinese community is in front of numerous opportunities and, at the same time, is also forced to face various risks. Under this emerging perspective, among others, the issue of cybersecurity obligations of ICT companies in China is becoming much more relevant and the undergoing debates on this can deeply help to understand better the real logic and approach of the actual Chinese cyber governance. In fact, as an important characteristic, the current numerous Chinese dispositions related to cybersecurity governance are basically provided at three levels, the systematic study of which helps to provide a complete insight on the effective cybersecurity obligations of ICT companies in China. Meanwhile, in practice, the before-mentioned multi-level cybersecurity obligations cannot be interpreted beyond the numerous institutional limitations already rooted in the current Chinese legal system, as the rational balance between the industry developments and the security interests, as well as the strict proportionality between the rights and the obligations, are always the top priority of the Chinese regulation approach in this area.

Keywords: *Cybersecurity obligations, ICT companies, China*

I. Introduction

In nowadays P. R. China, with the fast development of new generation of ICT technologies, the entire Chinese community is in front of numerous opportunities and, at the same time, is also forced to face various risks[1].

On one hand, thanks to the new technologies, the Chinese community can get benefits at three levels: (1) obtaining new technical supports, especially from big data, AI, etc.; (2) introducing new operation models, including cloud computing, IoT etc.; and (3) developing new business applications, such as eHealth, eLife, eFinance, etc.

On the other hand, the Chinese community is constantly suffering from more and more serious risks, which reflect at three levels as well: (1) new technical offences, such as virus, DDos attack, etc. (2) new organizational offences, especially ICT fraud, etc.; *and* (3) new content offences, including child pornography, terrorist propaganda, etc.

Indeed, from the year of 2014, China has started to accelerate its own policy and legal framework improvements, with the double purpose of promoting the digital economy development as well as enhancing the cybersecurity capacity building.

Under this emerging perspective, among others, the issue of cybersecurity obligations of ICT companies in China is becoming much more relevant and the undergoing debates on this can deeply help to understand better the real logic and approach of the actual Chinese cyber governance.

---

* *Associate Professor of Law School of Beijing Normal University, P. R. China.* *This research is supported by National Social Science Foundation of China (15CFX035).*

[1] On the scenario of ICT related opportunities and risks, see Zhang Boqin-Sun Shuyang, 2019 *Development Trend Prospects of Network Security in China*, in Cyberspace Security, 2019, no. 1, p. 37.

II. Policy and Legal Framework on Cybersecurity Obligations of ICT

Companies

In fact, as an important characteristic, the current numerous Chinese dispositions related to cybersecurity governance are basically provided at three levels: (1) the Policies; (2) the Legislations; and (3) other Norms.

Generally speaking, from the point of view of their functions, the Policies establish the *core values* pursued in the area of cybersecurity, the Legislations introduce the systematic rules as the essential *legal institutions*, and other Norms offer the more detailed *operational indications* for the further implementations:

1. Main Policies related to cybersecurity governance

Facing the cyber governance issues, the Chinese policy maker tries constantly to achieve the better balance between the development (digitalization) and the security (cybersecurity) as two basic values:

(1) The *„Internet Plus" Action Plan*[2], issued by the State Council on 4 July, 2015, strengthens the integration between the Internet related innovations and the traditional social-economic elements, as well as the necessity to enhance the cybersecurity through the improvement of the standard norms, the legal norms, the security awareness and the security managements.

(2) The *National Strategy for the Big Data*[3], issued by the State Council on 31 August, 2015, highlights the multi-benefits that the big data innovations can bring to the people, as well as the importance to guarantee the cybersecurity through the integration among the updated policies, legislations, standardizations, market development mechanisms, financial supports, talents educations and international cooperations.

(3) The *13th National Five-Year Plan for Informatization*, issued by the State Council on 15 December, 2016, considers the cybersecurity as the basis for the development and strengthens the high relevance of joint efforts of the governments, industries, civil societies and individuals for the safeguard of cybersecurity.

(4) The *Development Planning for the New Generation of Artificial Intelligence*[4], issued by the State Council on 20 July, 2017, highlights not only the great opportunities but also the serious security risks connected to the application of AI, and promotes the AI regulation through the ad hoc technical, legal and moral norms as well as the cooperations among the public and private stakeholders for the continuous risk assessment.

(5) The *National Cyberspace Security Strategy*[5], issued by the Cyberspace Administration of China on 27 December, 2016, establishes the targets, principles and tasks for the cybersecurity building, and declares the high necessity of rule of law for the open and transparent Internet governance, as well as the importance of the public

---

[2] On the practical perspective of „Internet Plus" Action Plan, see Li Congyuan, *Future of „Internet Plus" Action Plan*, in Information Research, 2018, no. 2, p. 95.

[3] On the logic of the National Strategy for the Big Data, see also Liao Jingwei-Yu Juan, *Research on the Big Data Industry*, in Modern Business Trade Industry, 2018, no. 6, p. 7.

[4] Related to the AI planning in China, see Yuan Hui, *Studies on the Development Planning for the New Generation of Artificial Intelligence*, in Tech Wind, 2018, no. 31, p. 37.

[5] On the approach of the National Cyberspace Security Strategy, see also Wang Kewei-Zheng Zai, *Analysis on the National Cyberspace Security Strategy*, in Digital Communication World, 2019, no. 2, p. 115.

private partnership for the further harmonization between the development and security interests.

(6) The *International Strategy of Cooperation on Cyberspace*[6], jointly issued by the Cyberspace Administration of China and Ministry of Foreign Affairs on 1st March, 2017, emphasizes the basic principles, strategic targets and action plans for the international cooperations in the are of Internet governance, and encourages the deep interaction among the public and private stakeholders to facilitate the mutual promotion between the ICT innovation and the cybersecurity.

2. Main Legislations related to cybersecurity governance

Indeed, on the basis of the values and approaches established by these Policies, the Chinese lawmaker starts to introduce the ad hoc cyber Laws and, at the same time, to reform and update the related traditional Laws, in order to provide a more systematic institutional framework. From these main legislations, the ICT companies in China can explore better their cybersecurity obligations for the compliance purpose.

2.1 In regards to the new cyber Laws, until now the most important are two:

(1) The *Cybersecurity Law*, as the actual „top-level design" for cybersecurity affairs in China, was issued by the Twenty-fourth Meeting of the Standing Committee of the Twelfth National People's Congress on 7 November, 2017 and entered into force on 1st July, 2017. This Law has 79 articles in total and is composed of the following seven Chapters: Chapter I General Provisions (Art.1-Art.14), Chapter II Cybersecurity Support and Promotion (Art.15-Art.20), Chapter III Network Operation Security (Art.21-Art.39), Chapter IV Network Information Security (Art.40-Art.50), Chapter V Monitoring, Early Warning and Emergency Response (Art.51-Art.58), Chapter VI Legal Liability (Art.59-Art.75), and Chapter VII Supplementary Provisions (Art.76-Art.79)[7].

(2) The *E-Commerce Law*, also containing cybersecurity obligations norms for this specific sector, was issued by the Fifth Meeting of the Standing Committee of the Thirteenth National People's Congress on 31 August, 2018 and entered into force on 1st January, 2019. This Law has 89 articles in total and is composed of the following seven Chapters: Chapter I General Provisions (Art.1-Art.8), Chapter II E-Commerce Businesses (Art.9-Art.46), Chapter III Formation and Performance of E-Commerce Contracts (Art.47-Art.57), Chapter IV Settlement of E-Commerce Disputes (Art.58-Art.63), Chapter V Promotion of E-Commerce (Art.64-Art.73), Chapter VI Legal Liability (Art.74-Art.88), and Chapter VII Supplementary Provisions (Art.89)[8].

Besides, in the beginning of 2019, the Legislation Plan of the Standing Committee of the Thirteen National People's Congress (2018-2022) has listed, among others, the *Personal Information Protection Law, the Data Security Law and the Telecommunication Law*, which means these three Laws will also be the future legislative reference for the discussions on the cybersecurity obligations of ICT companies in China respect to the specific technological environments.

---

[6] In relation to the values of cooperation on cyberspace for digital economy, see also Li Haiying, *Digital Economy and International Cooperation on Cyberspace*, in Civil-Military Integration on Cyberspace, 2018, no. 6, p. 24.

7 For more information on the framework of the Cybersecurity Law, see Meng Lu, *Analysis on the Rule of Law in Cyber Governance*, in Journal of Chongqing University of Science and Technology, 2018, no. 5, p. 21.

[8] Related to the regulation approach of the E-Commerce Law, see also Xue Jun, *New Questions in the Application of the E-Commerce Law*, in People's Rule of Law, 2019, no. 5, p. 1.

2.2 With reference to the reforms of traditional Laws for modern cyber governance purpose, the most relevant legislative initiatives can be found in the Chinese civil law and criminal law:

(1) The *General Provisions of the Civil Law*, adopted at the 5th Session of the Twelfth National People's Congress on 15 March, 2017 and entered into force on 1st October, 2017, has introduced the Art. 111 for the protection of personal information and the Art. 127 for the protection of data and network virtual property, both of which have enlarged the landscape of cybersecurity obligations for ICT companies[9].

(2) The *IXth Amendment of the Criminal Law*, adopted at the 16th Session of the Standing Committee of the Twelfth National People's Congress on 29 August, 2015 and entered into force on 1st November, 2015, has introduced the Art. 253-1 for the Crime against personal information, the Art. Art. 287-1 for the Crime of Illegal use of information network and the Art. 287-2 for the Crime of Assistance for cybercrime, all of which have provided the ICT companies with more criminal protection instruments in front of serious offences against their cybersecurity interests[10].

2.3 For the illustration completeness considerations, it seems necessary to point out also that there are several other related Laws, mentioned frequently during the discussions on the cybersecurity obligations for ICT companies in China, particularly: (1) the *Counterespionage Law*, adopted at the 11th Session of the Standing Committee of the 12th National People's Congress on 1st November, 2014 and accompanied with the *Detailed Rules for the Implementation* issued by the State Council on 22 November, 2017; (2) the *Counterterrorism Law*, adopted at the 18th Session of the Standing Committee of the Twelfth National People's Congress on 27 December, 2015 and amended on 27 April, 2018; as well as (3) the *National Intelligence Law*, adopted at the 28th Session of the Standing Committee of the Twelfth National People's Congress on 27 June, 2017 and amended on 27 April, 2018 (*See also III and IV for their more detailed analysis*).

3. Other relevant Norms related to cybersecurity governance

Furthermore, in order to facilitate the effective implementation of cybersecurity governance at substantive and procedural level, the Chinese Authorities don't hesitate to develop other norms in specific practice areas, which can be mainly divided in to two groups:

3.1. Firstly, at administrative level, there are various implementation norms usually issued, separately or jointly, by the State Council, the Cyberspace Administration of China, the Ministry of Public Security, the Ministry of Industry and Information Technology, etc.

These operational norms can provide more detailed practical rules for the activities of the Chinese Authorities, ICT companies and other stakeholders, already covering the issues related to online content governance, cybersecurity graded protection, critical information infrastructure protection, personal information protection, network products and services security review, cybersecurity incidents regulation and so on. Among others, the following regulations can be considered as the relevant references for understanding better the Chinese approach in this area.

---

[9] For analysis on the ratio legis of the General Provisions of the Civil Law, see also Wan Haoxuan, *Principles System of the General Provisions of the Civil Law*, in Legal System and Society, 2019, no. 13, p. 11.

[10] For more information on the background of the IX Amendment of the Criminal Law, see Wang Disheng, *Contributions of the IX Amendment of the Criminal Law for the current criminal system*, in Journal of Lanzhou Institute of Education, 2017, no. 4, p. 156.

(1) The *Regulations on Protecting the Safety of Computer Information Systems*, promulgated by the Order No. 147 of the State Council on 18 February, 1994 and amended by the Order No. 588 on 8 January, 2011, has 31 articles in total and is composed of five Chapters: Chapter I General Provisions (Art.1-Art.7), Chapter II System of Safety Protection (Art.8-Art.16), Chapter III Safety Supervision (Art.17-Art.19), Chapter IV Legal Responsibilities (Art.20-Art.27), and Chapter V Supplementary Provisions (Art.28-Art.31).

(2) The *Provisions on Internet Security Supervision and Inspection by Public Security Organs*, promulgated by the Ministry of Public Security on 5 September, 2018, has 29 articles in total and is composed of five Chapters: Chapter I General Provisions (Art.1-Art.7), Chapter II Supervision and Inspection Objects and Contents (Art.8-Art.12), Chapter III Supervision and Inspection Procedures (Art.13-Art.20), Chapter IV Legal Responsibilities (Art.21-Art.27), and Chapter V Supplementary Provisions (Art.28-Art.29).

3.2. Secondly, at judicial level, there are also numerous so called „Judicial Interpretations" issued, separately or jointly, by the Supreme People's Court and the Supreme People's Procuratorate. These general directives, focused on certain judicial phenomenon instead of single case, can offer the practice guidelines for the activities of the Chinese judicial Authorities to guarantee better the unified application of Laws on the emerging cybersecurity issues. Without doubt, it's necessary to strengthen the importance of the following two Judicial Interpretations for the purpose of this article.

(1) The *Provisions on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks*, issued by the Supreme People's Court on 21 August, 2014, has 19 articles in total and provides judicial guidelines for the civil litigation questions related to the rules of jurisdiction, the burden of proof, the forms of notifications, the attribution of liability, the legal nature of technological measures, the causes of justification, the petition for retrial, the trial supervision procedure, etc.

(2) The *Interpretation on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information*, jointly issued by the Supreme People's Court and the Supreme People's Procuratorate on 8 May, 2017, has 13 articles in total and provides a sophisticated set of operation rules for the judicial application of the Art. 253-1 (Crime against personal information) of the Criminal Law, and replies to the emerging concerns related to the criminal definition of the personal information, the classification of the personal information, the sources of legal obligations, the *actus reus* judgment rules, the *mens rea* judgment rules, the serious circumstances, the causes of justification, the criminal participation liability, the criminal assistance liability, the criminal liabilities of the entities, the lenient punishment rules, the calculation rules for the personal information, the criminal fine application rules and so on.

III. Systematic Understanding of Cybersecurity Obligations of ICT Companies

In reality, only by the systematic study of the aforementioned sophisticated cyber governance framework, it's possible to obtain a complete insight on the effective cybersecurity obligations of ICT companies in China.

In the first place, the current governance framework marks out in this regard the „bottom lines" for the daily operation activities of ICT companies:

On one hand, *there are eight activities that are clearly declared as forbidden*, i.e.: (1) using the network to conduct any activity that endangers national security, honor and interest; (2) inciting to subvert the state power or overthrow the socialist system; (3) inciting to split the country or undermine the national unity; (4) advocating the terrorism or the extremism; (5) propagating the ethnic hatred or discrimination; (6) spreading the violent or pornographic information; (7) fabricating or disseminating false information to disrupt the economic and social order; and (8) infringing upon the reputation, privacy, intellectual property rights or other lawful rights and interests of any other person.

On the other hand, *there are five conducts that are specifically provided as illegal and can be punished at administrative and criminal law level*, i.e.: (1) illegally intruding into any other person's network; (2) interfering with the normal functions of any other person's network; (3) stealing network data; (4) providing programs or tools specifically used for conducting activities endangering the cybersecurity, such as network intrusion, interference with normal functions and protective measures of the network, and stealing of network data; and (5) intentionally providing the technical support, advertising promotion, payment and settlement services or any other assistance to any other person that conducts any activity endangering the cybersecurity.

In the second place, the same Chinese cyber governance framework also gives birth to a full set of detailed cybersecurity obligations for the ICT companies in China, reflected at technical, organizational and content level, that can be mainly divided into the following four groups:

1. Obligations for the technological protection

Without doubt, the ICT companies shall adopt the technological measures to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified, especially including: (1) developing internal security management rules and operating procedures, determining the persons in charge of cybersecurity, and carrying out the responsibility for cybersecurity protection; (2) taking technical measures to prevent computer viruses, network attack, network intrusion and other acts endangering cybersecurity; (3) taking technical measures to monitor and record the status of network operation and cybersecurity incidents, and preserving relevant weblogs; and (4) taking measures such as data categorization, and back-up and encryption of important data; etc.

Besides, the ICT companies shall continuously provide security maintenance for their products and services, and shall not terminate the provision of security maintenance within the stipulated period or the period agreed upon by the parties. They shall not install malware and, when discover any risk such as security defect and vulnerability of the network products or services, shall immediately take remedial measures, inform users in a timely manner, and report to the competent Authority in accordance with relevant provisions.

Furthermore, the ICT companies shall make emergency response plans for cybersecurity incidents, and deal with system bugs, computer viruses, network attack, network intrusion and other security risks in a timely manner. When any incident endangering cybersecurity occurs, the related ICT company shall immediately initiate the emergency response plan, take corresponding remedial measures, and report to the competent Authority in accordance with relevant provisions.

2. Obligations for the organizational management

Considering the principle of proportionality, on the basis of technology and market power, the ICT companies shall also fulfill the various cybersecurity obligations at the organizational management level:

In the first place, Where the ICT companies provide network access and domain registration services for users, handle network access formalities for fixed-line or mobile phone users, or provide users with information release services, instant messaging services and other services, they shall require users to provide true identity information when signing agreements with users or confirming the provision of services. If any user fails to provide his or her true identify information, the ICT companies shall not provide him or her with relevant services.

In the second place, as the electronic information sent by and application software provided by any individual or organization shall not be installed with malware, or contain any information of which the release or transmission is prohibited by any law or administrative regulation, the electronic information release service companies and application software download service companies shall perform security management obligations.

If these companies find that any user commits any conduct as set forth in the preceding paragraph, they shall cease the provision of services, take deletion or any other handling measure, preserve relevant records, and report to the competent Authority.

In the third place, the ICT companies shall establish complaint and reporting systems for network information security, disclose the ways for filing complaints and reports and other information, and accept and handle complaints and reports related to network information security in a timely manner.

3. Obligations for the personal information protection

Actually, in today's China, the public opinion pays unprecedently high attention to the issue of personal privacy protection and building an outstanding reputation in this regard is becoming crucial for the business success of the ICT companies in the Chinese market. Therefore, the fulfillment of the obligations related to the personal information protection are widely considered by themselves as one of the top priorities, which covers at least the core legal requirements listed below:

(1) As the starting point for all, the ICT companies shall strictly keep confidential users' personal information collected by them, and establish and improve the system for the protection of users' information. They shall not divulge, tamper with or damage the personal information collected by them, and shall not provide personal information to any other person without the consent of the persons whose information is collected (except that the information has been processed in a manner that it is impossible to distinguish a specific person and it cannot be retraced).

(2) When collect and use the personal information, the ICT companies shall follow the principles of legality, rightfulness and necessity, disclose the rules for collection and use, explicitly indicate the purposes, means and scope of collecting and using information, and obtain the consent of the persons whose information is collected. They shall not collect personal information irrelevant to the services provided by them, shall not collect or use personal information in violation of the provisions of any law or administrative regulation or the agreement of both parties, and shall dispose of personal information preserved by them in accordance with the provisions of laws and administrative regulations and agreements with users.

(3) Where an individual finds that any ICT company collects or uses his or her personal information in violation of the provisions of any law, administrative regulation or the agreement of both parties, the individual shall be entitled to request the network operator to delete his or her personal information. If the individual finds that his or her personal information collected or stored by the ICT companies has any error, he or she shall be entitled to request them to make corrections and the ICT companies shall take measures to delete the information or correct the error.

(4) No ICT company may acquire personal information by stealing or any other illegal means, or illegally sell or provide personal information to any other person.

4. Obligations for the law enforcement assistance

Like in other jurisdictions where the ICT companies are comm considered as very important stakeholders also in the cybersecurity law enforcement area, the Chinese cyber governance system has introduced as well the specific norms to which they can refer when the competent Authorities require assistance or support for the law enforcement purpose.

For one thing, where any security incident occurs, the emergency response plan for cybersecurity incidents shall be initiated immediately to investigate and assess the incident, and the relevant ICT companies shall be required to take technical measures and other necessary measures to eliminate potential security hazards and prevent the expansion of the harm, and release to the public the warning information relating to them in a timely manner.

For another, where the relevant Authority at or above the provincial level finds any relatively high security risk or security incident on the network in the performance of cybersecurity supervision and administration functions, it may hold an interview with the legal representative or primary person in charge of the ICT companies according to prescribed powers and procedures, and the ICT companies shall take measures to make rectification and eliminate hidden risks as required.

Furthermore, as frequently discussed, the ICT companies shall provide technical supports and assistances to the public security and national security Authorities for their activities of investigating crimes or safeguarding national security according to the provisions of Law.

In this regard, it is necessary to point out that the similar assistance obligation of ICT companies can be found in several current Chinese Laws, including the Cybersecurity Law of 2017(Art. 28), the Counterespionage Law of 2014(Art. 13), the Counterterrorism Law of 2015(Art. 18) as well as the National Intelligence Law of 2017(Art. 7, Art. 12 and Art. 14), the effective application of which, however, should be integrated with other connected institutions established by the Chinese legal system (*See also IV for a more detailed analisys*).

IV. Principle of Legality and Cybersecurity Obligations of ICT Companies

As strengthened before, it's possible to more precisely determine the real extent of cybersecurity obligations of the ICT companies in China only by the the systematic reading of the entire Chinese cyber governance framework.

Meanwhile, in practice, the before-mentioned multi-level cybersecurity obligations cannot be interpreted beyond the numerous institutional limitations already rooted in

the current Chinese legal system, as the rational balance between the industry developments and the security interests, as well as the strict proportionality between the rights and the obligations, are always the top priority of the Chinese regulation approach in this area.

In fact, among others, the most fundamental benchmark for the fulfillment of the cybersecurity obligations by the ICT companies in China is the principle of legality, which effectively requires all stakeholders to avoid any extensive interpretation of these obligations without an explicit legal basis, in order to guarantee the correct implementation of the ratio legis.

As prominent example, specifically speaking to one of the most debated topics, with reference to the forenamed obligations of the ICT companies for the law enforcement assistance (*See also III.4 for a detailed illustration*), such interpretive paradigm is much more than emblematic and already reflected at the following three levels:

1. Principle of Legality and territorial scope of Cybersecurity Obligations

As the first interpretive limitation, it is indispensable to recall the territorial scope provided by the Chinese law for the cooperation and assistance obligations of the ICT companies.

For one thing, on the basis of the Art. 2 of the Cybersecurity Law, itself shall apply to the construction, operation, maintenance and use of the network as well as the supervision and administration of cybersecurity within the territory of the People's Republic of China. Logically, this means only the ICT companies directly operating within the Chinese territory should fulfill the cooperation and assistance obligations in front of the competent Authorities, and no overseas subsidiary of these ICT companies outside of the Chinese territory should satisfy the assistance requests of the Chinese Authorities.

For another, even in other Laws such as Counterespionage Law, Counterterrorism Law and National Intelligence Law, etc., there is no disposition that asks for extending the cooperation and assistance obligations beyond the Chinese territory to cover also the overseas subsidiaries of the ICT companies.

At the same time, for the business activities of the overseas subsidiaries of the Chinese ICT companies, the Chinese regulators commonly strengthen the necessity of the local compliance managements to guarantee the no harm for the interests of the host countries (regions):

The *Code of Conduct for Overseas Investment and Operation of Private Enterprises*, jointly issued by National Development and Reform Commission, Ministry of Commerce, People's Bank, Ministry of Foreign Affairs and All-China Federation of Industry and Commerce on 6 December, 2017, provides that the private enterprises carrying out investment and operation activities shall comply with the laws and regulations of the host countries (regions) and comply with the relevant treaty provisions and other international practices[11].

Furthermore, the same Code encourages the private enterprises to select and hire domestic and overseas firms specialized in law, assessment, and credit rating, etc., strictly implement compliance examination for major decisions and transactions, effectively conduct follow-up analysis and compliance training on the regulatory rules relevant to overseas investment business, strengthen the communication with the

[11] On the relationship between the international law and domestic law, see He Zhipeng, *Values of the International Law for Nowadays China*, in Tsinghua University Law Journal, 2018, no. 1, p. 10.

supervision departments in the host countries (regions), and actively cooperate with the supervision work.

More recently, the *Guidelines for Compliance Management of Enterprises' Overseas Operations,* jointly issued by National Development and Reform Commission, Ministry of Foreign Affairs, Ministry of Commerce, People's Bank, State-owned Assets Supervision and Administration Commission, State Administration of Foreign Exchange and All-China Federation of Industry and Commerce on 26 December, 2018, also requires that the overseas subsidiaries of the Chinese companies shall comply with the laws and regulations of the host countries (regions) related to employment protection, environment protection, data and privacy protection, intellectual property protection, anti-corruption, anti-bribery, anti-monopoly, anti-money laundering, anti-terrorist financing, trade control and financial taxation, etc., in order to effectively realize the all-round local compliance of their daily operation activities abroad[12].

2. Principle of Legality and Constitutionality of Cybersecurity Obligations

The second important interpretive limitation on the extending application of the cooperation and assistance obligations of the ICT companies is the constitutionality, which demands, among others, that: (1) the passive subject of assistance obligations should be determined; (2) the scope of assistance should be determined; (3) there should be no conflict of obligations.

(1) In regards to the first requirement of *determined passive subject of obligations*, a specific assistance obligation does not always cover all types of the ICT companies.

Actually, the Cybersecurity Law of 2017 aims the network operators (*including the owners, managers, and network service providers of the networks*) operating within the Chinese territory, which means the other ICT companies such as the manufacturers of telecommunication equipments cannot required by the Chinese Authorities to fulfill the assistance obligations on the basis of this Law when they merely engage in R&D and production and sale of telecommunication equipment.

In the same way, the Counterterrorism Law of 2015 provides the telecommunications business operators and internet service providers as the passive subjects of assistance obligations. Among them, the telecommunication business operators refer to the basic telecom service provider and the access provider, and the Internet service providers refer to providers who provide users with content services such as news, information, data, audio and video, and communication platform. Again, in this case, the manufacturers of telecommunication equipments as well as other ICT companies cannot be considered as the qualified passive subjects respect to their business activities different from the aforesaid ones.

(2) In relation to the second requirement of *determined scope of assistance*, it's also necessary to strengthen that the assistances of the ICT companies cannot serve the purpose beyond the specific scope established by the Laws.

The Counterespionage Law of 2014 applies only for the purpose of carrying out the counterespionage activities which are clearly defined by the Law itself and have obvious nature of defensive actions rather than attacking actions, which means, among others, the Chinese Authorities are not authorized to order the ICT companies to hack into products they make to spy on or disable communications of other countries. In fact, the same approach is followed also by the the Counterterrorism Law of 2015.

---

[12] On the current compliance practices of the Chinese companies, see Xie Jinhui, *Considerations on the Framework of the Compliance Practices*, in Construction Enterprise Management, 2019, no. 5, p. 25.

Meanwhile, the National Intelligence Law of 2017 refers only to the intelligence related to the conduct against the national security and other national interests of China, which means, for example, planting backdoors, eavesdropping devices or spyware in its equipment is obviously contrary to the ratio legis of the same Law.

(3) In concern of the third requirement of *no conflict of obligations*, the Chinese legal system substantively prohibits that the ICT companies can be put into a status of conflict when they are ordered to fulfill a determined obligation[13].

Among others, the first example is the National Intelligence Law of 2017, which contains a safeguard that discharges individuals and organizations from providing support, assistance and cooperation to the national intelligence agencies that would contradict their legitimate rights and interests, let alone where doing so would violate the laws of another country.

Another relevant example is the Cybersecurity Law of 2017 which prohibits definitively the conduct of installing malware, which means planting backdoors, eavesdropping devices or spyware in ICT equipments will be punished strictly according to the same Law. Without doubt, it's a serious conflict of obligation under this perspective if the Chinese Authorities require the ICT companies to plant backdoors, eavesdropping devices or spyware, hence this kind of requirement will be considered as unlawful.

3. Principle of Legality and due process

The third fundamental interpretive limitation on the extending application of the cooperation and assistance obligations of the ICT companies is the due process, which requires, among others, that: (1) the operational procedure of law enfocement; (2) the liability of the competent Authority; and (3) the right remedy of the interested party.

(1) In accordance to the first requirement of *operational procedure of law enforcement*, it's mandatory for the competent Authority to follow the operational procedure provided by the applicable Law when they exercise the statutory duties[14].

In case of the Cybersecurity Law of 2017, the special procedural provisions are indeed established. For example, information obtained by relevant authorities in fulfilling their duties of protecting cyber security can only be used for the purpose of maintaining cyber security, and must not be used for other purposes (Article 30).

Furthermore, the Counterespionage Law of 2014, the Counterterrorism Law of 2015 as well as the National Intelligence Law of 2017 respectively provide stringent procedural requirements and restrictions on specific law enforcement activities

(2) On the basis of the second requirement of *liability of the competent Authority*, the same competent Authorities should be liable for their law enforcement actions.

According to the Cybersecurity Law of 2017, if relevant authorities are in violation of the provisions of Article 30 of this Law and use the information obtained in performing their duties of cyber security protection for other purposes, the directly responsible person in charge and other directly responsible personnel shall be punished according to law. If the staff of the relevant authorities neglects their duties, abuses their power, or engages in malpractice for personal gains, which activities don't reach the threshold of crimes, they shall be subject to sanctions (Article 73). If they violate the

---

[13] On the principle of no obligation conflict in China, see Liu Sheng, *Studies on the Obligation Conflict*, in Law and Economy, 2011, no. 4, p. 9.

[14] On the legality requirements of statutory duties, see Wang Fang, *Legality for the Statutory Duties of the Modern Government*, in People's Tribune, 2019, no. 1, p. 15.

provisions of this Law and cause other people to suffer damage, they shall bear civil liability according to law.

Also the the National Intelligence Law of 2017 provided that the conduct of the state intelligence agency and its staff is subject to legal restrictions, and potential abusive conduct, including infringement of legitimate rights and interests of citizens and organizations, would be subject to investigation and punishment in accordance with the law. The same liability approach can be found in Counterespionage Law of 2014 as well as the Counterterrorism Law of 2015.

(3) For the sake of the third requirement of *right remedy of the interested party*, any ICT company has the right to seek judicial relief in accordance with the Administrative Procedure Law.

A common framework under the Cybersecurity Law of 2017, the Counterespionage Law of 2014, the Counterterrorism Law of 2015 as well as the National Intelligence Law of 2017 is that, as stipulated in article 12 of Administrative Procedure Law, citizens, legal persons and other organizations shall have the right to bring a lawsuit to the people's court if they believe that the administrative authorities have violated the law.

References

1. He Zhipeng, *Values of the International Law for Nowadays China*, in Tsinghua University Law Journal, 2018, n. 1, p. 10.

2. Li Congyuan, *Future of „Internet Plus" Action Plan*, in Information Research, 2018, n. 2, p. 95

3. Li Haiying, *Digital Economy and International Cooperation on Cyberspace*, in Civil-Military Integration on Cyberspace, 2018, n. 6, p. 24.

4. Liao Jingwei-Yu Juan, *Research on the Big Data Industry*, in Modern Business Trade Industry, 2018, n. 6, p. 7.

5. Liu Sheng, *Studies on the Obligation Conflict*, in Law and Economy, 2011, n. 4, p. 9.

6. Meng Lu, *Analysis on the Rule of Law in Cyber Governance*, in Journal of Chongqing University of Science and Technology, 2018, n. 5, p. 21.

7. Wan Haoxuan, *Principles System of the General Provisions of the Civil Law*, in Legal System and Society, 2019, n. 13, p. 11.

8. Wang Disheng, *Contributions of the IX Amendment of the Criminal Law for the current criminal system*, in Journal of Lanzhou Institute of Education, 2017, n. 4, p. 156.

9. Wang Fang, *Legality for the Statutory Duties of the Modern Government*, in People's Tribune, 2019, n. 1, p. 15.

10. Wang Kewei-Zheng Zai, *Analysis on the National Cyberspace Security Strategy*, in Digital Communication World, 2019, n. 2, p. 115.

11. Xie Jinhui, *Considerations on the Framework of the Compliance Practices*, in Construction Enterprise Management, 2019, n. 5, p. 25.

12. Xue Jun, *New Questions in the Application of the E-Commerce Law*, in People's Rule of Law, 2019, n. 5, p. 1.

13. Yuan Hui, *Studies on the Development Planning for the New Generation of Artificial Intelligence*, in Tech Wind, 2018, n. 31, p. 37.

14. Zhang Boqin-Sun Shuyang, *2019 Development Trend Prospects of Network Security in China*, in Cyberspace Security, 2019, n. 1, p. 37.

Criminal law protection of the financial interests of the EU results and conclusions of a Hercule III project*

Prof. Dr. Ákos Farkas CSc*
University professor
University of Miskolc
Faculty of Law

Dr. habil. Judit Jacsó PhD**
Associate professor
University of Miskolc
Faculty of Law

Dr. Bence Udvarhelyi PhD***
Assistant professor
University of Miskolc
Faculty of Law

Abstract:

The main objective of this paper is to present the most important conclusions and findings of the „Criminal law protection of the financial interests of the EU – Focusing on money laundering, tax fraud, corruption and on criminal compliance in the national legal systems with reference to cybercrime" project which was coordinated by the University of Miskolc, Faculty of Law. In the framework of the project a practice-orientated comparative research was carried out, two international conferences and two international workshops were organised, based on the results of which the Hungarian project team formulated the following conclusions.

Keywords: *European criminal law, protection of the financial interests of the European Union, EU fraud, money laundering, corruption, protection of fundamental rights, cybercrime, criminal compliance*

I. Introduction – short presentation of the „HUUNIMISKOLCPFI - 786253" Hercule III project

The *„Criminal law protection of the financial interests of the EU – Focusing on money laundering, tax fraud, corruption and on criminal compliance in the national legal systems*

* This publication was funded by the European Union's HERCULE III programme. The content of this publication represents the views of the authors only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

** E-mail: jogfa@uni-miskolc.hu.
*** Email: jogjacso@hotmail.com.
**** Email: jogbence@uni-miskolc.hu.

with reference to cybercrime" project was funded by the European Anti-Fraud Office's (OLAF) HERCULE III programme (2014–2020) *„Legal Training and Studies 2017"*. The project started in January 2018 with the University of Miskolc as main coordinator and academics and practitioners from six countries (Austria, Germany, Greece, Hungary, Italy and Romania).

The *general objective* of the project was the protection of the financial interests of the European Union and preventing and combating fraud, corruption, money laundering and other illicit activities affecting the financial interests of the Union. The action aimed at focusing on new practical challenges related to the topic (e. g. cybercrime).

In connection with this general objective, the *specific objectives* of the project were the following:

– the raise of the awareness of the branches of legal professions that are involved in the protection of the financial interests of the European Union through organizing international conferences, workshops and trainings

– improvement of cooperation between practitioners and academics

– comparative analysis of the legal regulation and practice of the Member States involved

– exchange of information and best practices

– use of the results in the legal education

– examination of the relationship between EPPO and non-EPPO countries and fostering the sensitiveness in connection with this question.

The project was coordinated by the University of Miskolc, Faculty of Law. The Hungarian project team included Prof. Dr. Ákos Farkas (university professor, project manager), Dr. habil. Judit Jacsó (associate professor, project coordinator), Dr. Bence Udvarhelyi (assistant professor, project coordinator), Dr. Erika Váradi-Csema (associate professor, project member) and dr. László Dornfeld (PhD student, project member).

In the project, the University of Miskolc had the following cooperation partners: National Office for the Judiciary, Office of the Prosecutor General of Hungary, National Tax and Customs Administration of B-A-Z County, Hungarian Financial Intelligence Unit of the National Tax and Customs Administration and LeitnerLeitner Budapest. Experts from five other Member States also participated in the project, including Prof. Dr. Gerhard Dannecker (Unversity of Heidelberg), Prof. Dr. Robert Kert (Vienna University of Economics and Business), Prof. Dr. Richard Soyer (University Linz), Prof. Dr. Maria Kaiafa-Gbandi (University of Thessaloniki), Prof. Dr. Mirisan Valentin (University of Oradea) and Dr. Vincenzo Carbone (University of the International Studies of Rome). Judges, public prosecutors and other academic and practical experts from the six Member States also participated in the implementation of the project.

The *opening conference* of the project with the title *„The Criminal Law Protection of the Financial Interests of the European Union Manifestations with Special Issues"* was organized in the University of Miskolc on the 23-24th March 2018. The aim of the conference was the practice-oriented discussion of the main questions and various special forms of the criminal law protection of the financial interests of the European Union through the presentation of the good practices of the Member States. The conference was focused on the criminal offences which fell in the narrower sense of the notion of EU fraud as well as on horizontal challenges like cybercrime and compliance, which were analysed in the context of the protection of the Union's financial interests.

Following the opening conference *two workshops* were held. The first workshop on the topic of corruption and money laundering was organized on the 2-4th July 2018 by

the project members from the Vienna University of Economics and Business and the University of Miskolc. The second workshop on VAT fraud was organized on 29-31st October 2018 by the University of Oradea and University on Miskolc. These events enabled the local (Austrian and Romanian) practitioners to share their experiences on the subject topics.

The closing event of the project was a Winter Academy with the title *„Current questions and answers relating to the criminal law protection of the financial interests of the European Union"* which was held on the 14-16th February 2019 at the Hungarian Judicial Academy. The event was organized by the Faculty of Law of the University of Miskolc, the Association of Hungarian Lawyers for the European Criminal Law, the Research Centre for European Criminal Law of the Faculty of Law of the University of Miskolc and the National Office for the Judiciary. The about one hundred participants of the Winter Academy could hear highly informative professional lectures, which were accompanied by a lively professional discourse. The complexity of the topics was clearly visible, since theoretical and practical experts working in different fields could express their opinion in connection with the topics of the conference[1].

II. Conclusions of the project

Based on the results of the complex, practice-oriented comparative research carried out within the framework of the project; the lectures of the international conferences and workshops and after detailed consultations with the foreign cooperatives, the Hungarian project group came to the following conclusions.

1. General conclusions in connection with the criminal law protection of the financial interests of the European Union

1) The Treaty of Lisbon can be regarded as an important milestone in the history of the protection of the financial interests of the European Union, since it empowered the European Union with a supranational legislative competence in the field of the protection of the financial interests of the Union. This legislative competence is regulated in Article 325(4) TFEU, according to which, *„the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, after consulting the Court of Auditors, shall adopt the necessary measures in the fields of the prevention of and fight against fraud affecting the financial interests of the Union with a view to affording effective and equivalent protection in the Member States and in all the Union's institutions, bodies, offices and agencies"*. These provisions of the Treaty enable the Union to adopt directly applicable, supranational criminal law norms in the form of regulations in this field. However, there are scholars and Member States who do not accept such a competence.

2) In 2017, the European Union adopted a new Directive on the fight against fraud to Union's financial interests by means of criminal law (PIF Directive)[2]. Although the European Union legislator could have adopted the Directive based on Article 325(4) TFEU, the legal basis of the Directive finally became Article 83(2) TFEU. According to

[1] More information about the activities and results of the project and the lectures and articles of the international conferences and workshops can be found at the website of the project: https://hercule.uni-miskolc.hu/.

[2] Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to Union's financial interests by means of criminal law, OJ L 198, 28.7.2017, pp. 29-41.

Article 83(2) TFEU, *„if the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned".* Since the Directive only contains minimum rules concerning the definition of criminal offences and sanctions with regard to combatting fraud and other illegal activities affecting the Union's financial interests, this decision pays attention to the national sovereignty of the Member States. However, a regulation could be a more effective tool for the protection of the financial interests of the European Union.

3) The PIF Directive regulates fraud as well as money laundering, corruption and misappropriation affecting the Union's financial interests. However, in order to provide a more effective fight against the criminal offences affecting the financial interests of the European Union, the scope of the PIF Directive could be extended to other criminal offences which could harm the financial interests of the European Union. For example, issuing of bogus invoices which can be qualified as aiding in tax evasion, especially VAT fraud system could be regulated as a specific separate criminal offence (lex specialis to VAT fraud) penalizing the businesslike behaviour of such enterprises. It could be considered to supplement the criminal offences of EU fraud with other alternative requirements, e.g. businesslike commission or commission of the criminal offence as a member of a group formed for the purpose of repeatedly committing such acts.

4) The PIF Directive regulates criminal offences affecting the Union's financial interests for which the European Union has already adopted several legal acts. In connection with these acts, the European Union has to pay special attention to guarantee the horizontal coherence between these legal acts since there could be practical problems in connection with their application. For example, regarding money laundering there are three different EU provisions, all of which have an impact on national legislation some of which are the same, but partly they are different:

- The 4th Anti-Money Laundering Directive[3], which in principle pursues preventive objectives, but which has led to the introduction of criminal offences in most of the Member States, has therefore influenced the national criminal laws. All PIF offences (with the possible exception of „misappropriation") are predicate offences of the 4th Money Laundering Directive's notion of money laundering.
- The PIF Directive obliges the Member States to introduce a criminal offence of money laundering involving property derived from any PIF offence. For the definition of money laundering it refers to the definition of the Anti-Money Laundering Directive. This means that the legal definition of the Money Laundering Directive must be applied to PIF offences.
- The Directive on combating money laundering by criminal law (6th Anti-Money Laundering Directive)[4] provides for an obligation to introduce a criminal offence of money laundering. The definition of money laundering in this directive is not exactly the same as the definition in the Anti Money Laundering Directive. Since money laundering as regards PIF offences as predicate offences is explicitly excluded from the scope of the

[3] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, pp. 73–117.

[4] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284, 12.11.2018, pp. 22-30.

Directive on combating money laundering by criminal law, for money laundering involving property derived from PIF offences the definition of money laundering is different compared to all other predicate offences foreseen in the Direction on combating money laundering by criminal law.

This leads to the result that Member States have different obligations because of different legal obligations and it might be a challenge to establish provisions which are in line the different EU regimes on money laundering.

5) Member States shall adopt and publish, by 6 July 2019, the laws, regulations and administrative provisions necessary to comply with the PIF Directive. In order to implement the provisions of the PIF Directive, an intensive legislation began in the Member States.

6) In 2017, the European Union adopted a Regulation on the establishment of the European Public Prosecutor's Office (EPPO Regulation)[5]. According to the Regulation, the EPPO shall be competent for the criminal offences affecting the financial interests of the Union in the PIF Directive as well as for any other criminal offence inextricably linked to these criminal conducts. In order to ensure an effective and unified fight against these criminal offences and to guarantee coordinated investigative measures it would be essential for the EPPO to exercise its competence in all cases where there is a possibility for the threat of the financial interests of the European Union.

7) The EPPO will not be applicable for all Member States; it will be established in the form of enhanced cooperation. However, for the unified protection of the financial interests of the European Union, it would be helpful to conclude an agreement between the non-EPPO Member States and EPPO Member States in order to develop an efficient and active cooperation. The Hungarian model („network model") could be regarded as a model for the cooperation between Member States that do not participate in the EPPO and the EPPO.

8) According to the recent judicial practice of the Court of Justice of the European Union, the effective protection of the financial interests of the European Union could lead to the challenge of fundamental rights and fundamental principles of criminal law. This tendency could lead to the decrease of the level of the procedural guarantees, too. Therefore, it is necessary to find a proper balance between the two competing interests: the protection of the fundamental rights and the protection of the financial interests of the European Union.

2. Special conclusions focusing on VAT fraud

9) Several documents of the European Union have highlighted the importance of the problem of tax fraud, particularly VAT fraud.

10) It can be regarded as a significant development in the field of the fight against VAT fraud within the European Union, that the scope of the PIF Directive covers VAT fraud as well. The EU legislator has also taken into account with regard to it the case law of the Court of Justice of the European Union, according to which there is a direct link between the collection of VAT revenue in compliance with the European Union law applicable and the availability to the European Union budget of the corresponding VAT resources, since any lacuna in the collection of the first potentially causes a reduction in the second. Therefore, the PIF Directive foresees minimum rules concerning the

[5] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office, OJ L 283, 31.10.2017, pp. 1-71.

definition and sanctions of VAT fraud, since it has to cover the most serious forms of VAT fraud, in particular carrousel fraud, VAT fraud through missing traders, and VAT fraud committed within a criminal organization.

11) Compared to other cases of EU fraud, the PIF Directive has narrowed the application of the Directive to VAT fraud, since the Directive only applies to this criminal offence if it is connected with the territory of two or more Member States of the Union and involves a total damage of at least EUR 10.000.000. According to the preamble, the notion of „total damage" refers to the estimated damage that results from the entire fraud scheme, both to the financial interests of the Member States concerned and to the Union, excluding interest and penalties. This solution resulting of a political compromise could cause practical problems in connection with the cross-border carrousel fraud cases.

12) The operation of tax systems falls primarily within the competence of the Member States. The organization of the tax administration, the control of taxable persons and the collection of the taxes are areas which belong to competence of the Member States. However, in order to ensure the proper functioning of the internal market and to provide an efficient protection of the financial interests of the European Union, the harmonization of substantive criminal law of the Member States plays an essential role. The PIF Directive could be regarded as an important step in this process.

13) However, there are a number of practical problems in connection with the fight against VAT fraud caused by the substantial difference between the regulations of the Member States. While in some Member States (Germany, Austria), self-reporting is regulated as a criminal impediment in case of tax fraud, in other Member States it is an unknown legal institution. Therefore, the introduction of a clear regulation of strategies by active repentance and self-reporting can be considered preferable.

14) The exchange of information (international requests) between EU Member States should be continuously improved and accelerated. According to the currently applicable rules, the deadline of the execution of the requests is 90 days which can be extended and there is no sanction in case of the lack of the fulfilment of this request. The European Union should prescribe sanctions in case of the non-compliance with the international requests taking into account the fundamental rights and principles, which could foster a more effective cooperation between the authorities of the Member States.

15) The introduction of the online cash register system in all EU Member States and the ameliorating of the electronical visibility given to tax administrations in the European Union in order to determine which commercial transactions have taken place between businesses in the Member States taking into consideration the data protection rules should be regarded as an important step to make. These could trigger the acceleration of the information, as the information requested could be directly available.

16) In 2018, the European Commission issued a proposal according to which the transitional destination VAT system would be replaced with the country of origin principle. It would result that the taxpayer will be taxed after the purchase in the country where he bought the good concerned, and not in the country where he was established for economic purposes. This measure would significantly reduce the functioning of the current taxpayers' sales chains, as the tax liability could therefore no longer be concealed from the tax authorities concerned. This would result in the termination of the currently applicable fraud mechanisms and make criminal law less necessary according to the ultima ratio principle.

3. Special conclusions focusing on money laundering

17) In 2018, the European Parliament and the Council adopted a new directive on the fight against money laundering by criminal law (6th Anti-Money Laundering Directive), which can be considered as an important milestone in the history of the Anti-Money Laundering legislation of the European Union. It is important to emphasize that the 6th Anti-Money Laundering Directive supplements and not replaces the preventive 4th Anti-Money Laundering Directive and its amendment (5th Anti-Money Laundering Directive)[6]. Since the Treaty of Lisbon, money laundering is among the ten particularly serious crimes with a cross-border dimension, i.e. the so-called eurocrimes referred to in Article 83(1) TFEU, in connection with which the European Union obtained legal harmonization competence. However, it is important to emphasize that the EU legislator has already regulated money laundering before the Lisbon Treaty in order to effectively protect the internal market.

18) One of the most significant development of the new Anti-Money Laundering Directive was the extension of the catalogue of the predicate offences. The Directive lists approximately 30 criminal offences as predicate offences and as a general rule it states every criminal offence can be regarded as predicate offences which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards Member States that have a minimum threshold for offences in their legal systems, any offence punishable by deprivation of liberty or a detention order for a minimum of more than six months.

19) Money laundering has also been regulated by the PIF Directive, therefore it can be regarded as a criminal offence affecting the Union's financial interests. According to the PIF Directive, money laundering are the conducts described in the 4th Anti-Money Laundering Directive involving property derived from the criminal offences covered by the PIF Directive (EU fraud, corruption, misappropriation). However, the 6th Anti-Money Laundering Directive states that it does not apply to money laundering as regards property derived from criminal offences affecting the Union's financial interests, which is subject to specific rules laid down in the PIF Directive. Money laundering cases may therefore be subject to different adjudication depending on whether they affect the financial interests of the Union or only the interests of the Member States. It may be a question how to separate the money laundering cases based on this aspect.

20) In addition to defining the substantive elements of money laundering, the 6th Anti-Money Laundering Directive also lays down rules to facilitate criminal proceedings. In order to ensure the effective fight against money laundering, the Directive states that a prior or simultaneous conviction for the criminal activity from which the property was derived is not a prerequisite for a conviction for money laundering. Furthermore, the conviction for money laundering can also be possible where it is established that the property was derived from a criminal activity, without it being necessary to establish all the factual elements or all circumstances relating to that criminal activity, including the identity of the perpetrator.

21) Regarding the cross-border nature of money laundering, it can be problematic in the practice where the predicate offence and the money laundering was committed in different Member States. In line with previous preventive regulations, the 6th Anti-

[6] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directives 2009/138/EC and 2013/36/EU [OJ L 156, 19.6.2018, pp. 43-74.

Money Laundering Directive also states that there should be no obstacle to the prosecution of money laundering if the predicate offence was committed in another Member State or in a third country. In this case, the conduct has to constitute a criminal activity in the criminal law of the Member State concerned.

22) Member States should ensure that certain types of money laundering activities are also punishable when committed by the perpetrator of the criminal activity that generated the property *(„self-laundering")*. In such cases, where the money laundering activity does not simply amount to the mere possession or use of property, but also involves the transfer, conversion, concealment or disguise of property and results in further damage than that already caused by the criminal activity, for instance by putting the property derived from criminal activity into circulation and, by doing so, concealing its unlawful origin, that money laundering activity should be punishable. Although the criminalization of self-laundering was introduced due to the requirements of the FATF, this could cause doctrinal problems in the national legal systems of the Member States, e.g. if the result is a double incrimination.

23) The national preventive AML/CFT regimes play an important role in the fight against money laundering. In particular, the important role of the financial intelligence units (FIUs) has to be highlighted. FIUs receive STRs/SARs, analyse them, disseminate the result of their analysis and exchange information in international context. As for the dissemination function, FIUs can proactively trigger cases of money laundering as well as support ongoing cases with financial and other information on funds that are the proceeds of criminal activity. However, all the above-mentioned actions of FIUs have to respect the fundamental right of the citizens and be monitored under this perspective.

4. Special conclusions focusing on corruption

24) Similar to money laundering, corruption can also be subject to legal harmonization of the European Union according to Article 83(1) TFEU.

25) Corruption constitutes a particularly serious threat to the Union's financial interests, which can in many cases also be linked to fraudulent conduct. Therefore, active and passive corruption is also regulated in the PIF Directive which defines their definition and the applicable sanctions.

26) Since passive corruption can only be committed by a public officer and active corruption can also be committed in relation to a public office, the PIF Directive contains the definition of public officials which covers all relevant officials, whether holding a formal office in the Union, in the Member States or in third countries. One of the most important improvements of the PIF Directive was the extension of the notion of public officer. As private persons are increasingly involved in the management of Union funds, in order to protect Union funds adequately from corruption, the definition of public official needs to cover persons who do not hold formal office but who are nonetheless assigned and exercise, in a similar manner, a public service function in relation to Union funds, such as contractors involved in the management of such funds.

27) Corruption is one of the most difficult crimes to investigate and prove. The mechanisms for criminal exploration and investigation, control and supervision mechanisms could be reinforced, and the access to electronic data is expected to facilitate e-evidence. An extension of the retention period of electronic data could be considered. Furthermore, the European Union has to establish a systematic protection for whistleblowers[7].

---

[7] See: Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law, COM(2018) 218 final, 23.4.2018.

5. Special conclusions in connection with criminal procedural questions and the protection of fundamental rights

28) The harmonization of the substantive criminal law of the Member States can only contribute in a more effective protection of the financial interests of the European Union if the criminal procedural rules of the Member States are also approximated for cross-border cases. Therefore, the European Union should focus on the establishing minimum rules for the specific aspects of criminal procedure, especially the gathering, evaluation and mutual admissibility of evidence, while respecting fundamental rights.

29) In the context of cross-border crime, it is also crucial to define and harmonise the mutual elements of fair trial requirements. This is also of utmost importance from the point of view that, according to the judicial practice of the Court of Justice of the European Union, the principle of effectiveness requires a re-evaluation of procedural safeguards. In this context, the European legislator must examine which common aspects and elements of the areas of the fair trial (rights of accused persons, rights of the defendants, presumption of innocence, etc.) can be further developed.

30) Although mutual recognition of cross-border evidence works in practice, mutual trust in principle could be further strengthened by harmonization measures. The Member States could cooperate more effectively if they had sufficient information on the procedural rules of the Members States. A standardized „information sheet" developed by each Member State for each investigative measure could provide the basis for the development of mandatory rules by the courts and enable the defence to argue for a fair trial in which evidence is not admissible. Some harmonized rules on the documentation of investigative measures may also be helpful.

31) According to the Treaty of Lisbon, the principle of mutual recognition is the cornerstone of the judicial cooperation in criminal matters. However, the recent jurisdiction of the Court of Justice of the European Union formulated a number of principles which could hinder mutual recognition. According to the judicial practice of the Court of Justice, the principle of mutual recognition can be rejected if there is objective, reliable, specific and properly updated evidence of systemic or generalised deficiencies in connection with the protection of human rights in the Member States concerned. In order to avoid abuse of decisions in the Member States, the European Union should find an appropriate balance between the effective cooperation in criminal matters and the protection of the fundamental rights with regard to the Commission's proposal on the protection of the Union budget in case of general deficiencies in the area of the rule of law in the Member States[8].

32) In order to ensure effective protection of the financial interests of the European Union, the EU must place greater emphasis on administrative cooperation with the Member States and with third countries.

6. Special conclusions in connection with cybercrime

33) Cyberspace is a perfect environment for criminal activity, and as technology advances, it is fundamentally changing crime. Most of what is collectively referred to as 'cybercrime' is basically old criminal behaviours committed through new means, but there are also new crimes that take place entirely in cyberspace (e.g. hacking). Cybercrime is a global phenomenon and it is a growing new threat in the areas of money

[8] Proposal for a Regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States, COM(2018) 324 final, 2.5.2018.

laundering, corruption and VAT fraud. Previous regulations drafted before the digital era fail to properly combat cybercrime and therefore new regulations are needed, preferably at EU level, but over-regulation must be avoided as it can hinder the further development of new technologies. Especially, the development of AI must be monitored.

34) The 4th and 5th Anti-Money Laundering Directives are certainly a step in the right direction as they focus on reducing the risks of virtual currencies and limiting the use of prepaid credit cards. The players in the crypto-currency market are now obliged to comply with the anti-money laundering rules. This market is inherently decentralized and lacks any authority, so great care must be taken to ensure that these rules are effectively enforced at national level. One solution could be a mandatory registration of users and a ban on certain aspects of the use of crypto currencies, aimed at keeping them untraceable. Further rules are needed, especially on the issues of taxation and confiscation of crypto currencies.

35) The proposed E-Evidence Regulation and the proposed European Union Directive[9] can be considered as an important development. The European Investigation Order[10] was mainly aimed at producing physical evidence, so the idea of a new European Production Order exclusively for producing e-evidence is certainly useful. It will enable authorities to obtain e-evidence within a very short period of time directly from service providers irrespective of their country, which is an ideal and convincing solution to the current problems of the current mutual legal assistance regime. EU legislation will also be applied to service providers established in third countries, which solves a long-standing problem of large technology companies not complying with EU rules. One of the weaknesses of the proposed regulation is the lack of rules on data retention, which could potentially lead to the data requested are no longer being available, while one should also be more cautious about fundamental rights protection, as in this field private individuals are acting in the field of gathering evidence.

36) New technologies should be used to solve problems. A system that logs transactions from electronic cash registers can be critical in preventing the concealment of income. The use of electronic invoices could also contribute to the transparency of the economic life and reduce the number of false invoices. There are no concrete answers to the problems raised, the approach should be „pilot project-like" and ideas from the private sector should not be excluded. Artificial Intelligence (AI) could be developed and used to monitor suspicious activities, log and analyse huge amounts of data with regards to its downsides (it cannot react to unforeseen situations, the question of accountability if it makes a mistake), respecting the rights of personal data and the fundamental rights.

37) The share of good practice and knowledge is very useful in preventing and prosecuting cybercrime, which adversely affects the financial interests of the European Union.

7. Special conclusions in connection with criminal compliance

38) Compliance is a broad term which must be framed. The term compliance, as it is used in the fight against economic crimes, tax crimes and corporate criminal law,

---

[9] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17.4.2018; Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, 17.4.2018.

[10] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, pp. 1-36.

refers to compliance with legal obligations (whereas non-compliance – which may or may not be a criminal offence – in any case creates an environment in which criminal offences can be committed). Thus, corporate criminal liability could be considered as a strengthening factor in the development of compliance structures that protect also the financial interests of the European Union.

39) (National) specialized public prosecutors against economic crimes and corruption turn out to be effective in investigating economic crimes. Where not yet done, implementation should be considered.

8. Special conclusions in connection with criminological questions

40) In order to make international comparisons, to identify trends and to develop effective preventive mechanisms related to illegal activities against the financial interests of the European Union, it is necessary to establish a unified criminal statistical system in the Member States.

References

1. Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office, OJ L 283, 31.10.2017.

2. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015.

3. Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to Union's financial interests by means of criminal law, OJ L 198, 28.7.2017.

4. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284, 12.11.2018.

5. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU [OJ L 156, 19.6.2018.

6. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014.

7. https://hercule.uni-miskolc.hu/.

8. Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law, COM(2018) 218 final, 23.4.2018.

9. Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, 17.4.2018.

10. Proposal for a Regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States, COM(2018) 324 final, 2.5.2018.

11. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17.4.2018.

Economic policy, criminal policy and economic crimes

Prof. Dr. István László Gál
Head of Department of Criminal Law
Faculty of Law
University of Pécs

Abstract

Economic policy and criminal policy have many conection points. Criminal policy today cannot be regarded as an independent science, but as a separate area within criminal sciences. It is part of the general policy of the state, including legal policy. The concept of response strategies for offenses already committed. Criminal policy guides criminal legislation, but plays only a modest role in law enforcement.

Finding a correlation between economic indicators and crime is not a recent research topic. This essay examines the relationship between the economic policy and the economic crimes int he period of the economic crisis.

Keywords: *economic policy, criminal policy, economic crimes, economic crisis, crime trends, macroeconomics, penal code, statistics, European Union*

I. Economic policy and criminal policy

Today, economic policy is closely linked to macroeconomics. We mean the state's views, decisions and decisions in the most general sense of the term economic policy, which the state (government) uses to influence the economy in order to achieve its social and political goals. Economic policy has a significant influence on the decisions and room for maneuver of society and economic actors. *„The XVIII. century and nineteenth century In the early 20th century, liberal thinkers demanded that the state abstain from economic interventions. At the same time, however, the state usually defines not only the legal-institutional system influencing the development of economic processes (system control policy), but also certain variables of this process (process control policy). Economic policy intervention is, in fact, a different phenomenon, with varying degrees of need and degree"*[1].

The two most important areas of economic policy are fiscal and monetary policy. The most important element of fiscal policy can be realized by changing the expenditures and revenues of the central budget. (In addition, public finances include segregated state funds, social security and local government budgets, but these are of lesser economic policy importance.) The budget is the government's financial plan, which typically defines revenues and expenditures for one year. Government spending is close to or even above 50% of GDP in developed countries by the central budget. The state is the largest investor and the largest employer.

The tasks of economic policy can be defined in several groups. The most important tasks are:

1. economic stability (price stability, stability of growth, stability of the labor market, keeping the unemployment rate low),

[1] Peter Dobias, *Gazdaságpolitika Közgazdasági és Jogi Könyvkiadó*, Budapest, 1988, p. 17.

2. to ensure institutional and legal conditions: to build and operate the institutional system that provides and supports the order of social coexistence and the smooth functioning and growth of the economy;

3. Limiting monopolies and monopolistic endeavors

4. reduce externalities (external economic effects) and address the problems they cause;

5. reduce income disparities,

6. production of public goods,

7. production of mixed goods.

Criminal policy today cannot be regarded as an independent science, but as a separate area within criminal sciences. It is part of the general policy of the state, including legal policy. The concept of response strategies for offenses already committed. Criminal policy guides criminal legislation (for example, establishing the legal facts of new crimes, raising or reducing punishment items, etc.), but plays only a modest role in law enforcement.

According to József Földvári, while the 19th century was the century of the dogma of criminal law, 20th century is the period of criminal policy thinking. There are four phenomena behind the change of interest. First, in the context of the evolution of crime, he notes that there was a qualitative and quantitative negative change (worsening). The second reason is the conviction that crime can be affected. Its causes must be explored and prevented as far as possible. The third factor is the increase in scientific knowledge that criminology and forensics are constantly taking over. Finally, according to Földvári, the fourth reason is the unfolding of a global codification wave, which has resulted in every state making a more efficient criminal code in the 19th century[2]. According to the definition of József Földvári, the science of criminal policy is the system of knowledge on the basis of which state power can organize the fight against crime, determining the means of this fight, the conditions and ways of using these tools in accordance with the general political objectives of the state[3].

It is up to the state to protect the interests of society and ensure social coexistence. However, the negligible means of accomplishing this task are in the area of criminal law[4]. The conditions and modalities for the use of these tools are set out in criminal law. The task of criminal policy is, among other things, to elaborate on the aspects to be applied in the application of criminal law. Criminal policy is always a dynamic activity that is adapted to the quantitative, qualitative change of the crime, the sense of security of the society, and consequently it is constantly changing, the tools of which are not determined by the quantitative and qualitative changes of crime, but the level of civilization of society[5].

In Hungary, since the change of regime, liberal (mitigating) and conservative (tightening) criminal policies have been replaced from time to time. Hungary's Fourth Penal Code reflects the principles and thinking of conservative criminal policy. In spite of a number of unlawful and some legitimate criticisms, Act C of 2012, which we will call the „New Criminal Code" for a few more years, I consider myself to be a very successful law. However, I must add immediately that I cannot make a completely unbiased

---

[2] József Földvári, *Kriminálpolitika Közgazdasági és Jogi Könyvkiadó*, Budapest, 1987, p. 11-13.

[3] Idem, p. 18.

[4] Idem, pp. 32-33.

[5] Ákos Farkas, *A kriminálpolitika és a büntető igazságszolgáltatás hatékonysága* in Tanulmányok Szabó András 70. Születésnapjára Magyar kriminológiai Társaság, Budapest, 1998, p. 81.

statement, as I was a member of the four-member expert body[6] between 2010 and 2012, who helped Barna Miskolczi and his colleagues in the Ministry of Public Administration and Justice to draft the law.

The New Hungarian Criminal Code it was a particularly moderate law that had to meet the fourfold requirements of efficiency, consistency, simplicity, and modernity, as outlined by theministry's work paper[7] on conceptual starting points. On the basis of the conservative concept[8] of criminal policy, the legislator proceeded on the basis that the new Criminal Code should be as strict or as strict as possible in each detail. As before. Of course, this could not be fully adhered to in every tiny detail, but at least it can be said that it was not milder than the previous law. Although we should do it right now: a lot of the tightening planned by the current government before they came to power, already in the opposition, has already been included by previous governments in the previous CC between 2008-2010[9].

Many believe that we have succeeded in establishing the most stringent criminal code of the European Union of 28 Member States. Of course, this can be argued, but the Institute of Law of the Shanghai Academy of Sciences translated the new Hungarian Criminal Code into Mandarin in 2014-2015 and will publish it in Shanghai in autumn 2015 as a book. In China, therefore, we consider our new Codex as a model to follow, which is a democratic but yet sufficiently strict law.

In my opinion, criminal law is only very limited in dealing with the symptoms of the economic crisis – if at all[10]. I say this despite the fact that, for nearly 150 years,

---

[6] The external (assistant to one of the Hungarian faculties of law) assisting codification was set between 2010-2012. E.g. Ádám Békés (PPKE), Balázs Gellér (ELTE), László Kőhalmi (PTE) and Gál István László (PTE).

[7] The working paper we have made available describes in detail the following: *„Efficiency is a fundamental social expectation that can be formulated as a legal policy goal than the new Criminal Code most important feature. Consistency and simplicity are partly about predictability and, on the other hand, ease of use, in this respect it is an important professional criterion and the most important guarantee of efficiency. Modernity - in our view - is by no means a counterpoint to value stability. The Criminal Code the provisions that passed the test of time are not intended to be modified. However, many provisions are no longer in line with the 21st century. with the expectations of the 20th century, and with no regard to Hungary's membership of the European Union. In the current law, the alignment of the provisions of the CC in EU law did not take place in the right way, resulting in empty facts; elsewhere, the necessary deregulation was left.*

*Priority is given to rethinking the sanction system and, in particular, the penalty items related to the individual facts in the Criminal Code. to restore its internal coherence due to changes in recent years. The solution to this problem could be to eliminate the persistent lack of consistency, often with reasons, against the current CC. The 1978 Act IV. The successive amendments to the Act have led to over-proliferation of particular circumstances, not even reflecting the intentions of the government in question. As a result, more and more factual situations have become more common in their special relationship, and in many cases the sanctions of special facts are milder than the general ones. The CC- BKFO plans to achieve simplification with a clear and significant profile cleanup. „(*Conceptual Starting Points, Work Paper, KIM, p. 1).

[8] The task of criminal policy is, among other things, to elaborate on the aspects to be applied in the application of criminal law. See Földvári József, *Criminal Policy*, Economic and Legal Publisher, Budapest, 1987, pp. 32-33. Criminal policy is always a dynamic activity that is adapted to the quantity and quality of crime, and consequently to the sense of security of society. quality changes, but the level of civilization in society. See Ákos Farkas, *Effectiveness of Criminal Policy and Criminal Justice* in Studies for *András Szabó's 70th Birthday,* Hungarian Society of Criminology, Budapest, 1998, p. 81.

[9] Following the invitation of Gergely Bárándy, Member of Parliament, since 2006, I helped through the 'Professional Circle' he created with criminal legislation in the period prior to 2010 as well.

[10] István László Gál, *Gazdasági büntetőjog, gazdasági bűnözés és a jelenlegi gazdasági válság,* PTE ÁJK Gazdasági Büntetőjogi Kutatóintézet, Pécs, 2012, p. 159.

researchers have shown a connection between economic crises and the development of crime[11]. This is briefly discussed in the next section.

II. Volume of crime and economic crises

Finding a correlation between economic indicators and crime is not a recent research topic. Based on Bavarian data series from 1835 to 1861, Georg von Mayr showed a quantifiable relationship between the change in grain prices and the number of thefts. The increase in grain prices led to an increase in the number of thefts and vice versa[12].

In the 1880s, Lacassagne, a famous French criminal lawyer and criminologist, also investigated the relationship between economic factors and crime. He thought he would discover that the change in wheat prices was almost entirely in line with the change in the number of crimes against property and the effects of the economic crises[13].

During the US economic crisis of the 1890s, crime statistics were also reported. „At the beginning of the crisis, newspapers reported an increase in hours of corruption. On January 1, 1895, an article in the Chicago Daily Tribune claimed that there was the greatest number of embezzlement in 1894 since 1878, which was also a serious crisis year[14].

According to a German study conducted by Exner after the First World War, the following correlation was found[15]: the increase in the number of unemployed by one million people is expected to increase the number of convicted prisoners by ten thousand on average. Between 1882 and 1914, rye and bread prices were moving almost together with the number of known thefts in Germany, according to Eduard Joachim's research[16].

At the beginning of the 20th century, between the two world wars, Dorothy Swaine Thomas investigated the correlation between economic cycles and various crime categories between 1865 and 1915[17].

According to a study during the World Economic Crisis of 1929-33[18], crime in Germany decreased overall, but in some crime groups, growth can be clearly seen after 1929.

---

[11] In the 1880s, Lacassagne, a famous French criminal lawyer and criminologist, also investigated the relationship between economic factors and crime. He believed that the change in wheat prices was almost entirely in line with the change in the number of crimes against property, and that the effects of economic crises could also be detected. See A. Lacassagne, *Marche de la criminalité en France 1825-80* in Revue Scientifique, 1881. During the US economic crisis of the 1890s, crime statistics were also reported. On January 1, 1895, an article in the Chicago Daily Tribune claimed that there was the greatest number of embezzlement in 1894 since 1878, which was also a severe crisis year. See George A. Akerlof, Robert J. Shiller, *Animal Spirits*, Corvina Budapest, 2011, p. 91. According to a German study conducted by Exner after the First World War (see F. Exner, *Krieg und Kriminalität,* Kriminalistische Abhandlungen Heft 1, Leipzig, 1926), the following correlation emerged: an increase of one million people is expected to increase the number of convicted offenders by ten thousand on average on average between 1882 and 1914. they almost completely co-operated with the number of known thefts in Germany, according to Eduard Joachim's research (See Eduard Joachim, *Konjunktur und Kriminalität*, Offenburg, 1933, p. 19).

[12] Ulrich Martens, Wirtschatfliche Krise, *Arbeitslosigkeit und Kriminalitätsbewegung*, Freiburg i. Br., 1978 pp. 5-6.

[13] A. Lacassagne, cited, see *supra* note 11.

[14] George A. Akerlof, Robert J. Shiller, cited, see *supra* note 11, p. 91.

[15] F. Exner, cited, see *supra* note 11.

[16] Eduard Joachim, cited, see *supra* note 11.

[17] Dorothy Swaine Thomas, *Social Aspects of the Business Cycle,* New York, 1927.

[18] Bruno Gleitze, *Die Konjunkturkriminalität in der Zeit der Weltwirtschaftskrise*, W. Kohlhammer Verlag, Stuttgart und Berlin 1941, p. 7.

After the World Economic Crisis, the relationship between economic crises and crime has been studied in the US. Thorsten Sellin draws attention to the following interesting relationships in his book[19]:

1. Not all types of crimes react sensitively to changes in economic indicators; therefore, investigations should be carried out only for certain types of crime.

2. Economic change does not affect all areas to the same extent.

3. Not all social classes are equally disadvantaged by the economic crisis. The impact of the crisis is more evident in the crime of groups more affected by the crisis.

4. Finally, it is important to underline that less severe economic downturns have less impact on crime rates than larger ones.

It is interesting to note that Thomas Robert Malthus has come to the same conclusion centuries earlier than the American author in the first half of the 20th century, that not all social classes are equally disadvantaged by the economic crisis. „Unfortunately, working classes, though benefiting from the general boom, are not as big as the overall downturn.

They are suffering the most from low wages, but they cannot receive adequate compensation even during high wages. For them, economic (economic) fluctuations always bring more bad than good and keeping the well-being of the vast majority of society in mind, our goal is to maintain peace and to have equal spending[20]".

After the Second World War, along with economic indicators, the number of crimes and the number and duration of prison sentences were steadily increasing. There seemed to be no correlation between economic crises and crime.

In 1978, Ulrich Martens examined the previous research with a critical view and stated that „neither in time nor in space can there be a general statement that there is any influence on the economic situation and, in particular, on unemployment[21]. In the literature, uncertainty can be observed in the 1970s, when researchers began to question the impact of economic crises on crime at that time. „At the beginning of the 1970s, in the economic crisis, the relationship between the economy and crime was once again on the agenda of changes in the values of society as a whole. The most comprehensive study, including international comparisons, was conducted within the framework of the Council of Europe, the results of which were published in 1985[22] and the temporal evolution of crime, as Katalin Gönczöl points out in her study:

„Unlike the methods used to date, they did not rely on indicators of the social situation of offenders but tried to show the impact of changes in the above-mentioned factors on the economy of the countries concerned. The analysis covered the period from 1963 to 1981. During this period, the number of perpetrators per 100,000 convicted residents in the Federal Republic of Germany increased from 2920 to 6,600, in France from 1,350 to 5370, in England and Wales from 2250 to 5660. In addition to the continuous increase in crime, economic development in some countries was not even. Between 1950 and 1960, national income increased to varying degrees, but in all three countries, the rate of growth declined and stagnated in the second half of the 1970s. Unemployment also reached 10% and then declined strongly as a result of favourable developments. For example, at the beginning of the 1960s, the NCO had no more than 1%. From 1975 onwards, however, it rose again, and in 1980 approached the previous high values.

---

[19] Thorsten Sellin, Research Memorandum on Crime in the Depression New York, 1937, pp. 19-20.

[20] Citate Tamás Szentes, *Ki, és miért van válságban?* Napvilág Kiadó Budapest, 2009, p. 108.

[21] Ulrich Martens, cited, see *supra* note 11, p. 36.

[22] Katalin Gönczöl, *Válság – munkanélküliség – büntetőpolitika,* p. 3.

Researchers have discovered that the cyclical development of the economy has no direct correlation with the numerical development of crime. The delayed reaction to the improvement or deterioration of economic conditions in the change of crime is not apparent. Thus, the hypothesis was not proved by the research that the effect of economic conditions does not appear in the current crime, but in a statistical series of a later period. Indeed, crime has steadily increased in all three countries. However, this increase took place in countries with very different situations in terms of perpetrators per 100,000 inhabitants, at the end of the period under review - by 1981 -. This means that crime has risen by 400% in France in 18 years, by 230% in the GDR, and by 250% in England and Wales to reach roughly the same level by 1981"[23].

Contrary to the findings of the works cited by Katalin Gönczöl, international literature sources, based on research completed since the second half of the 1970s, confirm that the number of property and economic crimes is increasing during the economic crisis.

In 1976, UNSDRI (United Nations Social Defense Research Institute), based in Rome, showed that some of the more specific forms of economic crime are growing during the economic downturns and crises. In this case, effective countermeasures must be taken, which of course not only involve the use of criminal law[24].

In 1983, a German study showed a reversal, meaning that the number of prison populations and the number of psychiatric patients undergoing economic booms are decreasing[25].

The author of a monograph published in 1987[26] found the following correlations between unemployment and the incidence of some serious crimes:

- burglary 0.572
- violent crime against a person 0.529
- damage 0.494
- Theft is 0.423
- robbery 0.342
- fraud 0.338
- sexual offenses 0.158

It can also be seen that there is a significant relationship between crises and more serious types of crime with the exception of sexual offenses. High unemployment is a very strong correlation with economic recessions, a typical and regular consequence of the crisis. Another American research[27] was designed to develop a model that explains the evolution of the crime rate against wealth, using economic variables. The dependent variables used to measure the crime rate of property were obtained from the FBI's Single Crime Reporting Program. Independent variables include: expenditure on public education, unemployment rate, GDP indicator, poverty rate, average income and the amount of heroin and cocaine seized. A correlation model was used for dependent or independent variables. Using a linear regression model, all independent variables were analysed. The results were:

---

[23] Ibidem.

[24] UNSDRI, *Economic crisis and crime,* Rome, May 1976, p. 18.

[25] Hans-Günther Heiland, *Economic Crisis and Crime*, Bremen, 1983, p. 25.

[26] Steven Box, Recession, Crime and Punishment (Totowa, New Jersey 1987.) 85. p

[27] Reza Fadei-Ttahraniés, Thomas M.Green, *Crime and Society,* International Journal of Social Economics Vol. 29, no. 10, 2002. pp. 785-788.

	Rate of crime against property	Amount spent on public education	Average Income	Rate of Poverty	Level of Unemployment	Indicator of GDP	Amount of heroin and cocaine seized
Rate of crime against property	1.000	-0.518*	-0.533**	-0.246	-0.028	-0.525*	-0.175
Amount spent on public education	-0.518	1.000	0.990**	-0.068	-0.368	0.987**	0.838*
Average Income	-0.533	0.990**	1.000	-0.125	-0.407	0.995**	0.845**
Rate of Poverty	-0.246	-0.068	-0.125	1.000	0.905**	-0.175	-0.069
Level of Unemployment	-0.028	-0.368	-0,407	0.905**	1.000	-0.469*	-0.313
Indicator of GDP	-0.525	0.987**	0.995**	-0.175	-0.469	1.000	0.843**
Amount of heroin and cocaine seized	-0.157	0.838*	0.845**	-0.069	-0.313	0.843**	1.000

*Note: * The correlation is significant at 0.05;*
*** Correlation is significant at 0.01 level.*

A negative correlation can be found, for example, in the following way: as the amount spent on public education increases, the rate of crime against property decreases. So there is an inverse relationship between the two variables. These relationships are usually felt or inferred by intuition, with the exception of the negative correlation between the unemployment rate and the rate of crime against property. Although we can immediately add that the correlation is very weak (-0.028). However, many independent variables are closely related. To avoid multicollinearity problems, the model creators selected three variables for the analysis: the GDP indicator, the poverty rate, and the amount of heroin (or cocaine) seized and arrested in the country.

The regression model uses the following formula:
$Y=b_0 + b_1X_1 + b_2X_2 + b_3X_3 + e$
ahol
Y = rate of crimes against property
b_0=constans
X_1= indicator of GDP
X_2= Rate of Poverty
X_3= quantity of seized drog
e= standard mistake
The result of the regression calculation was the following:
$Y =9985.626 - 0.554 X_1 – 172.016 X_2 + 2.396$
t =(-3.132)(-5.913)(19.975)(4.323)
$R^2 =0.704$
R = 0.860

The three independent variables of the model are responsible for 74% of the change in the crime rate between 1980 and 1997. This is an unusually robust model.

After 2007, the picture is varied, but most Western studies claim that the current economic crisis has affected and is still affecting crime today. After the outbreak of the current economic crisis in Greece, for example, the fear of property and violence has increased significantly in society. This is supported by criminal statistics, as there is a significant increase in the number of thefts, burglary and robberies. Between 2009 and 2011, the number of known theft and burglary thefts increased by 33%, from 72,658 to 96,925. Meanwhile, the robberies increased by 41%, from 4,708 to 6,636 (of course, there are counter-examples here[28]. In France, a recent news contradicts this: „Crime has declined in the past nine consecutive years, the Interior Minister said on Tuesday morning and then explained that crime fell by 0.34% in France in 2011. Although property crimes fell by 1.74% in 2011, Claude Guéant also recognized a negative tendency, an increase of 16% in the number of burglary thefts)[29]".

According to the United Nations Office on Drug and Crime 2010, the Monitoring the Impact of Economic Crisis on the Crime (Rapid Impact and Vulnerability Analysis Fund), the economic crisis that broke out in 2007 can be proven by statistical models (especially ARIMA models). volume. This conclusion was reached on the basis of statistics from 15 countries. The conclusion of the research was: 1) Economic factors have a demonstrable impact on crime statistics and crime trends. 2) In the case of 11 out of the 15 countries examined, there was a significant change in the economic indicators during 2008/2009, which can be called an economic crisis. In 8 of these 11 countries, the deterioration of economic indicators had an impact on crime. 3) Crimes against violence, such as robbery, have shown the closest correlation with economic factors. In addition, in the case of deliberate killings and motorcycle thefts, the relationship was confirmed by statistical methods. 4) The model always indicates a time lag between a change in economic indicators and a change in crime statistics. On average, adverse economic events in criminal statistics are showing a 4-6 month time shift. 5) On average, for three months you can predict well the prospective future development of crime at national level or for a city based on historical crime statistics and economic variables[30].

We agree with the view that not only economic crises, but also economic booms often act as a factor increasing crime. „Sudden adverse economic changes - the rise of misery, the increase in the number of the poor - are causing the rise of deviance, such as crime, as a welcome economic growth, if it is a result of very fast processes[31]". An excellent monograph on the relationship between socio-economic development and crime has already been established in Hungary[32].

The Hungarian situation also supports the results of foreign research[33]. Due to the many changes in the Criminal Code, the statistics of the period since the change of regime provide only a limited opportunity for comparisons and conclusions. For example, in 2007, the value threshold for property crimes increased from 10,000 to $

---

[28] Sappho Xenakis, Leonidas K.Cheliotis, *The politics of crime and the financial crisis in Greece*, 2 August 2012, http://www.opendemocracy.net/sappho-xenakis-leonidas-kcheliotis/politics-of-crime-and-financial-crisis-in-greece, accessed on 20.08.2012.

[29] http://www.lejdd.fr/Politique/Actualite/Gueant-annonce-des-chiffres-de-la-delinquance-a-la-baisse-458868/ accessed 17.08.2012.

[30] www.unodc.org/documents/data-and-analysis/statistics/crime/GIVAS_Final_Report.pdf accessed on 18.08.2012.

[31] E. Durkheim, *Az öngyilkosság*. Közgazdaságiés Jogi Könyvkiadó 1967, pp. 250-251.

[32] József Gödöny, *A társadalmi-gazdasági fejlődés és a bűnözés Közgazdasági,* Jogi Könyvkiadó Budapest, 1976.

[33] http://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_zjb002.html accessed on 20. 08. 2012.

20,000, and in 2011 to 50,000 forints: all this tens of thousands of previously criminal offenses are out of sight. These acts are committed in the same way, but statistics are now registered as an offense. Looking at the past decade, it can be clearly seen from the statistics that, although with some time lag compared to the outbreak of the economic crisis, the number of known crimes in Hungary has started to rise again in the last two years. This happens despite the fact that a significant decriminalization step was taken in 2007 and 2011, with the legislator raising the value threshold twice for nearly one-third of the total crime against crime, which we estimate has reduced the number of registered crimes by tens of thousands.

III. Final thoughts

There is no clear answer to the question of why crime has been decreasing in Hungary in recent years. The possible causes are likely to all play a role in this, but it is not possible to show in a precise way, by statistical methods, which causes a decisive or primary role. The reasons for the decrease in crime are, in my opinion, the following (the order is irrelevant):

- the „crash" of the crime wave generated by the economic crisis, ie the real decline of the phenomenon (total crime)
- the new Criminal Code has been changed the crimes (formal factor)
- a tightening criminal policy after 2010 - more effective action by investigating authorities - increase in latency All these factors play a role in the reduction of visible (registered) crime, however, whether this trend will last and will continue in the years to come after 2019 cannot be said.

References

1. Akerlof, G.A., Shiller, R.J., *Animal Spirits,* Corvina Kiadó Budapest, 2011.
2. Box, S., *Recession, Crime and Punishment,* Totowa, New Jersey 1987.
3. Dobias, P., *Gazdaságpolitika Közgazdasági és Jogi Könyvkiadó*, Budapest, 1988.
4. Durkheim, É., *Az öngyilkosság,* Közgazdasági és Jogi Könyvkiadó 1967.
5. Exner, F., *Krieg und Kriminalität,* Kriminalistische Abhandlungen Heft 1, Leipzig 1926.
6. Fadei-Ttahraniés, R., Green T.M., *Crime and Society*, International Journal of Social Economics Vol. 29, no. 10. 2002.
7. Farkas, A., *A kriminálpolitika és a büntető igazságszolgáltatás hatékonysága* in Tanulmányok Szabó András 70, Születésnapjára Magyar kriminológiai Társaság Budapest, 1998.
8. Földvári, J., *Kriminálpolitika Közgazdasági és Jogi Könyvkiadó*, Budapest, 1987.
9. Gál, I.L., *Gazdasági büntetőjog, gazdasági bűnözés és a jelenlegi gazdasági válság,* PTE ÁJK Gazdasági Büntetőjogi Kutatóintézet, Pécs, 2012.
10. Gleitze, B., *Die Konjunkturkriminalität in der Zeit der Weltwirtschaftskrise,* W. Kohlhammer Verlag, Stuttgart und Berlin 1941.
11. Gödöny, J., *A társadalmi-gazdasági fejlődés és a bűnözés,* Közgazdasági és Jogi Könyvkiadó Budapest, 1976.
12. Heiland, H.G., *Economic Crisis and Crime,* Bremen, 1983.
13. http://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_zjb002.html (2012. augusztus 20.)

14. http://www.lejdd.fr/Politique/Actualite/Gueant-annonce-des-chiffres-de-la-delinquance-a-la-baisse-458868/

15. Joachim, J., *Konjunktur und Kriminalität,* Offenburg, 1933.

16. Lacassagne, A., *Marche de la criminalité en France* 1825-80, in Revue Scientifique, 1881.

17. Martens, U., *Wirtschatfliche Krise*, Arbeitslosigkeit und Kriminalitätsbewegung Freiburg i. Br., 1978.

18. Sellin, T., *Research Memorandum on Crime in the Depression,* New York, 1937.

19. Swaine Thomas, D., *Social Aspects of the Business Cycle,* New York, 1927.

20. Tamás Szentes, C., *Ki, és miért van válságban?* Napvilág Kiadó Budapest, 2009.

21. www.unodc.org/documents/data-and-analysis/statistics/crime/GIVAS_Final_Report.pdf

22. Xenakis, S., Cheliotis, L.K., *The politics of crime and the financial crisis in Greece*, 2 August 2012, http://www.opendemocracy.net/sappho-xenakis-leonidas-kcheliotis/ politics-of-crime-and-financial-crisis-in-greece, accessed on 20.08.2012.

Lobbying and Corruption: comparative legal analysis of two notions

***Aleksandar Stevanović LL.M*[1]**
Institute for Criminological and Sociological Research

Abstract

The present paper presents the key issues of lobbyng with pointing on similarities and dissimilarities in comparison to corruption.We discussed lobbying that is directed to public officials since lobbying is a broader concept that implies different impacts on the public sphere, such as „mounting grass roots campaings", „talking with the people from the press and the media" etc. After introduction which explains some general features of corruption and lobbying, a brief comparative view of two notions was imposed emphasizing *the fact that there are many similarities between them that could* jeopardize the process of lobbying as an instrument of participatory democracy. *It was stated that lobbyng is still not recognize as legitimate and necessary in democracy. Howeever, recognizing the importance of lobbyng in modern democratic societies should lead to the regulating lobbyng in an adequate manner in trying to obtain a wider confirmation. It means that every single lobbying regulation needs to ensure: transparency of the process; useful definition of terms especially of lobbyng, lobbyst and lobbyed person; accountability for violation of the lobbying and all the other relevant norms. With this lobbyng cuold be the real alternative for the traditional participatory democracy. Contrary, lobbying is considered to be a significant generator of political corruption and other financial crimes, unless it is not properly regulated from the normative point of view*

Keywords: *lobbying, corruption, participatory democracy, interest groups.*

I. Introduction

In general public opinion, lobbyng is perceived as an activity with questionable legal and legitimate base. This is mostly the result of the absence of a clear idea of what lobbying means from a legal standpoint and what kind of influence exercised on integrity and trust in public institutions and officials. Hence it is not surprising the existence of diametrically opposing views on lobbying, especially in the context of the (anti) corruptive potential. Lobbying is for one, just a euphemism for abuse material and other resources and the realization of privileged private interests, while for others, it is part of human nature embodied in the desire to represent their interests in front of everyone[2], as well as an integral and constitutive element of any democratic process.

In the academic discourse, lobbying is most often associated with corruption, primarily as a way of its manifestations, while on the other hand, when it is regulated by law, lobbying is treated as an important anti-corruption instrument. However, it is crucial

---

[1] aleksandar.stevanovic993@gmail.com

[2] B. Kašćelan, *Uloga i mesto Zakona o lobiranju u političkom sistemu Srbije* in *Srpska politička misao* br. 17 vol 29, Beograd, 2010, p. 144.

to take into consideration the fact that the lobbying activities, mostly in the doctrine of the western world, are considered to be a significant mechanism of participatory democracy. In that sense, lobbying means an integral part of a democratic society since it allows proactive citizens and their participation in the political life of the community.

However, one should be careful in arguing that lobbying is an undisputed democratic instrument. As some authors state, lobbying has not always been accepted practice in democratic systems because it was considered that directly undermines the rule of law. Moreover, the fact is that in the XIX century lobbyng was prescribed as a crime in some federal country in USA[3]. Exercising influence on the process of political decision-making out of determined legal and constitutional framework, was considered dangerous and unnecessary parallelism that breaks down the principle of the rule of law. Regardless of idealistic and utopian attitude of representative democracy, lobbying has been imposed as a social reality due to the crisis of representative and participatory democracy.

Although lobbying in its semantic sense undoubtedly involves the exercise of influence on decision-making process that is traditionally in the focus of sociological, legal and economic studies of this phenomenon, academic researchers should pay attention on the approach to the centers of political or legislative and executive power[4]. This beacause lobbying today includes highly sophisticated activity, ie. a collection of various intellectual skills, social capital and material resources that are not available to any interest group, regardless of the public interest and the general objective which the group aims to reach. Access to decision-making power centers does not mean automatically the exercise of influence on it, but it is certainly the first stage of lobbying activities to which it is not easy to reach.

The influence of different media and other social constructs contributed to the creation of so-called. „The myth of lobbying"[5] that most often causes negative connotations in public opinion and associated lobbying with corruption and illegal influence on authorities.

II. Corruption – notion and main features

The etymology of the word corruption comes from the Latin word which indicates bribery, payoffs, moral spoilage and putrefaction, decomposition[6]. As stated by Vito Tanzi, who is one of the profound authors in the field of studying corruption, it could be regard as a deliberate violation of the principle of impartiality in decision-making process in order to acquire personal benefit[7]. Daniel Treisaman points out that corruption is acquiring the private, personal and material benefits by misuseing of public authority[8]. This definition is at the academic level, considered as the most

---

[3] S. Barić, A. Anciger, *Pravna regulacija položaja lobista u Sjedinjenim Američkim Državama* in Zbornik Pravnog fakulteta sveučilišta u Rijeci br. 2 vol 39, p. 899.

[4] P. Bouwen, *Corporate lobbyng in the European Union: the logic of access* in Journal of European Public Policy 9:3, 2002, p. 366.

[5] K. Joos, *Lobbyng in the new Europe – Successful representation of interests after the Treaty of Lisbon,* John Wiley and Sons, Minesota, US., 2011, p. 15.

[6] I. Šipka, M. Klajn, *Veliki rečnik stranih reči i izraza*, Novi sad, 2007., p. 664.

[7] V. Tanzi, *Corruption Around the World* in *IMF Staff Papers* Vol. 45, No 4, 1998., p. 7.

[8] D. Treisman, *The causes of corruption: a cross-national study* in *Journal of Public Economics*, p. 2000., 76.

accepted definition of corruption, taking into account that it actually reflects the very essence of the notion[9].

However, the overall development of society influenced the reshaping of corruption forms. Thus, there are a number of partial definitions depending on the segment of social life through which prism the corruption seeks to be identify and explain. In light of this, corruption can be viewed from an economic, political, legal, cultural, social or human rights perspective. Furthermore, depending on the the level of social danger which generates, corruption could be classified as a big, medium or small[10] and in a similar context some authors are preferring to talk about the existence of white, gray and black corruption, again depending on the caused harm. The most distinctive division is makig a difference between *administrative* and *political corruption*[11]. In the first case it is a corruptive influence linked to the implementation of existing laws, rules and regulations, while the essence of corrupt captured state is unlawful influence in terms of making a strategy platform for important decisions of national interest. Political corruption means corruptive relation between centers of economic power and politicians who are in high government positions and it is rightly considered as a powerful weapon of „econimc interest" regardless of whether it comes from legal or illegal business. On the other hand, in the broadest sense, administrative corruption includes lower echelon of public employees. However, it is not always possible to make a clear distinction between these two dominant manifestation of corruption, which in practice usually interfere, but it is important, from a methodological point of view, to bear in mind certain features of these two ways of manifestation of corruption, mostly because they usually imply different conditions and causes.

Corruption is most often equated with bribery of civil servants and public office holders. This is the position that is widely accepted at the normative level. In the United Nations Convention against Corruption – UNCAC 2005 (Merida Convention) bribery of public officials was determined as a mandatory crime and many countries have implemented such concept in their criminal legislation. Bribery was divided into active and passive what has to be considered as a positive solution since without that, there is only a criminal offense of taking bribes that excludes legal basis for the prosecution of those who offer bribes.

The development of scientific research and thoughts on the concept of corruption for many years dealt only with corruption in the public sector, limiting its scope only to it. UNCAC as well as many other international institutions (World Bank, Transparency International etc.) however inaugurate the notion of corruption in the private sector as an important social phenomenon. The explanation of this should be sought primarily in the post Cold War dominance of the neoliberal and capitalism model that values private property more than the public or state property. Regardless of this, it can not be concluded that the decision making process completely transferred to the private sector, if we take into account that public authorities are still making rules and regulations that needs to be respected in private sector.

---

[9] Robert Klitgaard has further developed this definition, giving a certain amount of ethical volume when said that corruption is unlawful act of the public officials, puting not only the personal interest above interest of people and citizens who elected them, but the ideals that sworn to serve.

[10] Ćirić J. *et al.*, *Korupcija: problemi i prevazilaženje problema*, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd, 2010., p. 8.

[11] Popović D, Ilić-Popov G., *Poreska struktura i korupcija* in *Anali Pravnog fakulteta u Beogradu*, (Vasiljević M. ur.), LXII, 1, 2014. Beograd, p. 6.

Corruption is necessary to be distinguish from the category of „abuse of power" for the first time mentioned in the Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power in 1985 which was subsequently adopted by the UN General Assembly. Abuse of power can be defined as the abuse of public authority by the person to whom it is assigned what is the most obvious feature of corruption, bu the concept of the „abuse of power" is a broader concept than corruption. Abuse of power as criminological category, does not imply individual violations of the laws or individual excesses, but a flagrant and systematic violation of human rights, which is reflected through an open abuse of state imperium[12]. It would be wrong to argue that corruption is not systemic phenomenon, but it is mostly limited to the narrow economic sphere of influence. On the other hand, abuse of power usually has a political connotation and political goal, so this includes torture, killing and intimidation of political opponents, violation of the electoral process, genocide, ethnocide, unlawful expropriation etc.[13] and this is perhaps the crucial distinction between two terms.

Corruption appears to be a kind of „business offer" made to public authorities. Therefore, corruption is able to provide a sphere of interest for both sides of corrupt relationships, making them interested to extend such relation in confidence. Because of this, it is extremely difficult to detect and even harder to get to any kind of evidence that could be used in court proceedings. This „business offer" is most often the result of a system of relations and Roust Kaliyev hence rightly notes that corruption is not only taking and giving bribes that harms the public sphere[14]. Indeed, it is a systemic activity conducted by the state authorities and corruptors.

There is a notable number of theorists who consider corruption as a positive phenomenon primarily for the economic and political aspects. For exemple, Samuel Huntington states that corruption, through various business arrangements, means benefits to the groups that would otherwise have been marginalized and alienated from society, comparing its social functionality with the implementation of reforms[15].

An interesting observation on corruption as an effective remedy for reducing tax evasion gave Dilip Mookherjee. He points out that the possibility of taking bribes by tax inspectors strongly motivate them to detect taxpayers who resort to evasion. Mookherjee argues that tax evasion would consequently become less attractive way for violation of tax laws[16]. „Corruption paradox" could be also find in the example of China, which is characterized by a high level of corruption, but also a high level of economic growth and investment. It is similar with Hong Kong and Singapore, which are experiencing considerable economic success and have high indices of corruption and high rate of convictions for corruption offenses, at the same time. Furthermore, it is stated that corruption can be successful arm in dealing with bureaucracy and it is mentioned that corruption could humanize the relationship between citizens and public officials[17]. However, all the mentioned effects of the so-called. „Useful corruption" can be

---

[12] Đ. Ignjatović, *Kriminalitet države*, *Kaznena reakcija u Srbiji V deo* (Ignjatović Đ. pr.), Beograd, 2015., p. 27

[13] M. O'Brien, M. Yar, *Criminology – Key Concepts*, London, 2008., p. 159.

[14] R. Kaliyev, *Russia's Organized Crime: A Typology, part I,* Euroasia Insight, 2002., p. 1.

[15] S. Huntington, *Political Order in Changing Societies*, Yale University Press, New Haven, CT, 1968., p. 64.

[16] D. Popović, G. Ilić-Popov, *op. cit.*, Poreska struktura i korupcija, p. 9.

[17] W.A. Clark, *Soviet Official Corruption under Perestroika: A Balance Sheet,* in *Current Politics and Economics of Russia* vol. 2, no. 3, 1991., p. 209.

achieved by introducing lobbying in the legal system in the proper manner respecting the principles of the rule of law.

However, a number of studies have determined the specific correlation between corruption and negative social consequences. For example, a study group from Harvard found that increasing the level of corruption to one point leads to a reduction of foreign direct investment to 16 percent. Previously established evaluation scale of corruption points from 1 to 10. Vito Tanzi says that research has come to a result that countries with a greater presence of corrupt relationships, *ceteris paribus*, have a smaller share of collected tax revenues in GDP[18]. Finally, according to one relevant research, increasing corruption for only one percent leads to a reduction in economic growth for 0.72 percent[19].

III.Lobbying – notion and main features

Lobbying is an activity that people take unconsciously in many situations and in everyday life takes place at all levels. However, such kind of lobbying is not the subject of this work, nor is it in the focus of a legal regulation. The need for a definition of lobbying and then its adequate regulation at the normative level, primarily exists when it is carried out by professional lobbyists who possess the necessary intellectual, material and social resources, when they lobbied the representatives of public authorities and when the aim of lobbying may affect the public interest.

In particular, lobbying is an activity that aims to influence the legislative and executive authorities[20]. The citizens in accordance with the proclaimed freedom of speech and political activism are seeking to directly or indirectly achieve their political demands usually by trying to influence the process of public policy making. For that reason, collective action is necessary realized by joining in different forms of groups and organizations in order to propagate the common interests of its members. Tradiotionally, political organizations are considered to be such organization formed for creating, advocating, and then, if they come to power, implementing public policy in accordance with previously adopted principles and set agenda[21]. However, the crisis of political parties contributed to the mutual expulsion of political parties and their leadership from the citizens-voters. Many theoreticians of political science find that the way out of the crisis that participatory democracy has embarked, could be the returning political parties to the citizens, what will make them more open to civic activism and political pluralism, by developing new forms of acitivsm and participation in the making political decisions process[22]. Lobbying is just one of those forms that provide „new democracy". It is a basic tenet of democratic rights that those affected by policies have the chance to be heard[23].

---

[18] V.Tanzi, H.R. Davoodi, *Corruption, Growth, and Public Finances*, Working Paper182, International Monetary Fund, Washington, D.C., 2000., p. 473.

[19] H. Mo, *Corruption and economic Growth* in *Journal of Comparative Economics*, vol. 29 no. 1, 2001., p. 74.

[20] L. Zetter, *Lobbying The Art of Political Persuasion*, Hampshire, 2008, p. 3.

[21] A. Stevanović, *Finansiranje političkih subjekata: koruptivni potencijal i značaj adekvatnog zakonskog regulisanja* in *Finansijski kriminalitet* (Kostić, Stevanović ur.), Zrenjanin, 2018., p. 335.

[22] G. Marković, *Uticaj političkih stranaka na razvoj političke participacije,* in *Anali Pravnog fakulteta u Beogradu* br. 2, p. 110.

[23] A. Polk, *Lobbying: Private Interests and Public Conduct*, Journal for Institutional Comparisons, Spring, 2011, p. 3.

However, the problem is that the services of lobbyists are not available to everyone, and there would be absolutely no grounds to expect that lobbying as „communication channel" in which citizens interact with public authorities would not be able to include every single paricular interest. On the contrary, forming a new „lobbying elite" or those privileged who can afford professional advocacy for their own interests, could be expected. Thus, lobbying should be understood as a more efficient technique (compared to traditional organizations such as political parties) providing the particular interests of the entities that possess the greatest economic power.

Broadly, the lobbynig process is a communication process in which lobbyists seek to persaude legislative and executive authorities to protect one particular interest by insert it into the legal norm. One of the major lessons that has been drawn so far from lobbying practise is the diversity and complexity of *modus operandi* which make reliable generalizations very dificult[24].

IV. Relationship between Lobbying and Corruption – a general remarks

Lobbying and corruption are important features of many societies and political systems. Before we get into detailed elaboration of relationship between lobbying and corruption it would be of great benefit to take into account an illustrative statement that talking to someone in order to achieve something is not illegal, but on the other hand, giving money for the same thing is illegal[25].

Some authors are arguing that there are no dissimilarities between two notion and if any, they are unimportant[26]. On the other hand, it has to be underlined that lobbying and corruption should not be identified as the same process, but the fact is that lobbying obtains main features of corruption due to its nature. Some academic researh show that lobbying is more likely in democratic countries, where the media and other relevant entities are independent and where the overall political process is more democratic at all[27]. Contrary to that, political instability has a positive effect on corruption. There is also evidence that federal or decentralised states favour lobbying over corruption. In general, lobbying seems to be more effective than corruption in pure parliamentary and presidential systems[28].

Some authors note the difference between lobbying and corruption based upon the fact where influence is being sought. According to them, lobbying is a rent-seeking activity aimed at rule makers whereas corruption is a rent-seeking activity aimed at rule enforcers[29]. Previous practice showed that such determination has a limited cognitive effect. Firstly, the corruption could be directed towards rule enforcers (administrative corruption) as well as to the rule makers.

Hence, it would be quite better to separate lobbying from corruption only because of the fact that lobbying process should be based on legally prescribed procedure and

---

[24] P. Bouwen, *Corporate lobbyng in the European Union: the logic of access,* in Journal of European Public Policy 9:3, 2002., p. 365.

[25] S. Barić, A. Acinger, *Pravna regulacija položaja lobista u Sjedinjenim Američkim Državama, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39, br. 2,2018, p. 900.*

[26] G. Grossman, E. Helpman, *Protection for Sale*, American Economic Review 84, 1994, p. 845.

[27] N. Campos, F. Giovannoni, *Lobbying, Corruption andPolitical Influence*, Public Choice131(1), 2007., p. 19.

[28] F. Giovannoni, *Lobbying versus Corruption*, CESifo DICE Report, Journal for Institutional Comparisons, Spring, 2011, p. 12.

[29] *Ibidem*

transparency. If it is done in this way, it would indeed have the potential to overcome all the troubles of participatory democracy and include a greater number of citizens in social dialogue. If these conditions are not fulfilled, lobbying and corruption come to a point of overlap and then we can really conclude that there are no significant differences between them.

Furthermore, lobbying should involve advocacy for a certain collective interest, while corruption, on the contrary, always strives to provide a narrow private interest of corruptors. It does not mean that behind the proclaimed collective interest one can not hide the narrow and private interest of a few. That is why it is important to make the lobbying process transparent with clear goals, ie to know *who, whom and for what* In the lobbying process. Open and transparent institutions followed by free media could possibly enhance the decision-making process and strengthenthe reliability of the political system. However, among many others, there is still an unresolved issue of inherent asymmetry of interest representation[30]. Such problems must be solved with the adoption of the systemic norms that regulate different areas of social life

In the both cases of lobbying and corruption, it comes to efforts to influence the legislative and executive branch of government. However, in contrast to the corruption that implies a direct unlawful financial or other material benefit, lobbying should be based on explaining why some partucular interest may positively affect public interest, in accordance with the moral and legal principles that does not distort the rules of competition in the market, fiscal policy, security issue etc.

Conflict of interest is basis of corruption[31] and as we previosly explained in the paper, the existence of a particular conflict of interest is a common place also when it comes to the lobbying activities. Accordingly, decision-makers who are targets of every lobbying process are generally in a position to decide on the public interest issue. First of all public interest should be determined by taking a clear stance towards concrete proposals that lobbyists make before it, opt for a more favorable solution, and ultimately making a decision with a general validity, supported by most of the social and economic groups in a particular society.

According to one theoretical model of public interest determination offered by Richard Stewart, it is necessary to have a government that is equally open to all stakeholders when deciding on a specific issue is at question[32]. This certainly does not mean allowing an open and undue pressure on public authorities, as Jody Freeman warned in his paper when he says that although the concept of public interest is not easily comprehensively and precisely defined, it is nevertheless imperative to neutralize every kind of pressure from those representing their narrow and generally lucrative interests[33]. One of the most serious problem facing the concept of legitimate and legal lobbying is that many relevant socio-economic factors (stakeholders) do not have access to public decision makers, and hence have no real possibility to express their own views and arguments on certain issues. In such circumstances, it is quite expected that those who have the necessary resources for lobbying will adjust their interests and will aim their influence on the government officials in order to adopt measures that would allow them a privileged position in the business market etc.

---

[30] A. Polk, *op cit*, p. 5.

[31] S. Rao, H. Marquette, *Corruption indicators in Performance Assessment Frameworks for Budget Support* in *Anti-Corruption Resource Centre*, Norway, 2012, p. 12.

[32] R. Stewart, *The Reformation of American Administrative Law*, 88 HARV.L. REV. 1975., p. 1796.

[33] J. Freeman, *The private Role in Public Governance*, 75 N.Y.U. L. REV. 2000., p. 550.

From the legal stand of point, lobbying is defined as an aleatory activity, from the perspective of the one who orders lobbying. This means that in a contract that a professional lobbyist signs with a lobbying contractor, he can not foresee a fee for lobbying services depending on the outcome of lobbying. Instead of this, according to comparative legislation lobbying must to be contracted in a fixed amount. Hence, it should not be a surprise when many stakeholders who have sufficient resources, in line with business pragmatism, are rather choosing corruptive ways to „convince" public authorities in decision making process[34].

The enormous impact on whether a particular interest will be represented in a corrupt or legal manner has both the integrity of public officials, the institutions they represent, and the trust of citizens in them. According to *Exchange theory*, developed by sociologists in the 1960s[35], the relationship between private and public entities could be defined as the series of information and resources exchanging. The potential benefit that a government has from „exchanging" with private (civil) entities can be multiple, without direct and unlawful benefit derived exclusively by an official such as the case in corruption. Namely, often when it comes to discussing a narrowly professional issue, legislators hire experts (university professors, researchers, consultants...) who can act as lobbyists of a particular interest. Lobbyists can also receive other important information such as the state of public opinion in relation to some political measure and topic, the feasibility of a particular project, etc. It is important to point out the attitude of executive and legislative authorities towards large corporations employing a few thousand or tens of thousands of people. The adoption of measures relating to the business of such economic entities without consulting the representatives of their interests could jeopardize the socio-economic order of the state.

Regulation of lobbying can make a distinction in relation to corruption, but only when this regulation means: 1) *clear and functional definition of lobbying, i.e. all the activities under this term are implied*; 2) *transparency of lobbying activities*; 3) *clear determination of who is a lobbyist and who is a lobbyed person and under what conditions the process has to be conducted*; 4) *introducing a clear and adequate system of liability for violations of regulations governing lobbying.*

The Organisation for Economic Co-operation and Development addressed the question of transparency and integrity in the lobbying process within the Recommendation with Principles for Transparency and Integrity in Lobbyingas guidance to decision-makers. The Recommendation points out that the following questions must be answered in order to regulate lobbying in line with principles of the rule of law[36]:

1. Do all stakeholders have fair and equitable access to the development and implementation of public policies?

2. Do rules and guidelines on lobbying respect the socio-political and administrative context?

3. Are the rules and guidelines on lobbying consistent with the wider policy and regulatory frameworks?

---

[34] There is a tendency to shift the center of lobbying activities from engaged professional lobbyists to the strategy of direct addressing to institutions.

[35] S. Levine,P. White,*Exchange as a conceptual framework for the study of interorganizational relationships,* in *Administrative Science Quarterly*, 1961, p. 585.

[36] CleanGovBiz, *Lobbying: Influencing Decision Making with Transparency and Integrity*, OECD, 2012, p. 3.

4. Are the terms „lobbying" and „lobbyist" clearly defined in the rules and guidelines on lobbying?

5. Is sufficient information on lobbying activities publicly available?

6. Can lobbying activities be scrutinised by stakeholders?

7. Are there clear rules and guidelines of conduct for public officialson how to engage with lobbyists?

8. Do lobbyists comply with standards of professionalism and transparency?

9. Is there a coherent spectrum of strategies and practices to ensure compliancewith rules on lobbying?

10. Is the functioning of rules and guidelines on lobbying periodically reviewedto ensure compliance?

V. Conclusion

Lobbying is a practice that has become increasingly widespread today. Nevertheless, currently only a small number of countries have any regulation of lobbying[37]. It has to be mentioned that defining lobbyists is always fraught with difficulties due to different views on decision making process in society. In such circumstances, lobbying often comes to a point of overlapping with corruption, since we have already indicated that two rather similar concepts distinguish the legal basis and regulation, as well as the transparency of the whole process. When undertaken with transparency lobbying is a legitimate communication channel for interest groups to be heard and to be involved in the deliberative process of law making. If the lobbying is not based on a legal norms and transparency, we can no longer talk about lobbying but about corruption. Hence, it should be concluded that lobbying and corruption are not the same terms. Lobbying is an activity that aims to influence the legislative and executive authorities in order to ensure that as many interests as possible are heard and that they are taken into account in the process of making public decisions. In light of this, lobbying becomes a kind of functional supplement of democratic process. This definition of lobbying aims to point out the difference in relation to corruption.

However, lobbying potentially can produce significant problems for society. For exemple, forming a new „lobbying elite" of those privileged who can afford professional advocacy for their own interests, could be expected problem. In addition, lobbying is in some way parallelism in making public decisions with capacity to undermine the foundations of the state functioning. To conclude, lobbying could be a favorable instrument in the crisis of democracy, but only if it is based on the rule of law, transparency. Otherwise, it will become legalized corruption.

References

1. Barić S., Anciger A., (2018), *Pravna regulacija položaja lobista u Sjedinjenim Američkim Državama,* Zbornik Pravnog fakulteta sveučilišta u Rijeci br. 2 vol 39.

2. Bouwen P., (2002), *Corporate lobbyng in the European Union: the logic of access* in Journal of European Public Policy 9:3.

3. Campos N., Giovannoni F., „*Lobbying, Corruption and Political Influence*", Public Choice131(1), 2007.

[37] *Ibidem.*

4. Clark W.A, *Soviet Official Corruption under Perestroika: A Balance Sheet*, in *Current Politics and Economics of Russia* vol. 2, no. 3, 1991.

5. CleanGovBiz, *Lobbying: Influencing Decision Making with Transparency and Integrity*, OECD, 2012.

6. Ćirić J. et al. (2010), *Korupcija: problemi i prevazilaženje problema*, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd.

7. Freeman J., (2000), *The private Role in Public Governance*, 75 N.Y.U. L. REV., 548-49.

8. Giovannoni F., *Lobbying versus Corruption*, CESifo DICE Report, Journal for Institutional Comparisons, Spring, 2011.

9. Grossman G., Helpman E., *Protection for Sale*, American Economic Review 84, 1994.

10. Huntington S. (1968), *Political Order in Changing Societies*, Yale University Press, New Haven, CT.

11. Ignjatović Đ., Kriminalitet države, *Kaznena reakcija u Srbiji V deo* (Ignjatović Đ. pr.), Beograd, 2015.

12. Joos K., (2011), *Lobbyng in the new Europe – Successful representation of interests after the Treaty of Lisbon,* John Wiley and Sons, Minesota, US.

13. Kaliyev R., *Russia's Organized Crime: A Typology, part I,* Euroasia Insight, 2002

14. Kašćelan B., (2010), *Uloga i mesto Zakona o lobiranju u političkom sistemu Srbije* in *Srpska politička misao* br. 17 vol 29.

15. Levine S., White P., (1961) *Exchange as a conceptual framework for the study of interorganizational relationships*, Administrative Science Quarterly 5:583–601.

16. Marković, G., (2006), *Uticaj političkih stranaka na razvoj političke participacije* in *Anali Pravnog fakulteta u Beogradu* br. 2.

17. Mo H., *Corruption and economic Growth* in *Journal of Comparative Economics*, vol. 29 no. 1, 2001.

18. O'Brien M, Yar M. (2008), *Criminology – Key Concepts*, London.

19. Polk A., *Lobbying: Private Interests and Public Conduct*, Journal for Institutional Comparisons, Spring, 2011.

20. Popović D, Ilić-Popov G. (2014), *Poreska struktura i korupcija* in *Anali Pravnog fakulteta u Beogradu*, (Vasiljević M. ur.), LXII, 1/2014, 5-22. Beograd.

21. Rao S., Marquette H., (2012), *Corruption indicators in Performance Assessment Frameworks for Budget Suppor*t in *Anti-Corruption Resource Centre*, Norway

22. Stevanović A., (2018), *Finansiranje političkih subjekata: koruptivni potencijal i značaj adekvatnog zakonskog regulisanja* in *Finansijski kriminalitet* (Kostić, Stevanović ur.), Zrenjanin.

23. Stewart R., (1975), *The Reformation of American Administrative Law*, 88 HARV. L. REV. 1790-18OO

24. Šipka I., M., Klajn M. (2007), *Veliki rečnik stranih reči i izraza*, Novi sad.

25. Tanzi V., *Corruption Around the World* in *IMF Staff Papers* Vol. 45, No 4, 1998.

26. Tanzi V., Davoodi H.R., *Corruption, Growth, and Public Finances*, Working Paper 182, International Monetary Fund, Washington, D.C., 2000.

27. Treisman, D. (2000) *The causes of corruption: a cross-national study* in *Journal of Public Economics*, 399-457.

28. Zetter L., (2008), *Lobbying The Art of Political Persuasion*, Hampshire.

Criminal regulations on money laundering in Hungary

Dr. Endre Nyitrai,
National University of Public Service
Faculty of Law Enforcement

Abstract

This study shall introduce combating money laundering from the aspects of criminal law and shall analyse the statutory provisions on money laundering. Effective criminal law regulations are indispensable, with special regards to the applicable Directives of the European Union.

Keywords*: money laundering, organised crime, illicit income*

I. Introduction

Organised crime is the greatest threat to society, since it is mostly manifested in the commission of major criminal offences and effects the financial interests of the European Union as well. Its severity is also well reflected in its impulse of legislative deficits, in the use of coded languages and rare dialects, alike to the invasion to otherwise legitimate enterprises, politics and economy[1]. Ill-gotten gains are being legalized by money laundering, in certain enterprises or through financial transactions, often using pseudo-corporations or banks to assimilate the assets[2]. Furthermore, through corruption and the conduct of economic offences, networks of organised criminal groups might weaken political, social, and financial institutions, and undermine economic development and accession, sustainability and, last but not least, they imperil the rule of law as well[3]. Such economic offences, for example, fraudulent bankruptcy, capital investment fraud, fraud related to crediting, and insider dealing[4]. Corruption is much like a business agreement, and regrettably, passive corruption is well known to everyday life in Hungary[5].

Corruption is the most expansive criminal offence these days[6]. The danger of money laundering to society is allowing criminal organisations to invade legitimate economy, so they can allocate and actually practice economic power[7]. Money laundering is a method, when the profits of the crime are made whiter through the business sector

---

[1] Ürmösné, Simon Gabriella (2018), *Organised crime* in Technical English for Officers. Dialóg Campus Kiadó, Budapest, pp. 89.

[2] Ürmösné Simon, Gabriella, *Organised crime*, RTF Publishing, 2002, Budapest, pp. 39.

[3] G. Rankin, N. Kinsella, *Intelligence Management, Knowledge Driven Frameworks for Combating Terrorism and Organised Crime,* Editors: Babak Akhgar, Simeon Yates, Springer, 2018, London, pp. 171–172.

[4] Ürmösné Simon, Gabriella, White collar crime, RTF publishing, 2002, Budapest, p. 28

[5] Gál, István László, *Economic Bribery as a Part of Economic Criminal Law and a Concomitant of Political Corruption*, Journal of Eastern European Criminal Law No. 1/2014., p. 23

[6] B. Unger, G. Rawlings, *Competing for Criminal Money,* Global Business and Economis Review 10, No.3. 3–6, 2008.

[7] D. Lamberto, *General Introductory Report*. International Conference on Preventing and Controlling Money Laundering and the Use of Proceeds of Crime: a Global Approach. Courmayeur Mont Blanc, Aosta Valley (Italy) 18-20 June 1994. Official United Nations document (E/Conf.88/7), ISPAC, 2.

tesznek[8]. The target of the operation is to make the origin of the illegal money unrecognizable, wich causes some loss[9]. In addition, money laundering also jeopardizes the legitimate financial balance of the competitive markets, as the underworld infiltrates and streams its illicit incomes to economic procedures, gathering ill-gotten gains[10]. The amount of money laundered may affect the national economy of each country[11]. Globalisation of the markets and the opening of borders, moreover, technological innovations created new possibilities of profiting for the present and shaping criminal organisations, who quickly adopt to exploit legal loopholes of different geographic areas[12]. Paying tax after the income is one of the tools to disguise the origin the guilty kind[13]. Typically, unlawful income appears in cash, whereas most of the dirty money is related to trade of drugs[14].

II. Criminal regulations on money laundering in Hungary

We refer to money laundering when the perpetrator conceals the existence, source or illicit use of money obtained by criminal activity, for the purpose of making the illegally gained proceeds clean, layering and integrating seemingly legal assets to the financial world[15]. The objective of Act XXIV of 1994 on the prevention and impeding of money laundering is to seize the flows and laundering of illicit money through the misuse of financial and investment systems. In accordance with the provisions of the First Council Directive on money laundering, the Act has implemented several new statutory obligations, for example, on customer identification, reporting and data keeping rules. The most important provisions of the Directive protecting the safety of the financial system refer to customer due diligence and reporting suspicious activity[16]. Implementing Act CXXI of 2001 'on the failure of reporting money laundering related activity', legislators ordered criminalization of the person who fails to report suspected money laundering. Act CXXXVI of 2007 on the prevention and combating money laundering and terrorist financing has implemented the provisions of the Third Council

---

[8] I.L. Gál, *A pénzmosás szabályozásának régi és új irányai a nemzetközi jogban és az Eu-jogban* (The old and new laws on money laundering in international and EU law), Európai Jog, 2007/7., Budapest, pp. 12.

[9] I.L. Gál, *Bejelentés vagy feljelentés? A pénzmosás és a terrorizmus finanszírozása elleni küzdelemmel kapcsolatos feladatok és kötelezettségek az Új Büntető Törvénykönyv alapján* (Tasks and responsibilities for combatting money launderind and terrorist financing under the New Criminal Code), Reproflex Kiadó és Nyomda kft., 2013., Pécs, pp. 5.

[10] I.Carr, M.Goldby, *Recovering the Proceeds of Corruption: UNCAC And Anti-Money Laundering Standards*, Journal of Business Law, Issue 2, 2011, p. 175

[11] I.L. Gál, O. Sinku, *Dinamikus és statikus pénzmosás- egy tényállás kritikai elemzése* (Dynamic and static money laundering- a critical analysis of the bearings of a case), Magyar Jog, 2008/55., Budapest, 130. o.

[12] S.Adamoli, A.Di Nicola, E. U. Savona, P.Zoffi, *Organised Crime around the world*. Helsinki, No. 31., 1998, pp. 23–26

[13] I.L. Gál, *Régi és új kísérletek a gazdasági bűnözés fogalmáénak meghatározására* (Old and new attempts to define the concept of economic crime), Rendészeti Szemle, 2009/7-8., Budapest, pp. 25.

[14] I.L. Gál, *Új Btk. kommentár 8. kötet* (Comentaries on the New Criminal Code Volume 8), 2013., pp. 45

[15] J. Jacsó, *Money laundering*, in F. Kondorosi, K.Ligeti, (Ed.), Handdbook of European Criminal Law, Official Gazaette Publishing, 2008, Budapest, pp. 508.

[16] J. Jacsó, *Bekämpfung der Geldwäscherei in Europa, unter besonderer Berücksichtigung des Geldwäschestrafrechts von Österreich, der Schweiz und Ungarn*, Schriftenreihe Sanktionenrecht in Europa 5. Band (Hrsg.: Dannecker, G., Höpfel, F., Schwarzenegger, Ch.). Neuer Wissenschaftlicher Verlag, Berlin-Wien-Zürich, 2007, pp. 98-113.

Directive, while Act LIII of 2007 has incorporated the Fourth Council Directive to Hungarian law[17]. The Fourth money laundering Directive has included tax offences related to direct and indirect taxation by the national laws of the member states into the definition of the predicate offence, however, the Directive has missed to define tax offence, stating only one requirement, namely, that such offences must be punishable by more than the minimum – one year of – imprisonment[18].

In December 2016, the Council has implemented a proposal of a Directive on countering money laundering. The European Parliament and the Council have not passed the proposal (COM (2016) 826) yet. In accordance with the proposed Directive, it shall improve transnational cooperation and information exchange between the authorities, furthermore, it shall help to prevent criminals to take advantage of the differences in the national legal regulations of the member states. These objectives shall strengthen the legal frames of the European Union responsible for countering money laundering, therefore, combating organised crime and financing terrorism shall become more effective, making EU's inner security, therefore, the security of the EU citizens a growing reality. (COM (2016) 826).

Section 23 of Act IX of 1994 has implemented the statutory provision of money laundering into the previously effective Act IV of 1978 (former Criminal Code or Btk.), into the chapter on economic crimes, under the main title Crimes Violating Economic Obligations and the Order of Economy.

Money laundering has been granted an individual chapter in Act C. of 2012 on the Criminal Code.

According to Section 399:

(1) Any person who, in connection with an asset obtained from any punishable criminal offence committed by others:

a) converts or transfers the asset in question, or performs any financial transaction or receives any financial service in connection with the thing in order to:

aa) conceal or disguise the origin of the asset, or

ab) frustrate the criminal proceedings conducted against the perpetrator of a punishable criminal offence committed by others;

b) conceals or disguises the origin of the asset and any right attached to the asset or any changes in this right, or conceals or suppresses the place where the asset can be found; is guilty of a felony punishable by imprisonment between one to five years.

(2) The penalty under Subsection (1) shall also be imposed upon any person who, in connection with an asset obtained from a punishable criminal offence committed by others:

a) obtains the asset for himself or for a third person;

b) safeguards, handles, uses or consumes the asset, or obtains other financial assets by way of or in exchange for the asset, or by using the consideration received for the asset; if being aware of the true origin of the asset at the time of commission.

(3) The penalty under Subsection (1) shall also be imposed upon any person who, in order to conceal the true origin of an asset that was obtained from a punishable criminal offence committed by others:

a) uses the asset in his business activities;

---

[17] J. Jacsó, *Money laundering*, in Ákos Farkas, (Ed.) *Chapters on the European Criminal Law*, Bíbor Publishing, 2017, Miskolc pp. 132-133.

[18] J. Jacsó, B. Udvarhely, *Actual tendencies of countering money laundering in the European Union*, Prosecutors' Journal, 2017/1, pp. 13-14.

b) performs any financial transaction or receives any financial service in connection with the asset.

(4) The penalty shall be imprisonment between two to eight years if the money laundering specified under Subsections (1)-(3):

a) is committed on a commercial scale;

b) involves a particularly considerable or greater amount of money;

c) is committed by an officer or employee of a financial institution, investment firm, commodities broker, investment fund manager, venture capital fund manager, exchange market, clearing house, central depository, body acting as a central counterparty, insurance company, reinsurance company or independent insurance intermediary, voluntary mutual insurance fund, private pension fund or an institution for occupational retirement provision, an organization engaged in the operation of gambling activities or a regulated real estate investment company;

d) is committed by a public official;

e) is committed by an attorney-at-law.

(5) Any person who collaborates in the commission of money laundering as specified under Subsections (1)-(4) is guilty of misdemeanor punishable by imprisonment not exceeding two years.

Section 400

(1) Any person who, in connection with an asset obtained from a punishable criminal offence committed by others:

a) uses the asset in his business activities;

b) performs any financial transaction or receives any financial service in connection with the asset, and is negligently unaware of the true origin of the asset is guilty of misdemeanor punishable by imprisonment not exceeding two years.

(2) The penalty shall be imprisonment not exceeding three years if the criminal act described in Subsection (1):

a) involves a particularly considerable or greater value;

b) is committed by an officer or employee of a financial institution, investment firm, commodities broker, investment fund manager, venture capital fund manager, exchange market, clearing house, central depository, body acting as a central counterparty, insurance company, reinsurance company or independent insurance intermediary, voluntary mutual insurance fund, private pension fund or an institution for occupational retirement provision, an organization engaged in the operation of gambling activities or a regulated real estate investment company; or

c) is committed by a public official.

(3) Any person who voluntarily reports to the authorities and unveils the circumstances of commission shall not be prosecuted for money laundering as specified under Subsections (1)-(2), provided that the act has not yet been revealed, or it has been revealed only partially.

Protected legal object of the statutory definition of money laundering are society's and community's interests in combating organised crime, furthermore, the public interests related to lawful and prudent operation of financial institutions and other actors of the economy[19].

The statutory definition of the offence is completed upon the execution of any of its elements thereto, whereas successful conduct of money laundering is no further

[19] E. Nyitrai, *Criminal and criminalistics measures of combating organized crime*, PhD study, 2018, Pécs, pp. 71.

requirement. Except for the perpetrator of the predicate offence, any capable person over the age of 14 may be chargeable for money laundering, who did not actually participate in the commission of the predicate offence[20]. Section 399 (3) of the Btk. defines the provisions of laundering own money, whereas any person who, in order to conceal the true origin of an asset that was obtained from a punishable criminal offence committed by others, uses the asset in its business activities, or performs any financial transaction or receives any financial service in connection with the asset.

III. Conclusions

Legalizing illicit money often gives assistance to further criminal acts, nevertheless, the person who, in connection with an asset obtained from criminal activity committed by others, uses the asset for business activities, performs any financial transaction or receives any financial services in connection with the asset, and is negligently unaware of the true origins of the asset, and voluntarily reports to the authorities or initiates such report shall not be liable for prosecution for money laundering, provided that the act has not yet been revealed, or it has only been partially revealed. However, the interest to eliminate money laundering is relevantly stronger than the interest in the accusation of the perpetrator[21].

Regrettably, most criminal acts stay in latency, thus eventual success of fighting money laundering remains one of the most sufficient measures to confine crime[22].

To sum it all up, we may state, that criminal organisations can be fought from different directions, but the most effective measure in this combat is still defecating financial assets, paralysing the organisation and making it non-functional. Laundered money can be safely used in economy, it can easily be transferred into legal businesses. By these means, as a final product, it shall become clean and legitimate money.

The most indispensable measure of effective countering of money laundering is coherent criminal regulation of money laundering, that is able to keep illicit incomes from being channelled into legitimate economy.

References

1. Adamoli, Sabrina, Di Nicola, Andrea, U. Savona, Ernesto, Zoffi, Paola, *Organised Crime around the world*. Helsinki, No. 31., 1998.

2. Berar, Călin, *Facing Organized Crime – between the Need for Security and the Protection of the Human Rights*. Journal of Eeastern-European Criminal Law, 1/2015, Timisoara.

3. Carr, Indira, Goldby, Miriam, *Recovering the Proceeds of Corruption: UNCAC And Anti-Money Laundering Standards*, Journal of Business Law, 2011 issue 2.

[20] I.L. Gál, *Money Laundering*, in M.Tóth, Z. Nagy, (Ed.), *Special Provisions, Hungarian Criminal Law*. Osiris Publishing, 2014, Budapest, pp. 524.

[21] E.Nyitrai, *Money Laundering and Organised Crime*, in Journal of Eastern European Criminal Law No.2/2015., pp. 94-100.

[22] In the course of investigating organised crime – therefore, when countering money laundering as well – numerous new investigating possibilities are available, that were limitedly exploited by the investigating authorities. For example, criminal geography is one of these fields. Regarding the new investigative possibilities offered by criminal geography see more in the studies of Mátyás, Szabolcs, titled Criminal geographic survey of organised crime (2018) and in Mátyás, Szabolcs, The interconnection of traveller crime and organised crime (2018).

4. Gál, István László, Sinku Pál, *Dinamikus és statikus pénzmosás- egy tényállás kritikai elemzése* (Dynamic and static money laundering- a critical analysis of the bearings of a case), Magyar Jog, 2008/55., Budapest.

5. Gál, István László, *Economic Bribery as a Part of Economic Criminal Law and a Concomitant of Political Corruption*, Journal of Eastern European Criminal Law No. 1/2014.

6. Gál, István László, *Money Laundering*, in Tóth, Mihály, Nagy, Zoltán (Ed.), *Special Provisions, Hungarian Criminal Law*. Osiris Publishing, 2014, Budapest.

7. Gál, István László, *A pénzmosás szabályozásának régi és új irányai a nemzetközi jogban és az Eu-jogban* (The old and new laws on money laundering in international and EU law), Európai Jog, 2007/7, Budapest.

8. Gál, István László, *Bejelentés vagy feljelentés? A pénzmosás és a terrorizmus finanszírozása elleni küzdelemmel kapcsolatos feladatok és kötelezettségek az Új Büntető Törvénykönyv alapján* (Tasks and responsibilities for combatting money launderind and terrorist financing under the New Criminal Code), Reproflex Kiadó és Nyomda kft., 2013., Pécs.

9. Gál, István László, *Régi és új kísérletek a gazdasági bűnözés fogalmáénak meghatározására* (Old and new attempts to define the concept of economic crime), Rendészeti Szemle, 2009/7-8., Budapest.

10. Gál, István László, *Új Btk. kommentár 8. kötet* (Comentaries on the New Criminal Code Volume 8), 2013.

11. Jacsó, Judit, Udvarhely, Bence, *Actual tendencies of countering money laundering in the European Union*, Prosecutors' Journal, 2017/1.

12. Jacsó, Judit, *Bekämpfung der Geldwäscherei in Europa, unter besonderer Berücksichtigung des Geldwäschestrafrechts von Österreich,der Schweiz und Ungarn, Schriftenreihe Sanktionenrecht in Europa*. 5. Band (Hrsg.: Dannecker, G., Höpfel, F., Schwarzenegger, Ch.). Neuer Wissenschaftlicher Verlag, Berlin-Wien-Zürich, 2007.

13. Jacsó, Judit, *Money laundering*, in Farkas, Ákos (Ed.), *Chapters on the European Criminal Law*, Bíbor Publishing, 2017, Miskolc.

14. Jacsó, Judit, *Money laundering*, in Kondorosi, F., Ligeti, K. (Eds.), *Handdbook of European Criminal Law*, Official Gazaette Publishing, 2008, Budapest, pp. 508

15. Lamberto, Dini (1994), *General Introductory Report*. International Conference on Preventing and Controlling Money Laundering and the Use of Proceeds of Crime: a Global Approach. Courmayeur Mont Blanc, Aosta Valley (Italy) 18-20 June 1994. Official United Nations document (E/Conf.88/7), ISPAC, 2.

16. Mátyás Szabolcs (2018), *Az utazó bűnözés és szervezett bűnözés kapcsolatrendszere.* In Frigyer László (ed.), *Nemzetközi jellegű szervezett bűnözés nyomozásának kutatása információáramlási szempontból. I.*, Nemzeti közszolgálati Egyetem, Budapest, ISBN: 978-963-498-013-1.

17. Mátyás, Szabolcs (2018), *A szervezett bűnözés kriminálgeográfiai vizsgálata* in Frigyer László (ed): *Nemzetközi jellegű szervezett bűnözés nyomozásának kutatása információáramlási szempontból. I.,* Nemzeti közszolgálati Egyetem, Budapest, ISBN: 978-963-498-013-1.

18. Nyitrai, Endre, *Criminal and criminalistics measures of combating organized crime*, PhD study, 2018, Pécs.

19. Nyitrai, Endre, *Money Laundering and Organised Crime*, Journal of Eastern European Criminal Law No.2/2015.

20. Rankin, Glynn, Kinsella, Nick, *Intelligence Management*, Knowledge Driven Frameworks for Combating Terrorism and Organised Crime (Eds. Babak Akhgar, Simeon Yates) Springer, 2018, London.

21. Ryder, Nicholas, *The Financial Services Authority and money laundering - A game of cat and mouse*, Cambridge Law Journal, 2008, 67(3).

22. Unger, Brigitte, Rawlings, Greg, *Competing for Criminal Money*. Global Business and Economis Review 10, No.3. 3–6, 2008.

23. Ürmösné Simon, Gabriella, *Organised crime*, in Technical English for Officers. Dialóg Campus Publishing, 2018, Budapest.

24. Ürmösné Simon, Gabriella, *Organised crime*, RTF Publishing, 2002, Budapest.

25. Ürmösné Simon, Gabriella, *White collar crime*, RTF publishing, 2002, Budapest

Criminal regulation and criminalistic aspects of money laundering with special focus on the criminal legislation of the Republic of Serbia

Doc. dr Aleksandar R. Ivanović*
Assistant Profesor of Criminal law
Faculty of law sciences, International University of Novi Pazar

Abstract:

The author discusses and analyzes the criminal offense of money laundering in accordance with the legal regulations of the criminal legislation of the Republic of Serbia. The author starts from the first incrimination of this work in the criminal legislation of the Republic of Serbia from 2001, pointing out all the changes that have been made so far in the content of the provisions which prescribed this criminal offense. The author devotes special attention to the interpretation of certain provisions of this criminal offense and to problems related to their practical application. In the second part of the paper, the author points out the basic ways of executing of this criminal offense, taking into account the legal regulation of the criminal offense in the Republic of Serbia. At the end of the paper, the author provides basic guidelines for the effective conduct of criminalistic investigation and criminal investigation of the criminal offense of money laundering.

The aim of the paper is to present in a comprehensive and detailed manner, all the confusions about the interpretation of the legal provisions on criminal legislation of the Republic of Serbia related to the criminal offense money laundering and to offer the answers on the same confusions, as well as to present criminal instructions in order to increase the efficiency of work on the field of countering of money laundering in the Republic of Serbia.

Keywords: *money laundering, criminal law of Republic of Serbia, criminalistics, investigation, prosecution*

I. Introduction

The criminal offence of money laundering from a phenomenological point of view is a special form of economic crime that has recently taken on enormous proportions and at the same time poses a major threat to the economic system of each state. Namely, professional criminals, and especially organized criminal groups, achieve their enormous unlawful property gain by their criminal activity, which is why they face the fact that unlawful property they should be used unhindered, without leaving a trace that could indicate their criminal activity. In order to reduce or completely exclude the risk of seizing unlawfully acquired funds and avoid punishment for the crimes they commit, they resort to the commission of a criminal offense of money laundering (Nicević & Ivanović, 2013).

* E-mail: a.ivanovic@uninp.edu.rs.

The term money laundering means those activities that are directed to the legalization of money that has been acquired through criminal activities. These are such activities that convert money or other property benefits that are acquired through criminal acts or other illegal activities into „clean" money, i.e. money that can be used as a legal income in banking, shopping, sales, investment, forex and other business or ways of investing (Babić, 2008).

Therefore, it is about the material gain that, according to the provisions of positive legislation, should be seized because it was created as a result of criminal activity. The enforcement of the criminal offense of money laundering also conceals the execution of a criminal offense by which has acquired the unlawful material gain, as well as the material gain obtained by the execution of that part. The essence of money laundering is reflected in the fact that the money, that is, the material gain obtained illegally by the criminal offense of tax evasion, trafficking in narcotic drugs, illegal smuggling and trafficking in arms and ammunition or trafficking in human beings, etc., in legal transactions and transactions used unhindered as money, or assets acquired in a legal way. In order to achieve this goal, the „money laundering" procedure is used, that is, the concealment of the existence and origin of illegally acquired funds and their inclusion in legal financial flows. Thus, money laundering is a type of crime, the purpose of which is to conceal the existence and origin of illegally acquired funds, by including these funds through transformation, transfer, exchange, concealment of intentions by interfering with legal means or otherwise into legal financial flows, by which, beside the hiding of illegal origin of assets, conceals criminal activity and achieves the ultimate goal of money laundering – unhindered use of revenues from criminal activity and avoidance of punishment for committed criminal acts (Bošković, 2005). The money was „laundered" that moment when the transaction gets a green light and money come in into financial flows as legal.

The term „money laundering" originated in the United States during the prohibition period (the time of banning the production and sale of alcoholic beverages) in the third decade of the last century, when criminals shown money earned from illicit production and smuggling of alcoholic beverages, as an earnings in the chain of their laundry and car washing facilities. On the occasion of this phenomenon in journalism, the term „money laundering" began to be used, from which it was taken over by criminological and criminal science (Teofilović & Jelačić, 2006).

Incorporating illegally acquired revenues into legal financial flows endangers the economic system and market competition and has an impact on economic, political and social flows on a national and international level. The most common negative effects of money laundering are manifested through: unfair competition with legal entities, reduction of tax revenues due to the movement of money by illegal financial flows, damage to financial institutions, the impact on public confidence in economic and other social institutions, the promotion of corruption and impeding economic development (Bošković, 2009). Money laundering is a phenomenon whose harmful consequences manifest both domestically and internationally. Money laundering as a criminal offense in Serbia appears as one of the most common forms of organized crime, along with drug trafficking, extortion, kidnapping, human trafficking, corruption (Pavlović & Bošković, 2015). Organized opposition to this negative phenomenon implies the existence of legal frameworks for the fight against money laundering, and in Republica Serbia such frameworks were set by the adoption of the Law on the Prevention of Money Laundering. This law criminalizes money laundering for the first time and in some way

establishes the criminal liability of all entities that commit or participate in the execution of unauthorized actions prescribed by such law. An effective system of measures and methods in suppressing money laundering constrains the ability of criminals and criminal organizations to use unlawfully acquired funds, thus destroying the economic barriers of the power of criminal organizations.

II. Criminal offense money laundering in criminal legislation of Republic of Serbia

Thus, in the criminal legislation of the Republic of Serbia, the criminal offense of money laundering was first time systematized as a criminal offense by passing the Law on the Prevention of Money Laundering in 2001 (which entered into force on 1 July 2002)[1]. Article 27 of the aformenthioned law defines the concept of money laundering, ways, procedures, actions and forms of its manifestation. Also, the law contains a number of measures, procedures and the manner of acting of authorized entities in order to detect, prevent and suppress the activities of natural and legal persons related to concealment of illegally acquired money and other property benefits.

According to the provisions of Article 27 of the Law on Prevention of Money Laundering, the criminal offense of money laundering had two basic forms. The first basic form of criminal offense of money laundering is reflected in the deposing of money (cash, foreign currency and other financial assets) acquired through the conduct of illegal activities (gray economy, arms trade, drugs, psychotropic substances, etc.) to accounts with banks or other financial organizations and institutions on the territory of the Federal Republic of Yugoslavia, contrary to the provisions of the law on the prevention of money laundering. The second basic form of this criminal offense consisted in the inclusion in another way of such money into legal financial flows – which domestic and foreign physical and legal persons perform in order to carry out the permitted economic and financial activity, for which offender knew that it was obtained by the criminal offense (Škulić, 2003).

From this way legal description, there were established two forms of the act of committing the criminal offense of money laundering emerged: 1) the deposit of „dirty" money on the account, and 2) the inclusion of „dirty" money in legal financial flows.

This definition of the criminal act of money laundering was not clear enough. Different interpretations of this provision resulted in inadequate application in practice. One of the problems was related to defining the notion of predicate offence[2], as a

[1] Law on the Prevention of Money Laundering („Official Gazette of FRY", no. 53/01).

[2] Pursuant to Article 2, h) United Nations Convention against Transnational Organized Crime, Official Gazette of FRY, International Treaties, no. 6 of 27.06.2001. year, „predicate criminal offense" means any offense whose execution is a gain that may be the subject of a criminal offense as defined in Article 6 of this Convention. Article 6 under the heading „Criminalization of laundering of proceeds of crime" in paragraph 2 of this convention states: For the purpose of applying paragraph 1 of this article: point (a), each State Party shall seek, by applying paragraph 1 of this Article, predicate offenses; paragraph (b), any State Party shall include in the predicate criminal offenses all the grave crimes defined in Article 2 of this Convention (crimes punishable by a maximum sentence of at least four years' imprisonment or some serious punishment) and offenses established in accordance with Articles 5 (punishment of participation in organized crime groups), 8 (punishment of corruption) and 23 (determination of interference with justice as a criminal offense) of this Convention. In the event that the legislation of the Member States provides for a list of specific predicate offenses, they shall, as a minimum, include a wide range of criminal offenses related to organized crime groups".

necessary element for the existence of a criminal offense of money laundering (Nikolić-Rsitanović & Ćopić, 2007). By analyzing the provision of the article law that prescribes this crime, it was noticed those vague terms such as „illegal activities", „gray economy" and „deposing."

There was also a question about what, in the sense of this law, are considered illegal activities. Does this term mean only activities that are considered unlawful under domestic law or wider (according to the provisions of the Strasbourg Convention of 1990[3]). Also, in this context, a question was raised as to whether the illegal activities, in the sense of this law, consider all activities which are contrary to the legal provisions in general or just criminal offenses, which is related to the question of what is considered to be a predicate criminal offense. As far as the term „gray economy" is concerned, it was quite clear that it was not legally defined in our country. And the question here is whether this term is interpreted restrictively or extensively. In addition to the aforementioned, money laundering under the 2001 Law on Prevention of Money Laundering encompassed only the placement of money into accounts with banks or other financial organizations, while the other two phases, namely the concealment stage and the integration phases, were not included. This law contained a very vague and imprecise definition of money laundering. Predicate offenses were also vaguely defined. The concept of a transaction was determined in a restrictive way. Because of all of the above, it was difficult to apply in practice (Marković, 2009).

With the adoption of the new Criminal Code of the Republic of Serbia from 2005[4] (which entered into force on January 1, 2006) the criminal offense of money laundering has been moved from the „secondary" into the basic criminal legislation into the head of criminal offenses against the economy. The criminal act of money laundering is incriminated in the aforementioned code in a different manner in relation to the criminalization in the 2001 Law on the Prevention of Money Laundering. Thus, the Criminal Code of the Republic of Serbia prescribes one basic (paragraph 1), three qualified forms of this criminal offense (paragraphs 2, 3 and 4) and one privileged form (paragraph 5) (Ivanović & Ivanović, 2014).

The legislator in article 231 defines the basic form of criminal offense of money laundering as the execution of a conversion or transfer of property with the knowledge of the perpetrator that this property originates from a criminal offense with the intention of concealing or falsely depicting the unlawful origin of the property or concealing or falsely presenting facts about the property originate from a criminal offense, or acquire, hold or use property with knowledge at the time of receipt of such property that its originate from the criminal offense (Article 231 paragraph 1 of the CC). It is a complex, legal and linguistically complicated and bulky disposition, for which Dragoljub Simonovic In his work titled: „Criminal offenses in Serbian legislation", rightly points out that „it is an example of way how a criminal law norm, and especially a criminal offense, should not be prescribed. Namely, legal and linguistically complicated provisions are difficult to grasp, since they are placed in a single sentence, and because of that are bulky and confusing, which here has be done with this way of prescribing of criminal offence of money laundering" (Simonović, 2010). The same author, in the aforementhioned work also pointing into the existance of a disagreement between the

[3] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, ETS No.141.

[4] Criminal Code of the Republic of Serbia („Official Gazette of the Republic of Serbia, No. 85/2005, 88/2005, 107/2005").

name of the criminal offence and the content of the provision. Namely, the criminal offense is titled as „money laundering" and in the basic form of this criminal offense (paragraph 1) word „money" does not mentioned at all, while word „property" are mentioning even for seven times in the content of provisions of this criminal offence, even the property has broather has a wider meaning then term money (Simonović, 2010). Because of this, most of the domestic theoreticians who deal with problems of money laundering from the criminal legal perspective do not dare to interpret, ie explain the meaning of the legal provision of the basic form of criminal offense of money laundering in their papers or textbooks and even in Comments of Criminal Code.

With the amendments to the Criminal Code of 2016[5], the criminal offense of money laundering with a small change in the content of the provision is now prescribed in the head twenty-two entitled „Criminal offenses against the economy" in Article 245 (Jovašević, 2018). In contrast to the old provision of this criminal offense (former Article 231 of the Criminal Code), which contained expresion: „property originate from a criminal offense" in the current provision (Article 245 of the Criminal Code), stand that it should be that: „property originate from criminal activity". At the same time, it should be noted that this is the only change in relation to the incrimination of this criminal offense under the provision of Criminal Code from 2005. Namely, law maker, in the amendments of 2016, deliberately instead of a precise term (property originate from a criminal offense), used an insufficiently precise term (property originate from criminal activity), which is more criminologycal, rather than criminaly legal term. Earlier use of a more precise term „criminal offense" led to the fact that in the practice it was mainly advocated that a final verdict for a so-called „predicate criminal offese". This led to the unjustified narrowing of the criminalization of money laundering in use (Stojanović, 2017). Using the term „criminal activity" instead of the term „criminal offense", conditions have been created for more efficient application of the provisions of the Criminal Code that prescribe the criminal offense of money laundering, because in practice, it is sufficient, for the needs of the concrete criminal case, to determine that the money or property were acquired by the activity which realisation contains elements of provision of criminal offense, that is, it is not necessary existence of final judgment for this offense.

Based on the aforementioned legal provision, we can conclude that the possible ways of executing the basic form of criminal offense of money laundering are as follows:

– conversion or transfer of assets with the intention of concealing or falsely displaying the unlawful origin of such property;

– concealment or misrepresentation of the facts about the property illegally obtained;

– acquisition, possession or use of illegally acquired property.

Conversion or transfer of assets in order to conceal or fraudulently display the unlawful origin of the property constitutes a performance action which is reflected in the transformation of a non valid legal transaction into a valid legal transaction whit retaining the same or similar economic effects achieved by the original legal transaction (Marković, 2009). Under the term „conversion or transfer of assets" means any action when a conversion is made from one form of property to another. For example, the use of unlawfully acquired cash for the purchase of precious metals or real estate, or the sale of illegally acquired immovable property, as well as the situations in which assets are

[5] Law on Amendments to the Criminal Code („Official Gazette of the Republic of Serbia", No. 94/2016).

transferred from one place to another or from one jurisdiction to another, as well as from one bank account to another (Nicević & Ivanović, 2013). For the existence of this form of criminal offense of money laundering, it is not necessary that the intention is achieved. For this part, an objective requirement of incrimination is prescribed, which is reflected in the fact that the property whose conversion or transfer is carried out must originate from the commission of a criminal activity. It also prescribes the subjective requirement of incrimination that is reflected in the fact that the perpetrator of the work has the knowledge that the property whose conversion or transfer is performs, originates from the criminal activity, as well as a direct intent, which is reflected in the intent to conceal or falsely display an unlawful origin property (Ivanović & Ivanović, 2014).

The concealment or misrepresentation of the facts of the property that is illegally obtained is reflected in the restraint or false presentation of facts regarding the property that is illegally obtained. Undercover means the activity by which other persons try to create a belief that it is not about the property that originates from the criminal activity, but about the legally acquired property (Babić, 2008). In this case, the perpetrator does not make a conversion, that is, the transfer of illegally acquired property already conceals or falsely presents facts indicating that the property is acquired by the commission of an offense. This is done by fabricating counterfeit documentation that fictitiously shows that it is a legally acquired property. As with the previous form it is necessary that the subjective condition is fulfilled, which is reflected in the fact that the perpetrator of the work has the knowledge that this property originates from the criminal activity?

Acquisition, possession or use of property, with knowledge, at the time of receipt, that property arises from criminal activity, is reflected in the acquisition of property that arises from criminal activity in any way, the exercise of a state, that is, factual authority over illegally acquired property or its use, ie. disposing of the said property in any way. Under acquisition, it is necessary to understand any activity by which acquires assets acquired through the commission of a criminal offense. Therefore, for the existence of the criminal offense of money laundering, is not important what kind of activity is in the question, but it is only important that by this activity realizing the possession of property that originates from the commission of the criminal activity. In this regard, the acquisition of property arising from the commission of a criminal activity can be accomplished by purchase, by swap, by receiving a gift, by confiscation, and the like. For the existence of a work, it is important that when acquiring the work of the perpetrator, there is knowledge at the moment of receipt of that property from the criminal activity. The methods of committing the criminal offense were alternatively given and each act in this sense represents the way of executing the basic form of criminal offense of money laundering. The criminal offense of money laundering is consider finished by executing some of the by criminal law prescribed alternative actions (or more simultaneously). For existence of the criminal offense there is no need for determination the occurrence of a certain negative consequence, since it is not even envisaged in the law. This is because money laundering belongs to the category of so called „formal" criminal offenses, or offense by doing (commision). In addition to the act of commision, the criminal offense of money laundering in relation to certain actions can also be carried out by omission. Namely, although this work is legally defined as an act of doing, it is possible to achieve it by omission, in the form of a failure to act (Article 15, paragraph 2 of the CC). The prepetrator of this offense by omission can only be a person who is located in a obligatiory position to do something. Namely, according to the provisions of the Law on the Prevention of

Money Laundering and Financing of Terrorism (about it will be more words in further part of this papaer) if during the performance of certain tasks, the lawyer carries out actions and measures for the prevention and detection of money laundering, when it helps in the realization of the sale of immovable property for the party (Articles 5 and 46 LPMLFT). If it establishes that, in relation to the person or transaction, there is a suspicion of money laundering, he is required to notify the Administration for the Prevention of Money Laundering (Article 48 LPMLFT). Therefore, the lawyer is a guarantor that the money supply agreement will not be carried out with the sales contract he makes for the client. If, however, a lawyer forms such a contract, knowing for the intention of the buyer that the purchase of real estate conceals the fact that the money for the payment of the price originates from the criminal activity, he may be responsible for money laundering as a co-perpetrator (Đorđević, 2016). The object of the execution of the basic form of the criminal offense of money laundering is the property for which the offender knows that it has been obtained by the criminal activity. Therefore, an important element of the basic form of criminal offense of money laundering is knowledge of the fact that the money is obtained by a criminal activity, and it is irrelevant whether the existence of that criminal activity (criminal offense) has been determined by a court decision. In the absence of this element, it will not be about the existence of the basic abundance of the criminal offense of money laundering, but about the privileged form envisaged in paragraph 5 of Article 245 of the Criminal Code of the Republic of Serbia.

The perpetrator of this from of criminal offense money laundering can be any person, except for the responsible person in the legal entity (because in the case of this category of perpetrator it will be form of criminal offense prescribed in paragraph 6 of Article 245 of the Criminal Code of the Republic of Serbia will be dealt with). From the point of view of guilty, there needs to be premeditation that must include the knowledge of the fact that the money originated from the crime, that is, the so-called „dirty money". For this form of work cumulatively, a prison sentence of six months to five years is envisaged and a fine.

Paragraph 2 gives a qualified form of this criminal offense, which exists when the amount of money or property that is the subject of the criminal offense exceeds the amount of one million and five hundred thousand dinars. For this form of criminal offense, a cumulative sentence of one to ten years in prison and a fine (Article 245 paragraph 2 of the CC) is envisaged.

Paragraph 3 foresees the special form of this criminal offense that exists when someone commit the basic (paragraph 1) and the first qualified form (paragraph 2) of the criminal offense of money laundering with the property he himself obtained by committing the crime. The perpetrator of this form of criminal offense of money laundering shall be punished by a fine prescribed for the basic and first qualified form and fine (Article 245 paragraph 3 of the CC).

Paragraph 4 provides for a second qualified form that exists when the basic form of the offense and the first qualified form are committed in the group. For this form of criminal offense, a cumulative sentence of imprisonment of two years to twelve years is envisaged and a fine (Article 245 paragraph 4 of the CC). It is a collective criminal offense of money laundering. Therefore, this form of work will exist when it is collectively, i.e. by at least three or more organizational connected persons, the operation of the basic form and the first qualified form of criminal offense of money laundering has been performed. Persons who commit this crime can be organized on various ways, with different roles of

individuals in the group. It is only important that there is their joint action in the commission of this criminal offense.

In paragraph 5, the legislator prescribes a privileged form of this criminal offense, when the perpetrator of the basic and first-qualified form of money laundering was not aware of the origin of the money or property, and he may have been obliged to know that the money or property constitutes the proceeds of the crime. It is about sanctioning unconscious negligence as a way of committing the crime of money laundering. For this form of criminal offense, a prison sentence of up to three years is prescribed (Article 245 paragraph 5 of the CC).

Paragraph 6 defines the responsibility of the responsible person in the legal entity that makes the basic form and the first qualified form of criminal offense. With regard to the guilty of the perpetrator, premeditation and unconscious negligence is sought, if he knew, or could and should have been aware that the money or property constituted the proceeds of the criminal activity (Article 245, paragraph 6 of the CC).

Paragraph 7 prescribes the obligation to apply the security measure of seizing money and assets that are the subject of the act of committing the criminal offense of money laundering.

In addition to the provisions of Article 245 of the Criminal Code[6], money laundering is also regulated in the positive criminal law of the Republic of Serbia by the Law on the Prevention of Money Laundering and Financing of Terrorism. The Law on the Prevention of Money Laundering and Financing of Terrorism[7] was adopted in 2009 in the Republic of Serbia as one of the steps towards harmonizing domestic legislation with the international legislation and guidelines of the European Union, in order to meet the requirements that the Republic of Serbia as a candidate for EU membership should fulfill in order to became a full member.

According to the current Law on Prevention of Money Laundering and Financing of Terrorism[8] (Article 4), entities that are obliged to apply this Law are: banks; authorized exchangers, economic operators who perform exchange transactions on the basis of a special law regulating their activity of the investment fund management company; voluntary pension fund management companies; financial leasing; insurance companies, insurance brokerage companies, insurance advisors and insurance agents, who have a license to perform life insurance activities, with the exception of representation firms and insurance agents, the work of which is the responsibility of the insurance company in accordance with the law; broker-dealer companies; organizers of special games of chance in toys and organizers of games of chance through means of electronic communication; audit company and independent auditors, e-money institutions; payment institutions; brokers in real estate and real estate leasing; factoring society; entrepreneurs and legal entities engaged in the provision of accounting services; tax advisers; a public postal operator based in the Republic of Serbia, established in accordance with the law regulating postal services, engaged in the provision of services for the purchase, sale or transfer of virtual currencies or the replacement of such

---

[6] Criminal Code of the Republic of Serbia („Official Gazette of the Republic of Serbia", No. 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108 / 2014 and 94/2016).

[7] Law on Prevention of Money Laundering and Financing of Terrorism („Official Gazette of the Republic of Serbia", no. 20/2009 and 72/2009").

[8] Law on Prevention of Money Laundering and Financing of Terrorism („Official Gazette of the Republic of Serbia", No. 113/2017).

currencies for money or other assets through an internet platform, physical devices or otherwise, or who intervene in the provision of these services. To apply this Law is also obliged to lawyers when: 1) they assist in the planning or execution of transactions for a party in relation to: the purchase or sale of a real estate or a company; asset management; opening or disposing of the account with a bank (bank account, savings deposit or securities account); by collecting the funds necessary for founding, performing activities and managing companies; establishment, operation or management of a company or entity of foreign law; 2) carry out a financial transaction or a real estate transaction on behalf of and for the account of the client.The notaries are also obligated to apply this Law in accordance with the special provisions of this Law. The applicable Law on the Prevention of Money Laundering and Financing of Terrorism in Article 2 defines the concept of money laundering. Thus, the following details are considered as money laundering: a) conversion or transfer of property acquired through the commission of a criminal offense, b) concealment or misrepresentation of the true nature, origin, location of the movement, movement, disposal, ownership or rights in relation to property acquired through the commission of a criminal offense and c) acquiring, holding or using property acquired through the commission of a criminal offense. In addition, Article 3 provides the definition and content of terms that are incorporated into the criminal offense of Money Laundering. Thus, according to these legal solutions, the object of execution on the criminal offense of money laundering is defined as: a) assets – things, money, rights, securities and other documents in any form, which can determine the property right and other rights, b) money – cash (domestic and foreign), funds on accounts (dinars and foreign exchange) and electronic money, and v) physically transferable means of payment – currency, checks, bills and other physically transferable means of payment, payable to the bearer. As acts of committing a criminal offense of money laundering, this Law explicitly specified: a) a transaction – the receipt, giving, substituting, keeping, disposing or other treatment of property with the taxpayer, b) cash transaction – physical acceptance or cash withdrawal, and v) cash funds – any transaction that is carried out electronically by at least part of the payment service provider on behalf of the payer, with the aim of making such funds available to the payee of the payment service provider, regardless of whether the payer or the payee kid paying the same person and are payer provider of payment services and the provider of payment services of the recipient to pay the same person. In order to prevent and disclose committed, tried or planned criminal offenses of money laundering, the Law in Article 5 foresaw a number of preventive actions and measures that are taken before, during and after the transaction or establishing a business relationship. These actions and measures include the following activities: 1) knowledge of the client and monitoring of its business; 2) provision of information, data and documentation to the Administration for the Prevention of Money Laundering, 3) appointment of the authorized person in charge of fulfilling obligations from the law and his deputy, as well as providing conditions for their work, 4) regular vocational education, training and training of employees, 5) ensuring regular internal control of the performance of obligations under this law, as well as internal audits, if this is in accordance with the scope and nature of the business of the obligor 6) creating a list of indicators (indicators) for identifying persons and transactions for which there are grounds for suspecting money laundering, 7) keeping records, protecting and storing data from those records, 8) implementing measures under this law in business units and subordinated companies of a legal person in the majority ownership of taxpayers in

foreign countries; and 9) the execution of other actions and measures pursuant to this Law. In carrying out preventive activities in the fight against various forms and forms of manifestation of the criminal offense of money laundering, the role of the Administration for the Prevention of Money Laundering is emphasized, in addition to the Tax Administration, the Customs Administration and regular criminal justice bodies (police, public prosecution and courts of general and special jurisdiction). The Administration for the Prevention of Money Laundering (Article 72) is formed as an administrative body within the ministry responsible for finance. It performs financial information activities such as: collecting, processing, analyzing and forwarding to the competent authorities information, data and documentation obtained in the exercise of its competencies and performing other activities related to the prevention and detection of money laundering.

III. Methodology of commiting of criminal offense money laundering

Money laundering is a process by which criminals try to conceal the true origin and ownership of assets acquired through criminal activities. Consequently, money laundering involves many different techniques that are commonly complex, imaginative and secretive. It is common for them to hide the original origin and ownership of the money, and that the criminals want to keep the control over the procedure itself and, if necessary, to make some changes within the procedure (Šikman, 2011). Money laundering is a complex system of criminal activities that is constantly evolving, and in which new methods and techniques of money laundering are constantly applied, and the money launderers themselves are increasingly improving techniques in realization of this type of criminal manifestation. Criminals hide behind complicated transactions involving international transfers, shrinking the transaction to smaller amounts or transferring to accounts of a larger number of people, changing the form of money, and in doing so, they also use advice from top bank experts, brokers, investment bankers, accountants, consulting firms, notaryes and lawyers. The money laundering process never stops: no matter how many phases of laundering „dirty" money has gone through, and how many forms of illicit assets have changed, such funds will never be „clean" in the eyes of the law (Bejatović, 2009). In accordance with the above-mentioned, modern forms of money laundering, it is characterized by:

– Continuous improvement of money laundering through the application of new sophisticated techniques and methods;

– Greater investment of funds derived from narcotics, terrorism and other illegal activities in legal affairs with the aim of increasing the amount of funds and masking the flow of the money in question;

– The instrumentation of the money laundering network, in which more and more countries and financial centers were imported;

– Intentional mixing of legal and illegal funds with the aim of obstruction the entry of audit or of official investigative authorities in the trace of illegal origin of the money;

– Increased money laundering activity among traders in actions that deal with illegal funds. After the passage of such funds through such a financial flow, such funds are no longer related to their initial illegal activities (Šaković, 2002).

The perpetrators of criminal offense of money laundering, so-called „money launderers" have elaborated a number of seemingly simple techniques by which trying

to fraud the legislation and financial controls of countries in which they want to legalize dirty money. Therefore, there are no easy recipes for the fight against money laundering in the first place because each case is special and a story for itself within legal financial and criminal transactions. Relying on the experience in the prevention and suppression of the criminal offense of money laundering, we think that special attention in countering this type of criminal manifestation must be focused on the following fields, ie activities: the real estate transaction; life insurance; gambling; gifts and inheritances, loans from abroad, as well as fictitious payments to other countries through fictitious invoices for non-existent goods or services.

Unlawful means mostly go through three basic channels. A relatively small portion of the illegal amount of funds is immediately reinvested into illegal actions and maintenance and jobs. Most of the funds are invested in sectors that have „lenient entrance membranes" with high profit margins and a high degree of competence (construction, agriculture, retail and the like), while most of the funds are usually in cash carrying out in abroad. For international money laundering, the perpetrators of this crime, for reasons of safety and efficiency, recruit financial experts with a task to perform their jobs based on the existence of differences in financial regulations and banking legislation. Therefore, funds moving through the first channel have no contacts with legal funds because they are used to expand legal affairs, while other funds that move through the other two channels launder through legal financial institutions (Šaković, 2002).

The money laundering procedure takes place in three phases:

a) the placement phase (depositing, or laying);

b) the phase of concealment (transformation, or stratification);

c) the integration phase.

The placement phase (placement) implies the physical placement of financial assets acquired through criminal activity, that is, cash, whose criminal origin the money launderers try to conceal, into the financial system of a country. Placement can be done in many ways, depending on the circumstances of the situation, or the available possibilities. In practice, two situations in which this phase is realized are possible. The first, in which „dirty money" is placed or deposited in the country in which it was acquired by the criminal activity, and the other in which it is carried out in another country. And in one and the other situation, the same activity is done, whereas in a different situation, that is, in a situation when money is deposited in the financial system of another state, the physical cash of criminal origin is first transported across the state border to a country where money laundering, and then transported (smuggled money) into the financial system of that country. The cash that is acquired by the criminal is physically transported to another country in one of the following two ways (Nicević & Ivanović, 2013):

– physical smuggling (transferring over the customs line avoiding customs control measures) into a country where tax laws are more liberal, so-called. countries of financial paradise;

– depositing cash in parallel banking systems (this is done by the one who makes money laundering deposits as a deposit with some of the „underground banks" (which do not provide a transaction report) and receives a certificate which is then presented to a similar banker in another country and from it receives the cash, minus the commission fee.

Money, which is physically transferred to another country, then deposits into the financial system of that country. It should be noted here that, in addition to physically

entering a „dirty money" into one country, a situation of direct inclusion into the financial system of another country is possible through bank orders or electronic money transfer. In this situation, by the transfer itself, the deposit is opened, ie the deposit of „dirty money" in the financial system of that country, i.e. It is about the same mode of operation as in the situation when „dirty money" is placed in the financial system of the country in which it was acquired by criminal activity.

Depositing „dirty money" into the financial system of a country is carried out in such a way that the cash obtained from criminal activities is mainly paid to bank accounts, usually under the pretext of some regular activity. Namely, most often deposits are claimed under the pretext of a false business where payment is mostly done in cash, such as garages, luxury boutiques, galleries, commissions, pizzerias, restaurants, antique shops, etc. (Teofilović & Radović, 2006).

The most effective system for placing dirty money is where cash obtained by criminal activites interacts with incomes acheived through legal business, because this reduces the possibility of quickly detecting „dirty" money. Payment of financial assets acquired through criminal activity to bank accounts is mainly done in the following ways:

– paying „dirty money" with excuse that it is a regular cash operating income;

– the establishment of false or phantom companies, the so-called „phantoms" that do not actually do business, but exist only as a paravane for payments, or the deposit of cash that has been acquired by criminal activities into accounts in banks, on the pretext that these are proceeds from their legal business;

– by breaking large amounts of „dirty money" on the more small amounts and placing them in financial system by more people, on several occasions, on several different bank accounts in sums, that is, amounts that are too small or below the legal censuses, which is why they are not suspicious to bank workers. It is a method of placing „dirty money" through the structuring of financial transactions, which is mainly applied in countries where financial regulations require banks to report all transactions above a certain amount. Money launderers therefore conduct a series of transactions in a number of banks in order to keep the amount of deposited „dirty money" below the limit, that is, the amount that is lower than the one that must be declared by law, and the cash is subsequently transferred to the central account (Šikman, 2003);

– conversion of „dirty money" into market instruments of payment, which is reflected in the purchase of checks, bills of exchange, guarantees, bonds and the like. from financial institutions. This method is also carried out through a large number of couriers, which makes this activity less visible to the judiciary and police authorities. It is a technique that is also referred to as „smurfing" in criminal jargon;

– by taking loans. It is a method that is reflected in the fact that „dirty money" is mainly in the so-called „ a financial paradise is deposited in a bank, then goes to another country in which a loan is sought from a bank, offering as a guarantee of money deposited with a bank in another country. The loan obtained is then used for investing in various jobs, and the origin of the money is justified by the loan, or by the debt to the bank on the basis of the borrowed loan;

– By purchasing capital with a bunch of cash is a method of depositing money that is reflected in the purchase of objects (cars, ships, artwork, gold and precious stones, etc.) and real estate of higher value, mainly in countries that do not raise the issue of the origin of money, the so-called offshore centers. Buying capital is used as a mortgage to borrow from banks and other financial institutions. The money so obtained is then used as in the previous case;

– through other commercial activities, such as gambling. This method of placing „dirty money" is reflected in the fact that the money launderer comes to the cash casino, which comes from criminal activity, for cash at the casino cash box, he buys chips, then plays several games, after which the rest of the tokens are returned to the cashier and requires payment by on the basis of the tokens that have been awarded, and the resulting money or check is shown as a gain that is generated from gambling.

In countries where the process of privatization of social property is in progress, there is also a practice of buying socially owned enterprises that are in serious financial problems, and then the accounts of these companies are used as so-called. „water heater" accounts, on which merging all the money deposited at the accounts with different financial institutions.

The phase of concealment (transformation, ie layering, laundering) is an activity that is reflected in the separation of the assets obtained by crime from their illegal source by creating layers of transactions designed to conceal and give the appearance of legitimacy (Šikman, 2003). Namely, when cash („dirty money") has entered into legal financial flows, or converted into a bank deposit, the stage in which the illicit origin of funds is changed (disguising the illegal revenue from their illegal sources) is followed. The layering is done in such a way that a series of financial transactions are carried out, which, according to their scope, content and complexity, resemble legal financial transactions. The phase of concealment is reflected in a series of transactions that involve moving it from one account to the accounts of various banks, business entities and other financial institutions in one or more countries. Such transactions are aimed at making it difficult or impossible for anybody who tries to investigate the true origin of money and succeed in doing so. The transformation of money or goods is done in many ways. Therefore, this phase represents a continuation of the previous deposit phase, ie, laying down, and it is sometimes difficult to make a distinction between these two phases, since it is about applying more or less similar methods. Namely, when the dirty money is converted into a bank deposit, or it is found on an account, everything is done according to the applicable legal regulations, in order to conceal its criminal origin. It purchases insurance policies, givin lends, buying expensive goods, real estate, shares, foreign exchange and other financial instruments. For the realization of these activities, usualy using banks and savings banks, investment funds, payment service organizations, privatization organizations, insurance institutions, stock exchanges, gambling organizations, securities trading organizations, exchange offices, organizations for employment, various legal or natural persons performing activities related to the sale and collection of receivables by issuing cash and credit cards, organizing travel, real estate transactions, precious metals, etc. (Šaković, 2002).

The integration phase represents the final stage in the money laundering process, which is reflected in the further placement of funds acquired through crime, whose illegal origin was previously concealed or hidened. At this stage, illegal and unlawfully acquired assets are transformed into forms that are difficult to detect and monitor because they are mixing with legally acquired and lawful means. The integration of money is most often seen in the purchase of movable and immovable property and securities by lending, the involvement of several foreign banks, the issuance of false import-export invoices, spending on luxury goods, and in recent times by investing a large amount of money into the revitalized enterprises that are located in big financial problems. It is noteworthy that the methods underlying this phase are identical to the methods by which the phase of concealment or transformation is realized. A logical

question arises, what is the difference between these two phases? The difference is reflected in the goal for which they are being undertaken. In the phase of transformation, the goal is to hide the traces of its true origin, that is, to conceal the links between dirty money and the criminal activity it originates from, while the goal of integration is to insert money that has been illegally originally concealed in legal affairs, for the purpose of its uninterrupted using as legally acquired property.

Further investing „dirty money" into legal financial flows in the third phase of money laundering represents tending to continue with the realization of criminal activity by making money that is acquired through criminal activity legally investing in legally permitted activities. The essence of the integration phase, and in general of the entire money laundering process, is best be shown by one of the famous sentence relating money laundering: „That the dream of every money launderer is to pay taxes". Namely, unlike rest of economic criminals who want to realize unlawful property gain by avoiding paying taxes for the activity they legally perform, money launderers are just trying to pay income tax that has been earned by illegal activity. The question arises as to why the payment of taxes by money launderers is so important when it is actually a loss for them. Namely, the payment of the tax on money acquired through criminal activity means a confirmation to the money launderers that the procedure has been successfully implemented, that is, in the financial system of a country, that money is treated as a legitimate (Ivanović & Ivanović, 2014).

IV. Instead of conclusion

The disclosure of money laundering is primarily related to the specificities of methods of money laundering, which indirectly affect the possibility of coming to the knowledge that in concrete situations there are elements of beings of this criminal offense. These particularities are first of all reflected in the following facts:

– the disposal of „dirty money" is conditioned by prior criminal activity;

– to achieve their goals criminals approach the realization of money laundering using different methods for money laundering and a combination of them;

– that the basic and usual money laundering scheme can be definitely defined in three phases known under the names: placement, concealment and integration;

– that the process of acquiring unlawful profits, its legalization can be divided into two phases: the first one that represents the essence of criminal activity, which acquires unlawful material gain and the other that illegally legalizes against legally acquired property.

These specificities must be taken into account primarily by the memebers of state autorities which dealing with fight against money laundering, or the investigating entities of the disclosure, if they want to achieve higher degree of efficiency in detecting the criminal offense of money laundering is desired. Successful detection of the criminal offense of money laundering implies continuous monitoring of the manner of committing the crime as well as an adequate analysis of the already discovered crimes. It is precisely in this way that an initial indicative basis for the detection of certain money laundering methods is opened, which should serve as a real basis for the adequate planning of operational criminal activity that is conducted through operational criminal control and processing. In any case, the detection of this crime should not only involve members of the internal affairs bodies, but it should be the work of all bodies involved in the prevention of illegal money flows. Considering the significance of the

issue, ie the problem, the same is also dealt with by the Administration for the Prevention of Money Laundering, as a body at the state administration level that studies the methods of execution and the possibility of money laundering and proposes, or informs the disclosure authorities about them. To the information about the criminal offense of money laundering has been most often provide by the operational activities of the interior ministry employees, however, the is possibility of finding information about the committed criminal offense through legal entities (banks, financial institutions, etc.), individuals, anonymous and pseudonymous applications and public discussions, and through media. Money laundering as a form of criminal manifestation is quite specific and difficult to detect because its conspiracy methodology of committing the crime, and money launderers tend to remain undetected, or tend to perform the so-called „jump into the dark". This is reflected in the conspiratorial preparation, execution and enjoyment of success, so that the police and the criminal justice authorities are often asked to disclose, clarify and sometimes adjudicate for criminal offenses solely on the basis of indications and / or indicative chains. Given that the first phase of money laundering is mainly reflected in the conversion of „dirty money" into bank deposits, we can conclude that bank employees are in a position to spot indications that indicate that the money laundering process is ongoing. Namely, employees of the bank, based on an internal procedure, notice indications that indicate the involvement of certain persons in money laundering and transactions that are suspected of being related to money laundering. In the observation of these indications, the employees in the bank should rely on the principles of knowing the client and his business, to take into account the economic and legal logic of transactions, to price the facts concerning the status and income of the client, and in particular the economic and political sensitivity of the region in which client operates. For the practical work of the bank employees in order to timely detect the criminal offense of money laundering, the most interesting are the indications that appear more often and on the basis of which real versions can be set, ie the assumptions about money laundering and persons who are possible money launderers. These are the following indications: attempts by clients to prove their identity in a different way, not by showing out a prescribed personal identification document, nervousness, impatience and rush during the transaction, opening an account in several branches of one and the same bank, opening an account outside their place of residence where a bank it already has a branch office, motives indications, ungrounded wealth, disproportionate spending of money, frequent travel abroad for no apparent reason and other indications that indicate the money laundering and the perpetrator of these criminal activities. Consequently, special attention should be paid to establishing close cooperation with banks and other financial institutions in the field of obtaining the basis for suspicion that criminal offense of Money Laundering is committed.

Also, in operative work, with the application of appropriate operational tactical measures and actions, there may be evidence that is related to the commission of the criminal offense of money laundering, but often also occurs in a special way during the criminal investigation for other criminal offenses that is most often conditioned and conditioning execution of this other criminal offense.

In proces of detecting and investigating criminal offense of money laundering all essential elements related to the criminal offense of money laundering are clarifying and determining, which is a condition for the successful completion of the criminal investigation. Within the framework of the indication of the method of clarifying and proving the criminal offense, an operational activity should be developed which should enable the collection of facts and data to clarify the following issues:

– whether in the specific case it is a criminal offense of money laundering, i.e. whether money or other property has been previously acquired by criminal activity;

– what kind of criminal activity is committed in the concrete case, ie. which criminal offense is committed for acquiring money or assets that are the subject of money laundering;

– the way of committing the crime, and fact whether the perpetrator was aware of the fact that money and other assets originate from criminal activity;

– whether the money so obtained has been deposited into accounts or included in legal financial flows;

– whether it is ilegal money or property and what is the value;

– place, time and method of money laundering;

– whether is money laundering committed by single perpetrator or is a crime committed by several persons who are doing that as an co-perpetrators or accomplices;

– whether it is a group of criminals that is organized in purpose of money laundering;

– whether it is a person who has previously committed a criminal offense, and later deals with money laundering or whether it is a matter ofanother person, and what kind of the guiltiness is in question.

For all this, it is necessary to provide valid both material and personal evidence. In addition to unlawful property gain that may be in different forms of material evidence, it is important to find documentation related to certain transactions that allows us to track financial flows. In order to monitor the financial flows and money traces, it is necessary to restore operational activity backwards and to use various documents, such as currency exchange receipts, postal orders for payment, certificates of possession of safes, brokerage certificates, various correspondence, and the like. The bank documents including electronic documents relating to invoices on accounts, credit cards about loans, suspicious transactions, and the like, should be finded and seized. Records relating to vehicle ownership, cadastral data, enterprise privatization, etc. These records may in many cases contain both indicative and evidence-based evidence of exceptional significance for directing both operational control and operational processing, and in that sense, and evidence of a criminal offense. Therefore, in the plan of operational activities, measures aimed at finding the mentioned documentation should also be planned. Namely, the money laundering procedure is followed by appropriate documentation, so it is necessary to take measures to find the same and to temporarily seize it with the issued certificate, which will most often be achieved by carrying out criminal investigation actions, insight into certain business documentation and searches. The extracted documentation is subject to adequate forensic expertise, thus creating the possibility for providing material evidence in relation to the criminal offense of money laundering and its perpetrator.

During the application of the indicative method in clarifying and proving the criminal offense of money laundering, it is proper to focus attention on persons who can be known facts relevant to both the work and the perpetrator. From these persons, information should be collected by conducting a conversation and creating conditions for them to be heard as witnesses during the conduct of criminal proceedings. In each individual case, both material and personal evidence should be sought to ensure that the combination of material and personal evidence is a formula for success. The necessary condition for the successful completion of criminal processing is certainly cooperation with financial and other institutions with strong team work.

References

1. Babić, M., (2008) Criminal law – general and special part [*Krivično pravo – opšti i posebni dio*], Law faculty, Banja Luka.

2. Bejatović, M., (2009) Money laundering as a criminal phenomenon of modern times [*Pranje novca kao kriminogeni fenomen modernog doba*], Conference proceeding: Corruption and Money Laundering, International Association of Criminalistics, Sarajevo.

3. Bošković, G. Dimitrašinović, S., (2009) The relationship of organized crime, corruption and money laundering [*Odnos organizovanog kriminala, kroupcije i pranja novca*], Conference proceeding: Corruption and Money Laundering, International Association of Criminalistics, Sarajevo.

4. Bošković,G., (2005) Money laundering [*Pranje novca*], Beosing, Belgrade.

5. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, ETS No.141.

6. Criminal Code of the Republic of Serbia („Official Gazette of the Republic of Serbia", No. 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108 / 2014 and 94/2016).

7. Criminal Code of the Republic of Serbia („Official Gazette of the Republic of Serbia, No. 85/2005, 88/2005, 107/2005").

8. Dođrević, M., (2016) Money laundering in Serbian criminal law [*Pranje novca u srpskom krivičnom pravu*], Crimen, 2016, vol. 7, no 2, Belgrade.

9. Ivanović, R. A., Ivanović, A., (2014) Money laundering and accounting sector in the Republic of Serbia [*Pranje novca i sektor računovodstva u Republici Srbiji*], Conference proceedings: IV International Scientific Conference „From the Crisis toward Development", University of Business Studies, Banja Luka, 2014, pp. 683-696.

10. Jovašević, D., (2018) Money laundering in international and criminal law of Serbia [*Pranje novca u međunarodnom i krivičnom pravu Srbije*], Proceedings of the Law Faculty in Nis, vol. 57, iss. 80, Nis.

11. Law on Amendments to the Criminal Code („Official Gazette of the Republic of Serbia", No. 94/2016).

12. Law on Prevention of Money Laundering and Financing of Terrorism („Official Gazette of the Republic of Serbia „, no. 20/2009 and 72/2009").

13. Law on Prevention of Money Laundering and Financing of Terrorism („Official Gazette of the Republic of Serbia", No. 113/2017).

14. Marković, M., (2009) Money laundering in the criminal legislation of the Republic of Serbia and comparative legislations [*Pranje novca u krivičnom zakonodavstvu Republike Srbije i uporednim zakonodavstvima*], Conference proceeding: Corruption and Money Laundering, International Association of Criminalistics, Sarajevo.

15. Nicević, M., Ivanović, R. A., (2012) Organized economic crime as a factor of endangering economic security [*Organizovani privredni kriminalitet kao faktor ugrožavanja ekonomske bezbednosti*], Ekonomski izazovi, International University of Novi Pazar, vol. 1, iss. 1, Novi Pazar, 2012, Novi Pazar.

16. Nicević, M., Ivanović, R. A., (2013) Economic crimes [*Privredni kriminalitet*], University of Novi Pazar.

17. Nikolić-Ristanović, V., Ćopić S., (2007) Developing of legislation on money laundering in Serbia and compliance with international standards [*Razvoj zakonodavstva o pranju novca u Srbiji i usklađenost sa međunarodnim normama*], Conference proceedings „Criminal in Transition: Phenomenology, Prevention and State Reaction", Institute for Criminological and Sociological Research, Belgrade.

18. Pavlović, Z., Bošković, A., (2015) Place of the crime of money laundering within the criminal law of Serbia, Journal of eastern-european criminal law, No. 2/2015.

19. Šaković, A., (2002) Economic Criminalistics – Methods of Prevention and Investigation Economic Crime [*Ekonomska kriminalistika – Metodika sprečavanja i istraživana ekonomskog kriminaliteta*], Magirstrat, Sarajevo.

20. Šikman, M., (2011) Organized crime [*Organizovani kriminal*], Higher school of internal Affairs, Banja Luka.

21. Simonović, D., (2010) Criminal offenses in Serbian legislation [Krivična dela u sprskoj legislativi], Službeni glasnik, Belgrade.

22. Škulić, M., (2003) Organized crime – concept, forms, criminal offenses and criminal proceedings *[Organizovani kriminalitet – pojam, pojavni oblici, krivična dela i krivični postupak]*, Službeni glasnik, Belgrade.

23. Stojanović, Z., (2017) Commentary on the Criminal Code [*Komentar krivičnog zakonika*], Službeni glasnik, Beograd.

24. Teofilović, N. Radović, N., (2006) Money laundering as a criminal activity [*Pranje novca kao kriminalna delatnost*], Perjanik: Journal of Theory and Practice in the Field of Police, Security, Criminal Justice and Law, vol. 4, issue. 11, Police academy, Danilovgrad.

25. Teofilović, N., Jelačić, M., (2006) Preventing, detecting and proving criminal acts of corruption and money laundering [*Sprečavanje, otkrivanje i dokazivanje krivičnih dela korupcije i pranja novca*], Police academy, Beograd.

On an internet service provider's content management obligation and criminal liability*

PhD TU Longke**

Abstract

The online content management is one of ISP's obligations of internet safety management. The ISP is not obliged to initiatively review and supervise the online content, but it shall perform the proactive obligations of report and deletion afterwards. Different ISPs' content management obligations and criminal liabilities are distinguished on basis of different types of content provided by ISPs. The Direct Control Theory shall be adopted to determine whether an ISP has the content management obligation and assumes criminal liability so as to reasonably delimit the scope of criminal liability and avoid the uncertainty and expanse of the subject of criminal liability.

***Keywords**: Internet Service Provider (ISP), Content Management Obligation, Criminal Liability*

I. Introduction

At present, cyber illegalities and crimes are rampant with unceasingly-spread violent, terrorist and sexual information, frequently-found online gamble and fraud, and personal information protection existing in name only. In current situation of huge number, extensive hazards and low cost of cyber illegalities and crimes and being hard to investigate and punish them, it becomes a common choice of criminal policy worldwide to curb cybercrimes, protect internet safety and regulate internet order from the perspective of regulating ISPs who enjoy technological advantages and controlling position. However, due to insufficient elaboration of theoretical foundation of criminal punishment, unclear delimitation of boundary of liability, vague standards for determining liability, there always are unceasing theoretical debates and indecisive judgments along with every nation's efforts in imposing criminal liability on ISPs. In China, some influential cases such as QvodPlayer case and deep linking case arouse attention of the whole society. The struggled performance of prosecutors in trial, the unclear elaboration in judgments of courts, divergent theoretical explanations in academia and the public's burning satire and freezing irony towards the criminal involvement constitute the practical scenery of imposing criminal liability upon ISPs in current China. The judicial embarrassment reflects the tenuity of the theoretical establishment and serious insufficiency of the connectivity between theory and practice, which influences the realization of aim of legislations on internet order governance and national strategy on internet safety, even fundamentally erodes the authority of criminal justice and hinders the whole process of modern legal construction.

---

* This paper is sponsored by the Innovative Project of Criminal Science of Law of Shanghai Academy of Social Sciences.

** Professor of Institute of Law of Shanghai Academy of Social Sciences, PhD in Law, a visiting scholar of School of Law of Oklahoma City University.

E-mail:tulongke1981@126.com.

The newly-adopted Amendment IX to Criminal Law of China creates a new mode of ISP's[1] criminal liability, that is to say, an ISP who fails to perform its obligation of internet safety management, thus resulting in hazardous consequences such as causing illegal information widespread, will face criminal punishment. The scope of internet safety management obligations is extensive, one of which is the online content management obligation aiming at prevention of illegal information from spreading on the internet. Currently, the criminal law scholars' research into the ISP's content management obligation and criminal liability in China is insufficient. There is a need to deeply analyse several issues such as whether it is necessary to reasonably delimit the scope of the content management obligation, whether it is all online content providers or certain online content providers have the obligation of content management and assume criminal liability accordingly, what differences there are in conditions for assuming criminal liability for different ISPs.

II. One Precondition for Criminal Liability: The Scope of Online Content Management Obligation

The ISP's online content management obligation may be classified into three types according to the time when there occurs illegal information: the first one is the obligation to pre-review online content; the second one is the obligation to real-timely monitor online content; the third one is the obligation to report and delete illegal information after it appears on the internet. Regarding whether an ISP's obligation to manage the content generated by the third party on the online platform offered by itself is a precondition for the ISP to assume criminal liability for the consequence of wide spread of illegal information, there are a lot of disputes abroad and they have not been settled yet. The positive argument states that the risk of bringing about illegal or right-infringing information is a natural side-product of internet service, so the principle of a responsible enterprise requires the ISP to regard the loss arising from such risk as a kind of business operation cost. This will force the internet servicer to prevent illegal information from occurrence and allocate the loss arising from such risk among the group of internet users[2]. In addition, the internet servicer enjoys ownership over devices storing, manufacturing and transmitting illegal information and the servicer's control over the ownership is sufficient for the service to be responsible for the emergence and transmission of illegal information on the internet[3]. The negative argument states that firstly, the internet servicer is not responsible for its user's behaviour. The internet service does not necessarily result in the emergency of illegal or criminal behaviour. Secondly, the expanse of ISP's responsibility will possibly make it have strong motive to delete users' materials from the internet for protecting its economic interests even though there is no illegal information. Thirdly, this kind of indifferent review system contradicts the regulation on freedom of speech in the

[1] Although the Criminal Law of China doesn't clearly state the connotation and types of ISP, after research into criminal legislation of China the author find that an online content provider generating or uploading content online does not belong to the ISP because there is another route for criminally investigating and prosecuting the former. Therefore, in this paper, unless otherwise stated, an ISP does not include an online content provider.

[2] Alfred C. Yen (2000). *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, The Georgetown Law Journal, 88, 4.

[3] Alfred C. Yen, cited, p. 38-45.

Constitutional Law[4]. Finally, it needs a lot of human resources to review such huge documents and information uploaded to the internet, so the addition of such obligation will lead to failure to get access to the internet[5]. Although the debate is fervent and long-lasting, in view of the balance among citizens' freedom of speech, internet technology development and protection of the victim's rights, it is commonly believed that an ISP shall undertake online content management obligation within reasonable scope.

The key issue is how to delimit the reasonable scope of online content management obligation of an ISP. The legal practices in foreign countries mostly deny the ISP's obligation to pre-review and real-timely monitor the content expressed by others on the internet. In 2011, the Court of Justice of the European Union decided in the influential *case of Scarlet v. SABAM*[6] that internet service providers have no general obligation to filter or monitor illegal information transmitted online and made clear that any competent authority shall not require the ISP to install the contested filtering system. The reasons are as follows: at the time of imposing obligations on an ISP, regard shall paid to the balance against the protection of the fundamental rights of individuals and the protection of the freedom of the ISP concerned to conduct its business. On one hand, the requirement for an ISP to install the contested filtering system would result in a serious infringement of the freedom of the ISP concerned to conduct its business; on the other hand, it is unnecessarily complicated or costly from the cost-benefit perspective[7]. Based on these reasons, the Court of Justice of the European Union denied the ISP's obligation to review the content. In the USA, there is no legislation specially clarifying whether the ISP has general review and monitoring obligation. It is commonly believed that the legislative intention of the Parliament is obvious that ISP has no obligation to monitor the content expressed by any third party in its website[8]. In the specialized legislation field, the principle of the copyright owner assuming responsibility to search infringement of copyright and inform service providers set forth in the Digital Millennium Copyright Act releases the ISP from the monitoring obligation[9]. The next issue is whether an ISP has the management obligation to report or delete the illegal information that has appeared. It is generally believed that ISP has no general management obligation unless specially otherwise stated. In the precedents such as Zeran v. America Online, Inc[10] Doe v. MySpace[11] and other classic cases, ISPs uniformly cited Section 230[12] to claim immunity from responsibility. This is a non-responsibility clause in the Communications Decency Act (CDA) provides immunity from liability for

---

[4] Alfred C. Yen, cited, p. 33-37.

[5] Lawrence G. Walters (2012), *Shooting the Messenger: An Analysis of Theories of Criminal Liability Used Against Adult- Themed Online Service Providers*, in Stanford Law and Policy Review, 171, 10.

[6]Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs SCRL（EU: Case C-70/10 Celex No. 610CC0070）.

[7] *Case of Scarlet v. SABAM,* Court of Justice of the European Union, Judgment of the Court (Third Chamber), 24 November 2011, In Case C‑70/10.

[8] See *case Stoner v. eBay*, Inc., No. 30566, 2000 WL 1705637, at *3 (Cal. Sup. Ct., Nov. 1, 2000) („[M]any of these products may be contraband, and however many it might be possible for defendant to identify as such, Congress intended to remove any legal obligation of interactive computer service providers to attempt to identify or monitor the sale of such products."); 141 Cong. Rec. H8468-69 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

[9] See Robert A. Gorman, Jane C. Ginsburg, 2006. *Copyright: Cases and Materials,* 7th ed., Foundation Press.

[10]Case *Zeran v. America Online*, Inc., 129 F.3d 327 (4th Cir. 1997).

[11] *Case Doe v. MySpace*, Inc., 528 F.3d 413 (5th Cir. 2008).

[12] 47 U.S.C. §230

those servicerswho provide visiting access to information generated by any third party or users, thus essentially denying ISPs' content management obligation. However, in circumstances where the law specially states otherwise, for example in the case of intellectual property infringement, upon the valid notification by the property owner, the ISP shall fulfill its management obligation. For example, in the attention-arousing and disputable Digital Economy Act of UK, in case of Online infringement of copyright, an internet service provider must provide a copyright owner with a copyright infringement list for a period if the owner requests the list for that period and an initial obligations code requires the internet service provider to provide it. if necessary, an ISP shall adopt technical measures to limit some or all relevant users' internet access for preventing or reducing copyright infringement through internet[13].

There were doubts about the ISP's content management obligation in China in the course of drafting and deliberating the Amendment IX to Criminal Law. The main reasons were as follows: It's hard to define the ISP's content management obligation; An ISP hasn't enough time and resources to tell whether relevant information is illegal or not; The imposition of obligation to review appendixes may hinder the development of internet science and technology[14]. Investigating substantive laws, we find that Article 5 of Decision of the Standing Committee of People's Congress of PRC on Strengthening Internet Information Protection sets forth that ISPs shall strengthen the management of information published by their users, promptly stop transmitting information prohibited by a law or regulation from publishing or transmission if any being found, take countermeasures such as deletion, keep relevant records and send a report to the competent authority. The dominant view in China denies the ISP's content review obligation by citing this article with the reason that the precondition for an unit providing internet service to assume such obligation is any illegal information „being found", which obviously does not impose the obligation to proactively „find out"illegalities and hazardous information on such unit, but means that the unit shall undertake corresponding responsibility when someone tell it or there is proof showing that the unit is aware of the existence of relevant illegalities and hazardous information[15]. The ISP generally assumes no statutory obligation to proactively review or monitor information uploaded or transmitted by any third party, but passively delete or report it afterwards. However, there is also another understanding on this issue. Some courts hold that the ISP, compared with the copyright owner, is more able to control and reduce such infringement, so from the perspective of the balance between rights and obligations, abilities and responsibilities, it is fairer to impose the obligation of strictly reviewing the content transmitted by internet users upon the service provider[16].

This paper holds that it is not suitable to impose pre-review and real-time monitoring obligation upon the ISP because such imposition would inevitably result in too heavy burden on the ISP, harm the freedom of the ISP concerned to conduct its business and narrow its development space. With social development changing rapidly and new things emerging in an endless stream, the legal obligation will definitely often evolve and is updated. The scope of „illegal information" is so extensive, including various types of information violating a law or regulation such as violating an administrative law

---

[13] Digital Economy Act 2010.

[14] Zhou Guangquan, The Scope of Criminal Liability of Internet Servicers, 2 China Law Review (2015).

[15] Civil Judgment (2011) Z.L.M.Z.Z. No. 40 issued by Zhejiang Province Lishui City Intermediate People's Court.

[16] Civil Judgement (2006) Y.G.F.M.S.Z.Z. No. 355 issued by Guangdong Province Higher People's Court.

or regulation and infringing other's civil rights, that the ISP will bear too heavy legal burden, being difficult to advance. The unceasing change of legal obligation would make the ISP not know what course to take. Even more, the criminal punishment like the Sword of Damocles overhead makes the ISP be in a constant state of anxiety, thus definitely limiting the healthy development of internet technology and internet service industry tremendously. Therefore, it's not suitable for the ISP to assume the pre-review and concurrent monitoring obligation but only the ex post reporting and deleting obligation. Moreover, the ISP's reporting and deleting obligation is passive, which means that the ISP has no obligation to proactively review or monitor the internet content. Such obligation is just a general obligation imposed on the ISP, that is to say, in a field where there is no special legal provision, the ISP assumes no special management obligation.

To clarify the scope of the ISP's internet management obligation is a precondition of determining the ISP's criminal liability. For example, according to Amendment IX to Criminal Law, one of conditions for prosecuting the ISP is its failure to make correction after a supervisory authority orders it to take corrective measures. Then, does a supervisory authority has the power to give ISP an abstract order about corrective measure such as „illegal information is not allowed to appear next time", „please carry out real-time monitor over illegal internet information and delete it upon its emergence"? This paper gives a negative answer. The reason is that such abstract order about correct measure essentially requires the ISP to monitor the internet content at all times, thus practically transferring the review and monitoring obligation originally not assumed by the ISP to the ISP and increasing the ISP's legal obligation without legal foundation. A supervisory authority can only ask the ISP to delete illegal information such as violent or terrorist information or sexual photos which have appeared on its website. The scope of „correction requirement" shall be based on the following two points: the first one is that the corrective measure must be a specific and targeted requirement of deleting or preventing some type of illegal information. The second one is the corrective measure is targeted at practical and objectively existing illegal information rather than future and possibly emerging illegal information. The ISP will not take any criminal liability for failure to implement or complete such kind of correction required by a supervisory authority.

III. Foundation for Criminal Liability: Establishment of Online Content Management Obligation Based on Classification of Internet Services

The internet service, in broad sense, includes all types of service constituting and guaranteeing the normal operation of the internet, with extensive content and various types. The ISPs include those who utilize public tele-communication infrastructure to connect service node with internet backbone and then provide basic hardware service of internet access such as China Telecom and China Mobile, those who provide internet end-users with broadband installation, internet test and reparation and other services such as network technology companies in the market, and internet cache providers by means of WEB cache re-direction technology, as well as platform providers who are internet servicers creating internet space for content providers to publish information, for example the commonly-seen operators of BBS, microblog and other internet space. When a platform itself publishes information, it is also the content provider. In addition, the ISPs also include those who provide users with services such as online payment and

recharge, and providers of software engaging in one or more activities of transmission, receipt and representation.

In the internet information system, due to different service provided, each ISP enjoys different status in the internet system, ability of controlling information, likeliness of preventing illegal or criminal behaviors. Where the internet service content provided is different, the provider may face different legal obligation and punishment. For example, a pure internet content provider would not assume liability for the loss of data stored on the internet and an internet hardware access provider generally assumes no liability for illegal information emerging in the internet space. Therefore, it is a common practice all over the world to classify service providers according to their different service content provided and then set forth their respective criminal liability accordingly rather than impose a uniform criminal liability. For example, the Digital Millennium Copyright Act of USA[17] (hereinafter referred to as DMCA) classifies internet servicers into (1) those providing transitory digital network communications[18]; (2) those providing system caching service[19]; (3) those providing information residing on systems or networks at direction of users[20]; (4) those providing information location tools[21], and the Communications Decency Act defines the meaning of information content providers and accordingly sets forth their respective legal liabilities and constituents[22]. The Telecommunication and Media Act of Germany distinguishes service providers' functions and thus classifies internet servicers into content providers, access providers, caching providers and trusteeship providers[23], and establishes a liability system with different levels for different internet service providers. Where the internet service content provided is different, the provider's legal responsibility is different and the type of legal sanctions varies. In a situation where the law sets forth the criminal liability, the legal obligation of different service providers and the condition for constituting a crime due to failure to fulfil the aforesaid obligation are different.

From the criminal legislation practices in China, it is found that the legislator is not apt to adopt the mode of classifying the service content for distinguishing different ISPs' internet content management obligations and corresponding scopes of criminal liabilities and conditions for incrimination. Amendment IX to Criminal Law establishes a special rule of criminal punishment for the ISP's behaviour of failing to perform its legal obligation and creates a new mode of criminal lability of the ISP. The provision on the ISP's behaviour of failing to perform its safety management obligation sets forth three specific circumstances such as „resulting in wide spread of illegal information" besides the miscellaneous paragraph. In fact, in such three circumstances, not all legal obligations have the same source and different ISPs are involved. For example, „the wide spread of illegal information" is generally due to the platform provider' failure to perform its content management obligation of a website or information interactive communication platform, so the criminal liability shall not be imposed on operators providing internet hardware access service or caching service providers. As for „leakage of users' information resulting in serious consequences", the ISP providing information

[17] Digital Millennium Copyright Act.

[18] Above 20, 512(a).

[19] Above 20, 512(b).

[20] Above 20, 512(c).

[21] Above 20, 512(d).

[22] 47 U.S.C. §230(f).(3) (2006).

[23] Dieter Dörr, Steffen Janich（2011. *The Criminal Responsibility of Internet Service Providers in Germany*. *Mississippi Law Journal*, 80, 1247-1261.

storage generally assumes the criminal liability and other service providers have nothing to do with this. The responsible subject for „resulting in the loss of evidence of a criminal case and having serious circumstance" can only be the ISP providing data storage and having the obligation to store evidence. However, in practice, the smooth running of a network depends on normal operation of all components. Any behaviour of the ISP cannot be separated from other service providers' technological and equipment support. For example, in the circumstance of „resulting in the wide spread of illegal information", undoubtedly the first one who should assume the liability is the platform provider, but objectively the perpetrator cannot commit or complete its offence without the internet access service or access software service. The criminal liability cannot be extended without limitation to the ISPs in the interlocking internet service supply chain. At this point, there are some questions to answer: (1) Which type of ISPs is the competent subject of criminal liability? Where is the boundary of criminal liability? (2) Are legal obligations of and criminal constituents for different ISPs totally the same? At the level of criminal law, the legislation of China does not give clear clarification of ISPs nor define different ISPs' special legal obligations and corresponding criminal liabilities, so the consequence is that the scope of imposing criminal liability is not clear and the responsible subject is vague. The legislation may call all servicers providing various kinds of internet service as ISPs due to legislative technique, but during the application of judicial interpretation, it is unsuitable to vaguely and undistinguishably impose criminal liability on different ISPs, the criminal liability of which shall be judged on basis of the service content provided. The aim of classifying internet services is to define a certain ISP's role and status in the transmission, deletion or control of illegal information by specifying the difference among services provided by different ISPs, which is the precondition for judging whether the ISP has the internet content management obligation or assumes criminal liability or not.

IV. The Standard for Determining Criminal Liability: The Theory of Direct Control

The next question after solving the issue of classification of internet services is which approach and standard shall be adopted for determining different ISPs' content management obligations and subsequent criminal liabilities. For this, there are generally two directions in the academia. The first one is based on the traditional theory of joint offence and realizes the purpose of preventing the imposition of criminal liability on ISPs from expanding by limiting the radiative scope of the theory of joint offence. It's a common practice in both Civil Law and Case Law countries to hold the ISP criminally responsible as an accomplice. Till now, the USA also brings the ISP to criminal justice for imposing the accessorial liability according to the theory of joint offence. The famous case of BuffNET[24] opened a gate to prosecuting the ISP on the ground that the ISP provides electronic means or opportunity for the third party's criminal behaviour and thus „promote" or „assist or help" the illegal activity. The prosecutor may cite Title 18 of the U.S. Code to charge a website operator with criminal activities[25]. Prior to the adoption of Amendment IX to Criminal Law, the mode of the ISP's criminal liability in

[24] *Case People of the State of New York v. Buffnet.* 272 A.D.2d 982. 708 N.Y.S.2d 227, 2000 N.Y. Slip Op. 04475.

[25] Shahrzad T. Radbod, cited, p. 613.

China is similar to that in the U.S.A. In practice, it is the judicial interpretation states that the ISP assumes accessorial liability for its assistance in a cybercrime. For example, Article 7 of Interpretation of Several Issues concerning Legal Application in Criminal Cases of Making, Copying, Publishing, Selling or Transmitting Obscene Electronic Information by Use of Internet, Mobile Communication Terminal or information service center promulgated by the Supreme People's Court and the Supreme People's Prosecutor in 2004 and Article 6 of Interpretation (II) of Several Issues concerning Legal Application in Criminal Cases of Making, Copying, Publishing, Selling or Transmitting Obscene Electronic Information by Use of Internet, Mobile Communication Terminal or information service center promulgated by the Supreme People's Court and the Supreme People's Prosecutor in 2010impose criminal punish on ISPs for their crime-assisting behaviours such as internet access, server hosting, network storage space and communication transmitting channel. The Amendment IX to Criminal Law incorporates similar provisions scattered in many judicial interpretations and upgrades the level of such provisions through legislation. Meanwhile, it protects legal interests in advance and makes a crime-assisting behaviour become a principal offence. In essence, such legislation is not separated from the framework of existing criminal law theories or does not impose new legal obligation upon the ISP. However, in fact, the traditional theory of joint offence in China is insufficient to punish and govern ISPs because it cannot provide theoretical basis of justification in criminal regulation of ISPs' behaviours nor reasonably limit the combating scope. Therefore, the theories in China move towards different directions. Some scholars introduced the theory of neutral assisting-behaviour from Germany and Japan, trying to limit the scope of the ISP' criminal liability. Mr. Chen Hongbing introduced the analytic tool of the theory of neutral assisting-behaviour on basis of drawing on cases in Japan and Taiwan of China in the earlier time and holds that it's not suitable to punish the ISP as an accomplice if the assistance is neutral and does not create law-forbidding danger[26]. Around the adoption of Amendment IX to Criminal Law, Mr. Zhou Guangquan and Mr. Che Hao, according to such theory, reflected the reasonability of using criminal punishment as a means to punish and control behaviours providing IT support and hold that an apparently legal daily behaviours cannot be criminally punished just because the actor knows to some extent in individual situations that others may utilize those behaviours to commit a crime. The loss may outweigh the gain in terms of protecting legal stability and forming the legal order if the scope of an accomplice is excessively expanded[27]. On the whole, the theory of neutral assisting-behaviour derived from the framework of the traditional theory of joint offence holds the stance of restraining or limiting the participation and intervention of criminal law when judging ISPs.

In fact, the theory of neutral assisting-behaviour has obvious deficiencies in limiting or defining the ISP's criminal liability. Firstly, regarding the theory of neutral assisting-behaviour, there are many controversial opinions about the definition of a neutral behaviour and the standard of each opinion is very vague, thus receiving doubts about the operability. Secondly, in cyber space, it is impossible for the theory of neutral assisting-behaviour to distinguish different ISPs, hard to connect with the criminal liability system based on the classification of services, unable to realize the purpose of

[26] Chen Hongbing, *Research into the Punishability of Neutral Behaviors on the Internet: Centered on the Judgment of P2P Service Providers' Behaviors*, 3 Journal of Northeastern University: Social Sciences Edition (2009).

[27] Zhou Guangquan, *The Scope of Criminal Liability of Internet Servicers*, 2 China Law Review (2015).

limiting the scope of imposition of criminal liability. In a word, either the traditional theory of joint offence or the theory of neutral assisting-behaviour enjoys limited capability to explain the issue of ISP's criminal liability.

The second direction is to introduce other theories to explain and analyse the ISP's criminal liability. After the adoption of Amendment IX to Criminal Law, there emerged various views such as the Theory of Guarantor[28] and the Theory of Supervisory Negligence[29] when discussing the theoretic foundation for the ISP's criminal liability, and no agreement is reached. When the ISP refuses to perform its management obligation after being informed by a competent authority, the subjective state of mind is obviously not negligent, so the view of supervisory negligence is not accurate. Comparatively, „the Theory of Guarantor" could better solve issues of brining the ISP to criminal justice and limiting its criminal liability. Especially after the Amendment IX to Criminal Law imposes criminal liability on the ISP for its refusal to perform internet safety management obligation, it is particularly necessary to reasonably adopt the Theory of Guarantor to explain the ISP's criminal liability. According to the view of the Theory of Guarantor, whether the actor has the obligation to act depends on whether the actor enjoys the status of a guarantor. Only when the actor is the person enjoying the status of a guarantor and is able to perform the guaranty obligation, but fails to perform it resulting in hazardous consequence, is there omission equivalent to an act[30]. The huge advantage of the Theory of Guarantor is the matching and connectivity between the ISP's status of a guarantor, the ability to perform special guaranty obligation and the ISP's status and role in managing and controlling internet information, thus reasonably delimiting the scope of the ISP's criminal liability on basis of classification of internet services. That is to say, the ISP's objective capability to get access to and control information determines the existence and the size of the ISP's obligation to monitor or delete illegal information and whether an offence of omission is formed[31]. Therefore, this paper holds that the standard for determining the existence of the ISP's obligation of managing internet illegalities and crimes and the ISP's criminal liability is such service provider's direct control over illegal and criminal information. Such standard contains the following several meanings: Firstly, the ISP has control over illegal and criminal information and decides whether certain illegal or criminal information can be transmitted through certain channels and within certain scope. The service provider is not responsible for safety management regarding illegal and criminal information beyond its influence and control. Secondly, the ISP's control over illegal and criminal information is direct. The term of „direct" may be understood from two aspects: (1) If an ISP has the capability to control over illegal and criminal information and such control is not direct but needs help or intermediation of other ISPs, the former ISP's management obligation in terms of criminal law and criminal liability shall be denied. (2) In the chain of information transmission and dissemination, the ISP is only responsible for the illegal information of the first link and level under its direct control. The purpose of the standard of direct control is to limit the scope of imposition of criminal liability and

[28] According to the Theory on Guarantor, both the Crime of Assisting Implementation of Online Criminal Activities and the Crime of Refusing to Perform Internet Safety Management Obligation can be understood as offences of omission and accomplice.

[29] Lu Xu, *On the ISP's Criminal Liability and Related Issues*, 6 Research on Rule of Law (2015).

[30] Gong Houjun, *On the Evolution of the Theory on Guarantor and Its Enlightenment*, 4 Studies in Law and Business (2007).

[31] Yang Caixia, *New View on Omission Cybercrimes*, 2 Seeker (2007).

prevent the criminal liability from expanding even unlimited imposition along with the causal chain. Thirdly, the standard of direct control cannot be violated unless major social public interest is involved and such situations must be statutory and have clear basis in legislation.

V. Miscellaneous Issues Related to Determining the Criminal Liability

As for objectively hazardous consequence of the wide spread of illegal information, not all ISPs shall undertake the same criminal liability. The ISPs shall be distinguished according to different types of services they provided and their criminal liabilities shall be analysed specifically. The content generators are unexceptionally responsible for the content published in the cyber space whether it is on their own computers or on other severs. In addition, according to the general rule, the content providers assume the full responsibility regardless of the fact whether they have the right of copy or use[32]. The punishing rules all over the world are basically the same with differences that some countries punish the content provider by regarding it as one of ISPs, while some countries independently enact criminal rules other than those on the ISPs. Except for the content provider, other service providers assume different criminal liabilities on basis of different content management obligations. The specific analysis is as follows:

(I) Criminal Liability of the Internet Platform Provider

The criminal liability of the internet platform provider, different from that complete and unexceptional criminal liability of the content provider, is limited and conditional. The platform service provider assumes no criminal liability for the content generated by others, but shall be criminally responsible for failure to perform subsequent obligations after being given effective notice. However, under certain circumstances, the platform provider may have its identity changed due to participation in generating the internet content and thus assume the criminal liability of the content provider.

The precondition for the ISP being immune from civil and criminal liabilities is that the illegal internet information is uploaded by a third party but generated by the platform provider itself. Then, does the fact that the content is uploaded by a third party ensure the internet platform provider's immunity? The judicial practice has the tendency to hold the stance of strict interpretation and limited scope. It is generally believed in the judicial practice of China that the ISP shall be regarded as a content provider and assume corresponding legal liabilities if it edits or amend information uploaded by others or change the receivers[33]. Other countries such as Germany adopt the similarly same stance. The U.S.A. adopts a stricter mode for limiting the application of the ISP's immunity when the ISP participates in generating the internet content. In the famous case of Roommates.com[34], the court excluded the application of Section 230 on the ground that users are required to complete a questionnaire including users' gender, sexual orientation and other personal information. The court held in this case that the website actually served as an information and content provider[35]. Therefore, the ISP's

[32] Koch, CR 1997, 193 (197); Spindler, NJW 1997, 3193 (3196); Pelz, ZUM 98, 530(532).

[33] Judgment (2011) Z.L.M.Z.Z. No. 40 issued by Zhejiang Province Lishui City Intermediate People's Court.

[34] Roommates.com, LLC, 521 F.3d 1157, 1161 (9th Cir. 2008) (en banc).

[35] Roommates.com, LLC, 521 F.3d 1164 (9th Cir. 2008) (en banc).

participation in generating the content may result in its identity shift towards a provider and the content management obligation. Under such type of situations, the internet platform provider shall assume corresponding criminal liability as an internet content publisher or provider.

Shall an internet platform assume the criminal liability of the content provider if the platform does not directly provide information but presents links to illegal information? In Germany, there are a lot of controversies over this issue. Generally, the link is only regarded as an intermediary for getting access to external content. However, case differences shall be considered. If a platform explicitly expresses its approval of the linked content, such external content provided by others may be regarded as provided by the platform itself. Meanwhile, when making such decision, the quantity of the linked content and data shall be taken into account. If a platform generally and massively cites others' data or documents, the content provided by others cannot be regarded as provided by the platformed. If those who setting the link accept (external) content as their own content, they will be punished for an assisting behaviour. However, if there is a further link in the cited website, the criminal liability shall not be extended to the link of the second tier[36]. It is obvious that Germany holds a relatively looser stance in the platform service provider's identity shift. This paper agrees on that the platform provider shall not assume responsibility for the content generated in the link of the second tier or above because the service provider has no direct control any more. However, the platform provider participation in generating the content is not a behaviour simply guiding user's access but a real transmission[37], so excessively loose standard of legal application isn't beneficial to the effective control of illegal information. More importantly, when a platform provider participates in generating the content, it has complete autonomy and control in choosing to provide or not to provide relevant links without restriction. In addition, such choice may not increase any extra business cost of a platform provider. From the perspective of balance of interest, it is not unsuitable to hold the platform provider responsible for this. Therefore, the platform provider shall undertake the duty of care for its behaviour of providing the first-tier link, know the linked content and assume corresponding criminal liability because the intermediary for assess is provided by the platform.

(II) The Software Assess Provider's Criminal Liability

A software assess provider refers to a software provider engaging in one or more activities such as transmission, receipt, exhibition, forwarding, search[38]. The attention-focused QvodPlayer case is a suitable example for discussing this issue. The prosecutor argued that the QvodPlayer provides internet videos publishing, searching, downloading and playing services on basis of streaming media technology and by means of publishing free installation program of QVOD media server and QvodPlayer player software in international internet. The prosecutor considered that the QvodPlayer company and persons in direct charge, knowing that users use installation program of QVOD media server and QvodPlayer player software for obscene videos, let them alone and result in

[36] Flechsig & Gabel, CR 1998, 351 (356); Lhnig, JR 1997, 496 (498); Park, GA 2001, 23 (32); Gehrke, ZUM 2001, 34 (39); Spindler, MMR 2002, 495 (503); SIEBER, supra note 14, at pt. 308. Contra Lackner& Kahl, pt. 7b.

[37] Yu, Zhigang, *The Criminal Law Theory in Virtual Space*, China Fangzheng Press (2003), 185.

[38] 47 U.S.C. §230(f). (4) (2006).

wide spread of mass obscene videos on the internet[39]. In this case, the prosecutor's train of thought is that the QvodPlayer company and the persons in direct charge are accomplices of the crime of the dissemination of obscene materials for a profit[40]. Some scholars question the necessity and reasonableness of criminally punishing such type of behaviours of QvodPlayerwhich apparently seems neutral and harmless but objectively helpful to the criminal, and hold that it should be prudent to punish neutral assisting-behaviours, the scope of which criminally punished shall be limited as far as possible[41].

The issue discussed herein is whether a provider of assess software such as QvodPlayer shall assume criminal liability of an ISP for the wide spread of illegal information under the framework of Amendment IX to Criminal Law. This paper holds the negative view on the ground that roles and statuses of assess software in internet service system are not the same. After an access software is published, the provider loses control over users' using behaviours and modes of use. The use of the software by users is independently from the software provider, so the software provider shall not assume criminal liability for users' behaviours. However, it's a different case for the internet platform. Because the internet platform is always under the control and dominance of the platform provider and the platform provider has special obligation to manage the content in the platform, the platform provider shall assume corresponding criminal liability when requirements are satisfied. In fact, an access software provider and an internet hardware access provider enjoy the similar roles and statuses, both objectively acting as one of conditions for disseminating illegal information. Not all ISPs providing information dissemination conditions but those directly controlling illegal and criminal information shall be included in the scope of criminal liability, otherwise all parties related to internet service even computer producers and sellers are possibly punished criminally. This is obviously ridiculous.

(III) Criminal Liabilities of Other ISPs such as Internet Hardware Assess and Cache Providers

Generally, the internet hardware access and cache provider will not be held criminally responsible for the use of its access and cache service by uses. However, the hardware and cache service provider's immunity from criminal liability is not absolute. For example, Item 2 of Paragraph 1 of Section 8 of Telecommunication and Media Act of Germany states that the privilege (immunity from criminal liability) is not applicable if the service provider intentionally collaborates with served users to commit illegal activities. Such collaboration is not necessarily between a provider and an user, but it can be between providers who act as joint offenders[42]. There is a similar provision in China. Article 7 of Interpretation of Several Issues concerning Legal Application in Criminal Cases of Making, Copying, Publishing, Selling or Transmitting Obscene Electronic Information by Use of Internet, Mobile Communication Terminal or

---

[39] Gao Jian, *Haiding District Court Accepting the QvodPlayer Case Involving Pornographic Materials*, Beijing Daily, Feb. 11, 2015.

[40] There are also some scholars considering that in such circumstance, the actor shall be regarded as the principal offender of the crime of dissemination of obscene materials for a profit, i.e. an accomplice becoming a principal.

[41] Che Hao, *Who Shall Be Responsible for the Consequence of Neutral Behaviors in the Internet Age*, 1 China Law Review (2015).

[42] Theodor Leckner et. al. § 184 pt. 58, in Adolph Schonke, Horst Schroder, *Kommentar zum Strafghesetzbuch* (2006).

information service center promulgated by the Supreme People's Court and the Supreme People's Prosecutor in 2004 sets forth that the actor, knowing that another person commits an offence of manufacturing, coping, publishing, selling or disseminating obscene electronic information, provide assistance such as internet access, server hosting, network storage space and communication transmitting channel and expense settlement, is regarded as a joint offender. It should be noted that the aforesaid „knowing" is specific and targeted and shall not be abstract, that is to say, the access service provider has the intention to commit a crime jointly with another person (collaboration). As everyone knows that the existence of illegal information in cyber space, the access and cache service provider could not have been unaware of such internet access service will objectively result in the dissemination of illegal information. If the „knowing" is required to be abstract rather than specific, any internet access and cache service will definitely constitute a crime. This is obviously not what we hope.

In the context of Amendment IX to Criminal Law, the internet hardware access and cache service provider shall be criminally responsible for the wide spread of illegal information arising from its failure to implement an internet supervisory authority's order and refusal to make correction. However, it should be noted that due to the specialness of internet access service, the scope of access service is more extensive than the platform service and the social influence is huger, involving many interested parties, an order issued by a supervisory authority shall be strictly limited. This paper holds that only there is a risk of spreading information constituting serious crimes such as endangering national safety or public safety, can a supervisory authority issue an order to ask the hardware access service provider take measures. In addition, it is formally limited to the clear expression in a law.

References

1. Caixia, Yang, *New View on Omission Cybercrimes*, 2 Seeker (2007).

2. *Case Doe v. MySpace*, Inc., 528 F.3d 413 (5th Cir. 2008).

3. *Case of Scarlet v. SABAM,* Court of Justice of the European Union, Judgment of the Court (Third Chamber), 24 November 2011, In Case C70/10.

4. *Case People of the State of New York v. Buffnet*. 272 A.D.2d 982. 708 N.Y.S.2d 227, 2000 N.Y. Slip Op. 04475.

5. *Case Stoner v. eBay*, Inc., No. 30566, 2000 WL 1705637, at *3 (Cal. Sup. Ct., Nov. 1, 2000). 141 Cong. Rec. H8468-69 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

6. Case *Zeran v. America Online*, Inc., 129 F.3d 327 (4th Cir. 1997).

7. Civil Judgement (2006) Y.G.F.M.S.Z.Z. No. 355 issued by Guangdong Province Higher People's Court.

8. Civil Judgment (2011) Z.L.M.Z.Z. No. 40 issued by Zhejiang Province Lishui City Intermediate People's Court.

9. Dörr, Dieter, Janich, Steffen, 2011. *The Criminal Responsibility of Internet Service Providers in Germany*. *Mississippi Law Journal*, 80, 1247-1261.

10. Gorman, Robert A., Ginsburg, Jane C., 2006. *Copyright: Cases and Materials (*7th ed.*)*, Foundation Press.

11. Guangquan, Zhou, *The Scope of Criminal Liability of Internet Servicers*, 2 China Law Review (2015).

12. Hao, Che, *Who Shall Be Responsible for the Consequence of Neutral Behaviors in the Internet Age*, 1 China Law Review (2015).

13. Hongbing, Chen, *Research into the Punishability of Neutral Behaviors on the Internet: Centered on the Judgment of P2P Service Providers' Behaviors*, 3 Journal of Northeastern University: Social Sciences Edition (2009).

14. Houjun, Gong, *On the Evolution of the Theory on Guarantor and Its Enlightenment*, 4 Studies in Law and Business (2007).

15. Jian, Gao, *Haiding District Court Accepting the QvodPlayer Case Involving Pornographic Materials*, Beijing Daily, Feb. 11, 2015.

16. Judgment (2011) Z.L.M.Z.Z. No. 40 issued by Zhejiang Province Lishui City Intermediate People's Court.

17. Lawrence G. Walters (2012), *Shooting the Messenger: An Analysis of Theories of Criminal Liability Used Against Adult- Themed Online Service Providers*, in Stanford Law and Policy Review, 171, 10.

18. Leckner, Theodor et. al. § 184 pt. 58, in Adolph Schonke, Horst Schroder, *Kommentar zum Strafghesetzbuch* (2006).

19. Roommates.com, LLC, 521 F.3d 1157, 1161 (9th Cir. 2008) (en banc).

20. Roommates.com, LLC, 521 F.3d 1164 (9th Cir. 2008) (en banc).

21. Xu, Lu, *On the ISP's Criminal Liability and Related Issues*, 6 Research on Rule of Law (2015).

22. Yen, Alfred C. (2000). *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, The Georgetown Law Journal, 88, 4.

23. Yu, Zhigang, *The Criminal Law Theory in Virtual Space*, China Fangzheng Press (2003), 185.

24. Zhou Guangquan, *The Scope of Criminal Liability of Internet Servicers*, 2 China Law Review (2015).

Computer crimes in Republic of Serbia

Dr Dragan Jovašević[1]
Full Professor of the Faculty of Law, Niš

Abstract

Criminal Legislation of the Republic of Serbia, which started applying as of 1 January 2006, provides for criminal responsibility and punishment for several criminal offences against safety of computer data. Those are computer criminal offences which a perpetrator (who obviously has unique, special knowledge of information, compute technology – IT sector) commits by abuse of computers, computer systems or network, thereby causing material or non-material damage to other natural or legal persons, as well as a whole social community. The basis of those incriminations are European standards established under the Budapest Convention on Cyber Criminal and Additional Protocol to this Convention, as well as many other European documents. The paper analyses basic characteristics of computer criminal offences in Serbia and the degree of their compatibility with European standards.

Keywords: *computer abuse, european standards, crime, responsibility, sanction*

I. Introduction

When adopting the Convention on Cybercime, ETS 188 of 23 November 2001 the Council of Europe[2] tried to set up basis of a unique European system of substantial and procedural criminal law in the field of necessary cooperation of State members in fighting various forms and kidns of cyber crime. The Convention itselft (Articles 2-13) stipulated five such crimes directed against security, entirety and availability of computer data and computer systems. Hereby, basis for some national legislations have been set more precisely in term of determining features and characteristics of individual computer crimes, their basic, minor and more severe forms, and prescribing criminal sanctions for their perpetrators (natural and legal persons)[3].

An additional Protocol on criminalisation of acts of a racist and xenophobic nature committed through computer systems has been adopted with this Convention. In Articles 3-7 this Protocol stipulates criminal responsibility and penalties for abuse of computers in committing crimes out of racial and xenophobic impulses (motives)[4].

By accepting the above mentioned Convention, and amending the Criminal Code of the Republic of Serbia in April 2003, numerous computer crimes have been introduced into the criminal and legal system in Chapter 16a, under title „Crimes against security of computer data"[5]. The same crimes were introduced into the 2003 Criminal Code of Monte Negro in Chapter 28 with the same title[6].

---

[1] University of Niš, Law Faculty, Trg kralja Aleksandra Ujedinitelja 11, 18 000 Niš, Srbija.
[2] B.Petrović, D.Jovašević, *International Criminal law*, Sarajevo, 2010, pp. 89-92.
[3] D.Jovašević, *International Criminal law*, Niš, 2011, pp. 109-111.
[4] D.Jovašević, V.Ikanović, *International Criminal law*, Banja Luka, 2015, pp. 97-99.
[5] D.Jovašević, *Commentary of Criminal code of Republic of Serbia*, Neograd, 2003, pp. 389-392.
[6] Lj.Lazarević, B.Vučković, V.Vučković, *Commentary of Criminal code of Montenegro*, Cetinje, 2004, pp. 639-644.

II. General characteristics of criminal and legal protection of computer data

Object of protection of these crimes is security of computer data and systems, that is of computer network. The legislator uses for it the term computer crime. But, aside from this term, the legislation of the Republic of Serbia uses the term of hi-tech crime for crimes being systemized here.

Article 112 of the 2005 Criminal Code of the Republic of Serbia[7] (hereinafter: the Criminal Code) determines the term and characteristics of: computer data, computer network, computer programme, computer virus, computer and computer system in term of object of attack in case of these crimes. The term computer crime understands all various shapes, kinds and forms of expression of illegal behaviors directed against security of computer and information systems as a whole or some of their parts, in different ways and with different means, with intention to gain the benefit for himself or the other person (of material or non-material nature) or to cause damage to other person. Characteristic of a computer crime is huge dynamics and extreme variety of its appearance forms and kinds and manifestation forms.

Perpetrators of these crimes are in a specific category of persons. They are mostly non-delinquents and socially adjustable, non-violent persons. They must have certain special, expert and practical knowledge and skills in the domain of information and computer techniques and technologies.

In practice, there is a greater or lesser time difference between the action taken and the moment when the consequences occur. These crimes are difficult to detect and even harder to prove, they remain practically undiscovered for a long time, until the damaged person suffers harm in the domain of information and computer data or systems.

III. Individual computer crimes

1. Damaging computer data and programmes

Crime under Article 298 understands unauthorized deletion, alteration, damage, concealement or otherwise making unusable a computer data or programme[8].

Object of protection is security of computer data or computer programmes, and object of attack is computer data or programme.

Computer data is every representation of facts, information or concepts in a form suitable for processing in a computer system, including appropriate computer software necessary for the functioning of the computer system. A computer programme is a regulated set of orders serving to control computer operations, as well as solving specific tasks by means of a computer.

Consequence of this crime is violation of protected good – computer data or programme belonging to natural or legal persons in term of its usability or usefulness in general, or for a specific time, at a specific place or for specific purpose.

The perpetrator of the crime may be any person, and the guilt requires intent.

A fine or sentence of imprisonment of up to one year is prescribed for this crime. The court shall obligatory impose on the perpetrator a security measure of seizure of

---

[7] Official Gazette of Republic of Serbia No. 85/2005, 88/2005, 107/2005, 72/2009, 105/2011, 121/2012, 108/2014, 94/2016 and 35/2019.

[8] D.Jovašević, *Criminal law, Special part*, Beograd, 2017, pp. 232-234.

equipment and devices if the following two conditions are fulfilled: 1) the equipment and devices were used for commission of the crimes and 2) the equipment and devices are the property of the perpetrator.

This crime has two aggravating forms[9].

The first form of this crime exists if the action taken in the execution of the basic crime caused damage amounting to over RSD 450,000. The amount of material damage caused at the time of the commission of the crime in the amount established under the law constitutes a qualifying circumstance. A sentence of three months to three years of imprisonment is prescribed for this crime.

The second form of this offence, for which a sentence of three months to five years of imprisonment is prescribed, exists if the action taken in the execution of the basic crime caused material damage amounting to over RSD 1.500.000.

2. Computer sabotage

This crime set out in Article 299 of the Criminal Code is committed by whoever enters, destroys, deletes, alters, damages, conceals or otherwise makes unusable computer data or programme or damages or destroys a computer or other device for electronic processing and transfer of data, with intent to prevent or considerably disrupt the procedure of electronic processing and transfer of data that are of importance for government authorities, public service, institution, enterprise or other entities[10].

The entry is entering or storing of a new, previously non-existing data or alteration of already existing computer or other data in the computer programme. Destroying is a complete and permanent destruction of a substance or form of a specific object so it cannot not be used for any purpose or previous intention it was used for. Deletion is removing of computer data or programme in its entirety or a part of it, often by use of mecanical or other means.

Alternation[11] is partial change of existing data in term of its substance, place of its whereabouts or nature, or entering of other untrue data into computer system. Damage is temporary, partial or short-term disability of a computer data, programme, computer or other device to serve its regular purpose. Concealment is removing of data or object from the place where it was, the place known to everyone, and its transfer to another, mostly hidden place where other persons cannot be introduced to its content in general or for a certain period of time. Making unusable computer data or programme is any action which, to a greater or lesser extent, affects the usability of computer data or programme.

The perpetrator of the crime may be any person, and the guilt requires a direct intent characterized by mentioned intention. A sentence of imprisonment of six months to five years is prescribed for this offence.

3. Generating and introducting computer viruses

A specific crime set out in Article 300 of the Criminal Code consists of generating computer virus with intention of its introduction or its introduction into somebody else's computer or computer network[12].

---

[9] B.Petrović, D.Jovašević, *Criminal law, Special part*, Sarajevo, 2005, pp. 297-299.
[10] M.Simović, D.Jovašević, *Lexicon of Criminal law*, Sarajevo, 2016, pp. 583-585.
[11] D.Jovašević, V.Ikanović, *Criminal law, Special part*, Banja Luka, 2012, pp. 212-214.
[12] B.Petrović, D.Jovašević, A.Ferhatović, *Criminal law 2*, Sarajevo, 2016, pp. 313-315.

Object of protection is security of a computer and computer network from viruses of different kinds and nature, and object of attack is a computer virus. That is a computer programme or some other set of commands introduced into the computer or computer network generated to multiply itself and affect other programmes or data in the computer of computer network by adding of that programme or set of commands to one or more computer programmems or data.

Perpetrator of the crime may be any person, and in practice those are persons having special knowledge in the scope of computers and informatic technologies. As to the guilt a direct intent characterized by mentioned intention is necessary.

A fine or sentence of imprisonment of up to six months are prescribed for this crime. Equipment and devices for commission of this crime are obligatory seized when appying security measure of seizure of object.

Aggravated form of this crime, for which a fine or sentence of imprisonment of up to two years is prescribed, exists if damage is caused by a virus generated in this way and introduced into somebody else's computer or computer network. For the existence of crime it is important that the perpetrator is aware and knows that, during the time of committing a crime – work on a computer, he thereby introduces a computer virus into somebody else's computer or computer network. Damage caused thereby may be of material or non-material character. It is important that a damage caused is a result of commission of a basic crime and that the perpetrator acts with negligence in relation to it.

4. Computer fraud

Computer fraud set out in Article 301 of the Criminal Code consists of entering incorrect data, failure to enter correct data or otherwise concealing or falsely representing data, thereby affecting the results of electronic processing and transfer of data with intent to acquire for himself or another unlawful material gain and thus causing material damage to another person[13].

Object of protection is securing of computer systems from entering incorrect and false data and trust in those systems.

Concealing is failure to enter a data by a person who is obliged to enter it into computer or a computer network. It may involve any data. False representing of computer data exists when false data (be it entirely or partialy false) is represented, published, entered or used in the computer network. Both actions have to be taken in relation to the data which is, by its significance, nature, character and time of entering or use, capable of affecting the result (course and procedure) of electronic processing and transfer of data in computer system.

All the actions in term of commission of this crime have to be taken with certain intent – intent of the perpetrator to acquire for himself or another unlawful material gain. The perpetrator has to have that intent in time of commission of the crime, but does not have to be acquired in the concrete case. A result of this crime is violation causing material damage to another person.

Perpetrator of the crime may be any person, and as to the guilt a direct intent characterized by mentioned intention is necessary.

A fine or sentence of impirsonment of up to three years is prescribed for this crime.

Lighter form of crime exists when a perpetrator committed a crime – hiding or false presentation of data in the computer or computer network in a legally preserbied

[13] D.Jovašević, *Lexicon of Criminal law*, Beograd, 2011, pp. 590-593.

manner with intention to cause damage to another person, that is to cause damage to another natural or legal person. Malicious intention of the perpetrator to cause material or non-material damage to another person is a privileged circumstance for which a fine or sentence of imprisonment of up to six months is prescribed under the law.

This crime has two aggravated forms[14].

The first one, for which a sentence of imprisonment of one to eight years of imprisonment is prescribed, exists when material gain (for perpetrator or another person) is acquired by committed basic crime in the amount of over RSD 450,000. The amount of acquired material gain is a qualifying circumstance. It has to be in cause-and-effect connection with commission of the crime.

The second form of aggravated crime exists if a perpetrator acquired illegal material gain by committing the crime in the amount of over RSD 1,500,000. Sentence of imprisonment of two to ten years is prescribed for this crime.

5. Unauthorised Access to Protected Computers, Computer Networks and Electronic Data Processing

This crime set out in Article 302 of the Criminal Code consists of accesses to a computer or computer network without authorisation, or accesses to electronic data processing without authorisation by breaching of protection measures[15].

Object of protection is security of a computer or computer network, or system of electronic data processing protected by a special technical and other protection measures.

Perpetrator of the crime may be any person having specific knowledge in the field of protection of computers or computer systems. As to the guilt a direct intent is necessary.

A fine or sentence of impirsonment of up to six months is prescribed for this crime.

This crime has two aggravated forms.

The first one exists in case of recording or use of computer data, obtained by accessing somebody else's computer or computer network or system of electronic data processing without authorization, given that it was done by breaching of protection measures. A fine or sentence of imprisonment for up to two years is prescribed for this crime. It has no significance which purpose or intention such obtained (recorded) computer data was used for.

The second aggravated form of this crime, for which a fine or sentence of imprisonment of up to three years is prescribed, exists if computer data (one or more) is obtained by accessing somebody else's computer or computer network or somebody else's system of electronic data processing without authorization by breaching protection measures, and is subsequently used which results in suspensioin or serious malfunction in electronic processing and transfer of data or of the network, or other serious consequences have occurred for another (natural or legal) person.

6. Preventing or Restricting Access to Public Computer Networks

A crime prescribed under Article 303 of the Criminal Code consists of preventing or hindering access to a public computer network without authorization[16].

---

[14] D.Jovašević, Lj.Mitrović, V.Ikanović, *Criminal law, Special part*, Banja Luka, 2017, pp. 278-291.
[15] M.Kokolj, D.Jovašević, *Criminal law, General and special part,* Bijeljina, 2011, pp. 389-391.
[16] D. Jovašević, *Criminal code with Commentary*, Beograd, 2007, pp. 67-71.

Object of protection is public computer network and its free access to individually undefined number of persons. Motive of this incrimination is prevention of monopol for using of public computer network.

Prevention is unabling another person to access public computer network completely, permanently or for certain shorter period of time. It may be done by physical prevention, setting of some requirements or obstacles, or requesting fulfillment of certain assumptions. Hindering means partial complication, making difficult or inaccessible, or conditioning another person to access or use public computer network without disturbances and freely, at its own discretion.

Perpetrator of the crime may be any person, and as to the guilt a direct intent is necessary.

A fine or sentence of impirsonment of up to one year is prescribed for this crime.

Heavier form of this crime, for which a sentence of imprisonment for up to three years is prescribed, exists if the crime is committed by an official in discharge of duty.

7. Unauthorised Use of Computer or Computer Networks

A crime prescribed under Article 304 of the Criminal Code consists of use of computer services or computer networks without authorization and with intent to acquire unlawful material gain for himself or another person[17].

Object of protection is legality and conscientiousness in use of computer systems – services or networks, of all forms of abuse and negligence.

There has to be an intent of the perpetrator at a time of comission of the crime, but it does not have to be realized in the concrete case.

A perpetrator of crime may be any person, and as to the guilt a direct intent characterized by mentioned intent is necessary.

A fine or sentence of imprisonment for up to three months is prescribed for this crime.

8. Manufacture, Procurement and Provision to others Means for the Committing Criminal Offences against the Security of Computer Data

This is a new computer crime[18] (Article 304a of the Criminal Code) introduced into the Criminal Code by novelty from 2009. Actually, these are punishable preparation acts for commission of a computer crime. The crime itself consists of possession, manufacture, procurement, sale or giving to another person for his use of computer, computer system, computer data or programme intended for committing of crimes against security of computer data. Prescribed sentence for this crime is imprisonment for six months to three years, while the objects of commission of the crime shall be seized from the perpetrator by use of a special security measure of seizure of object.

Object of protection in this case is also a security of computer systems and data, which is applied in a specific manner – just before the commission of a crime.

IV. Conclusion

When accepting provisions of numerous relevant European documents finally inaugurated by adoption of the Convention on Cyber Criminal, state members of the

[17] D. Jovašević, Lj. Mitrović, V. Ikanović, *Commentary of Criminal code*, Banja Luka, 2018, pp. 699-701.
[18] Official Gazette of Republic of Serbia, No.121/2012.

Council of Europe created in their national legislations legal basis for introduction of a specific kind of „computer" crimes, with the aim to provide performance of various tasks and services by use of a computer with confidence and in an efficient, quality, lawful and secure manner.

Accordingly, in Republic of Serbia many crimes of this kind have been introduced into its criminal and legal system and the legislator, having respect for established European standards, provided criminal sanctions for some forms and kinds of prescribed computer crimes. Thereby, with appropriate process requirements (establishing of special organs for fighting hi-tech crime within the police, public prosecution and the court), basis for efficient fight of our state with this modern forms and kinds of criminality knowing no boundaries between the states have been created.

References

1. Jovašević, D., *Commentary of Criminal code of Republic of Serbia*, Neograd, 2003.
2. Jovašević, D., *Criminal code with Commentary*, Beograd, 2007.
3. Jovašević, D., *Criminal law, Special part*, Beograd, 2017.
4. Jovašević, D., Ikanović, V., *Criminal law, Special part*, Banja Luka, 2012.
5. Jovašević, D., Ikanović, V., *International Criminal law*, Banja Luka, 2015.
6. Jovašević, D., *International Criminal law*, Niš, 2011.
7. Jovašević, D., *Lexicon of Criminal law*, Beograd, 2011.
8. Jovašević, D., Mitrović, Lj., Ikanović, V., *Commentary of Criminal code*, Banja Luka, 2018.
9. Jovašević, D., Mitrović, Lj., Ikanović, V., *Criminal law, Special part*, Banja Luka, 2017.
10. Kokolj, M., Jovašević, D., *Criminal law, General and special part*, Bijeljina, 2011.
11. Lazarević, Lj., Vučković, B., Vučković, V., *Commentary of Criminal code of Montenegro*, Cetinje, 2004.
12. Official Gazette of Republic of Serbia No. 85/2005, 88/2005, 107/2005, 72/2009, 105/2011, 121/2012, 108/2014, 94/2016 and 35/2019.
13. Official Gazette of Republic of Serbia, No.121/2012.
14. Petrović, B., Jovašević, D., *Criminal law, Special part*, Sarajevo, 2005.
15. Petrović, B., Jovašević, D., Ferhatović, A., *Criminal law 2*, Sarajevo, 2016.
16. Petrović, B., Jovašević, D., *International Criminal law*, Sarajevo, 2010.
17. Simović, M., Jovašević, D., *Lexicon of Criminal law*, Sarajevo, 2016.

Specific aspects on the right to a fair trial in the recent caselaw against Romania

PhD Laura Stănilă*
Senior Lecturer
Faculty of Law
West University Timişoara

Abstract

The right to a fair trial provided by art. 6 ECHD is one of the most important elements of the Rule of law. The general content and the specific elements of the right to a fair trial are subject to the constant and contextual teleological interpretation of the European Court of Human Rights. Also, the right to a fair trial received an autonomous interpretation in relation with substantive and procedural provisions of the domestic law. The present study focuses on the recent caselaw of the European Court of Human Right agains Romania regarding the violation of art. 6 ECHD.

Keywords: *right to a fair trial, European Convention of Human Rights, specific guarantees, entrapment, incitement, reasonable duration of the trial,* Al-Khawaja test

I. General aspects on the right to a fair trial as regulated by European Convention of human Rights (ECHD)

The right to a fair trial provided by art. 6 ECHD as a procedural guarantee of the rights and freedoms of a person facing national criminal courts, constitutes one of the premises of ensuring pre-eminence of the Rule of Law in a democratic society. The legal text of the precited article contains a description of the mechanisms of this specific guarantee, the limits of its application and its general and specific content[1].

a) the description of the mechanisms of the guarantee is made by art. 6 § 1 ECHD in determination of *„(...) any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law."* The text establishes both the object of the guarantee, and the entitled person, natural or legal, the debtor of the obligation being the State party to the convention under whose jurisdiction the holder of the right is.

---

* E-mail: laura.stanila@e-uvt.ro.

[1] *See* Ovidiu Predescu, Mihail Udroiu, 2007, *Convenţia Europeană a drepturilor Omului şi dreptul procesual penal român*, Ed. Ch.Beck, Bucureşti, p. 258-261. According to other scholars, the right to a fair trial is divided now in three pylons: the main pylon refers to the procedural safeguards *stricto sensu,* the equality of arms, the independence and the impartiality of the court, the publicity and celerity of the criminal trial. The second one refers to two other material rights, the right to access a court, the right for the enforcement of decisions; the third refers to the right of every person to access a court. *See* F. Sudre, 2005, *Droit Européen et international*, Ed. Presses Universitaire de Rance, 7e édition refondue, p. 338.

b) the limits of the guarantee application are set by the same art. 6 § 1 ECHD art. 6 § 1 ECHD as the *„determination of civil rights or any criminal charge against one person"*. The right to a fair trial presumes both civil obligations and criminal accuzations.

c) the general content of the guarantee refers to a *„fair and public hearing within a reasonable time by an independent and impartial tribunal established by law"*. The folowing general elements are set by the art. 6 as following: the right to be heard by a legal, independent and impartial tribunal (court), the right to a public trial, the right to be judged within a reasonable time, the principle of equality of arms, the principle of contradictority, the right to remain silent and not to self-incriminate oneself, the obligation of motivating the decision by the court.

d) the specific content of the guarantee is set on paraghaph 2 and 3 of the art. 6 ECHD which regulates the specific elements of the right to a fair trial: the presumtion of innocence[2] and the rights of defence[3].

All the rights regulated by Art. 6 § 3 ECHD are elements of the general notion of *„fair trial"*. The Strassbourg Court has stated in *Colozza v. Italy* that *„the guarantees contained in paragraph 3 of Article 6 are constituent elements, amongst others, of the general notion of a fair trial"*[4]. Also, the Strasbourg Court has constantly shown in its caselaw that the obligations instituted for the states by art. 6 are to be fulfilled by them even if the Court cannot substitute the national courts in their reasoning or national legislators in their regulating activity[5].

Article 6 § 3 ECHR regulates specific guarantees of the fair trial principle in respect of typical procedural situations which arise in criminal cases. These specific elements are not an end in themselves and must be interpreted in the light of the function which they have in the overall context of the proceedings. As stated in Mayzit v. Russia, *„the specific guarantees laid down in Article 6§3 exemplify the notion of fair trial in respect of typical procedural situations which arise in criminal cases, but their intrinsic aim is always to ensure, or contribute to ensuring, the fairness of the criminal proceedings as a whole.*

---

[2] Art. 6 § 2 ECHD: *„Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law."*

[3] Art. 6 § 3 ECHD: *„3. Everyone charged with a criminal offence has the following minimum rights:*

(a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;

(b) to have adequate time and facilities for the preparation of his defence;

(c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;

(d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

(e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court."

[4] Case *Colozza v. Italy*, paras. 26-27, Application no.9024/80, Judgment 15 february 1985, https://hudoc.echr.coe.int, acessed on 20.06.2019; Same statement in Case *Goddi v. Italy*, Application no. 8966/80, Judgment of 9 April 1984, par. 28, https://hudoc.echr.coe.int, acessed on 20.06.2019

[5] Case *Schenk v. Switzerland*, paras. 45-46, Application no.00010862/84, Judgment 12 July 1988, https://hudoc.echr.coe.int, acessed on 20.06.2018:*"According to Article 19 (art. 19) of the Convention,the Court's duty is to ensure the observance of the engagements undertaken by the Contracting States in the Convention. In particular, it is not its function to deal with errors of fact or of law allegedly committed by a national court unless and in so far as they may have infringed rights and freedoms protected by the Convention.*

While Article 6 (art. 6) of the Convention guarantees the right to a fair trial, it does not lay down any rules on the admissibility of evidence as such, which is therefore primarily a matter for regulation under national law."

The guarantees enshrined in Article 6 § 3 are therefore not an end in themselves, and they must accordingly be interpreted in the light of the function which they have in the overall context of the proceedings"[6].

These specific rights/guarantees set by art. 6 § 3 ECHD are:

1. Information on the nature and cause of the accusation - Article 6 § 3 (a) ECHR;
2. Preparation of the defence - Article 6 § 3 (b) ECHR;
3. Right to defend oneself in person or through legal assistance - Article 6 §3(c) ECHR;
4. Examination of witnesses - Article 6 § 3 (d) ECHR;
5. Interpretation -Article 6 § 3 (e) ECHR.

Due to its complexity, art. 6 is approached by the European Court of Human Rights (in the following „the Court") as subject to teleological interpretation[7]. The Court avoids theoretical and illusory approaches, giving a contextual interpretation of art. 6 ECHD in its efforts to give practical effect to the purpose of the provision, establishing the so-called principle of effectiveness.

Another observation regarding art. 6 ECHD refers to the fact that this provision must be interpreted in the light of present-day conditions, in regard with the economic, social, legal frame of the domestic State[8] also taking into account the principles of international law applicable in relations between the State parties[9]. Finally, by analysing the arguments of the Court in cases like *Khan v. the United Kingdom,* the scholars[10] observed that art. 6 „enjoys significant autonomy within the domestic law in its substantive as well as its procedural provisions"[11].

Even if the Court has shown a creative and profound interpretation of the art. 6, the Court cannot act as distinct instance in order to re-examine the alleged breaches of domestic law nor to dictate its content, States remaining free to apply the criminal law to any act and to define the constituent elements of the offence committed.

II. Recent caselaw against Romania

Recent cases agains Romania have shown the same meticulous preoccupation of the Court to observe domestic legislation while seeking to provide real guaratees of a person indicted or convicted in a criminal trial in order for that person benefit of his or her procedural rights.

---

[6] Case *Mayzit v. Russia*, par. 77, Application no. 63378/00, Judgment 6 July 2005, https://hudoc.echr.coe.int, acessed on 20.06.2019.

[7] Dovydas Vitkauskas, Grigoriy Dikov, 2017, *Protecting the right to a fair trial under the European Convention on Human Rights*, Second edition, Council of Europe, p. 10.

[8] Case *Marckx v. Belgium,* par. 41, Application no.6833/74, Judgment 13 June 1979, http://hudoc.echr.coe.int, acessed on 20.06.2019.

[9] When the Court *„considers the object and purpose of the Convention provisions, it also takes into account the international law background to the legal question before it. Being made up of a set of rules and principles that are accepted by the vast majority of States, the common international or domestic law standards of European States reflect a reality that the Court cannot disregard when it is called upon to clarify the scope of a Convention provision that more conventional means of interpretation have not enabled it to establish with a sufficient degree of certainty."* Case *Demir and Baykara v. Turkey,* par. 76, Application no. 34503/97, Judgment 12 November 2008, http://hudoc.echr.coe.int, acessed on 20.06.2019.

[10] Dovydas Vitkauskas Grigoriy Dikov, *op. cit.*, p. 12.

[11] Case *Khan v. the United Kingdom*, Application no. 6222/10, Final Judgment 20 March 2012, http://hudoc.echr.coe.int, acessed on 20.06.2019.

II.1. Case Ursu v. Romania 2018

In case *Ursu v. Romania*[12], the Court has emphasized the importance of the principle of equality, establishing the double test standard for incitement oncemore.

The applicant, Mr. Ursu, was convicted in Romania for drug trafficking, in violation of Law no. 143/2000 on the fight against drug trafficking and illegal drug use, as a member of a network of dealers that was trafficking drugs in city Constanța. At the time of committing the acts, the applicant was a student and an acquaintance of another convicted person in the same case, studying at the same university. The applicant was caught bringing drugs to the other convicted and an undercover agent (eighteen ecstasy tablets and 0.46 grams of cannabis resin).

The applicant's first statement to the police (given on 26 June 2005), was given in the absence of a lawyer and interpreter. He maintained his allegations in a statement given in the presence of two lawyers of his choice on 19 July 2005. He added that he had accepted to provide D. with the ecstasy tablets in the hope of having an intimate relationship with her during his stay in Constanța. On the occasion of several hearings held in 2005 before the Constanța County Court, the applicant denied his involvement in drug trafficking and claimed that he had been entrapped by the police.

In 2007 the Constanța County Court convicted the applicant of drug trafficking and sentenced him to one and a half years' imprisonment suspended on probation dismissing his allegations that he had been entrapped. The Constanța County Court did not provide any reasons justifying the fact that, in spite of the applicant's insistence, D. had not been heard. The Constanta County Court convicted the applicant reliyng on his own statements, corroborated by the statements made by the friends who had accompanied him, as well as on reports produced by the undercover agent and the police following the police operation leading to the catch of the applicant in the act of committing a crime.

The Appeal Court dismissed the applicant's appeal and upheld the County Court's findings without providing any additional reasons, reiterating that the evidence obtained by using an undercover agent was in accordance with Law no. 143. It did not refer at all to the applicant's argument that D had not been heard.

The appeal on points of law based on the same arguments – Mr. Ursu had been unduly incited by D to commit the offence of which he had been found guilty and that throughout the proceedings he had not had an opportunity to have her questioned has been dismissed in 2009 by the High Court of Cassation and Justice as ill-founded, the highest Court of Romania upholding the reasoning of the two previous lower courts.

Mainly, the reasoning of the Court in this case is based on the notion of *„entrapment"* which includes the notion of *„incitement"*. The concept of entrapment in breach of art. 6 § 1 of the Convention, is distinguished from the use of legitimate undercover techniques in criminal investigations. While the use of special investigative methods in general and the undercover techniques in particular, cannot in itself infringe the right to a fair trial. The Court explicitly emphasized that the risk of police incitement entailed by such techniques meant that their use must be kept within clear limits. For example, in case Ramanuskas v. Lithuania, the Court stated that the use of special investigative methods, on account of the risk of police incitement entailed by such

[12] Case *Ursu v. Romania* (2018), Application no. 44497/09, Judgment 18 December 2018, http://hudoc.echr.coe.int, acessed on 20.06.2019.

techniques, must be kept within clear limits[13]. Police incitement occurs where the officers involved – whether members of the security forces or persons acting on their instructions – do not confine themselves to investigating criminal activity in an essentially passive manner, but exert such an influence on the subject as to incite the commission of an offence that would otherwise not have been committed, in order to make it possible to establish the offence, that is, to provide evidence and institute a prosecution[14].

The Court has recognised in general that the rise in organised crime and difficulties encountered by law-enforcement bodies in detecting and investigating offences has warranted appropriate measures being taken and that the police are increasingly required to make use of undercover agents, informants and covert practices, particularly in tackling organised crime and corruption. The use of undercover investigative techniques in combatting crime is accepted by the Court as a necessity of this facts and on several occasions undercover operations *per se* did not interfere with the right to a fair trial. The presence of clear, adequate and sufficient procedural safeguards set permissible police conduct aside from entrapment[15].

The general principles concerning the issue of entrapment were set out in the case of *Ramanauskas* (2008) and reafirmed 10 years later in *Ramanuskas 2* (2018)[16]: the right to a fair trial in regard of the issue of entrapment would be violated where police officers had stepped beyond an essentially passive investigation of a suspect's criminal activities and had exercised an influence such as to incite the commission of an offence that would otherwise not have been committed. The Court has made a step further and considered that the issue of entrapment could be relevant even where the operation in question had been carried out by a private individual acting as an undercover agent, when it had actually been organised and supervised by the police. In *Vanyan v. Russia*, the Court has stated that the use of undercover agents must be restricted and safeguards put in place even in cases concerning the fight against drug trafficking. The requirements of a fair criminal trial under Article 6 entail that the public interest in the fight against drug trafficking cannot justify the use of evidence obtained as a result of police incitement[17]. *„Where the activity of undercover agents appears to have instigated the offence and there is nothing to suggest that it would have been committed without their intervention, it goes beyond that of an undercover agent and may be described as incitement. Such intervention and its use in criminal proceedings may result in the fairness of the trial being irremediably undermined"*[18].

The Court had also established a set of criteria to distinguish entrapment breaching Article 6 § 1 of the Convention from permissible conduct in the use of legitimate undercover techniques in criminal investigations. The Court's examination of complaints of entrapment has developed on the basis of two tests: the substantive and the procedural test of incitement.

---

[13] Case *Ramanauskas v. Lithuania*, par. 51, Application no. 74420/01, Judgment 5 February 2008, http://hudoc.echr.coe.int, acessed on 20.06.2019.

[14] Ramanuskas v. Lithuania, par. 55.

[15] Case *Ramanauskas v. Lithuania (2),* par. 52, Application no. 55146/14, Judgment 20 February 2018, http://hudoc.echr.coe.int, acessed on 20.06.2019.

[16] See *supra* note 12.

[17] Case *Vanyan v. Russia*, par. 46, Application no. 53203/99, Judgment 15 March 2006, http://hudoc.echr.coe.int, acessed on 20.06.2019.

[18] Case *Vanyan v. Russia*, par. 47.

The criteria for the substantive test were set up in case Ramanuskas cited above[19] and reiterated in the courts further judgments, such as Case of *Matanović v. Croatia*[20]:

- whether the offence would have been committed without the authorities' intervention, that is to say whether the investigation was *„essentially passive"*;

- was the execution of the simulated purchases performed by an undercover officer or informant particularly well justified, was it subject to a stringent authorisation procedure, and was it documented in a way that allowed a subsequent independent scrutiny of the actors' conduct.

If the results of the substantive test are inconclusive or positive, the court steps to the procedural test. The Court applies the procedural test of incitement in order to determine whether the necessary steps to uncover the circumstances of an arguable plea of incitement were taken by the domestic courts and whether in the case of a finding that there has been incitement or in a case in which the prosecution failed to prove that there was no incitement, the relevant inferences were drawn in accordance with the Convention[21].

In Case *Ursu v. Romania* the Court's examination of complaints of entrapment has meticulously developed on the basis of the substantive and the procedural test of incitement as follows:

As a preliminary step, the Court had to establish whether the situation under examination falls prima facie within the category of *„entrapment cases".* In case of a positive answer, the Court had to proceed with the substantive test, followed by the procedural test.

a. Substantive test of incitement

The Romanian authorities' statement differed from the applicant's as to D's role in the applicant's acting as an intermediary for the drug sale and the existence of objective suspicions that the applicant had been regularly trafficking drugs prior to the setting up of the undercover operation. Romanian authorities have produced no evidence to substantiate their claim that before the intervention by D., the police had reason to suspect that the applicant was a drug dealer due to the fact that the police report did not offer any more details in respect of the information the authorities had about the applicant's alleged involvement in drug trafficking and how that information had been acquired by the police. The mere claim by the police to the effect that they possessed information concerning the applicant's involvement in drug dealing does not provide a sufficiently solid basis to conclude that the applicant's criminal activities were already ongoing prior to him being contacted by D[22]. In addition, the applicant's behaviour was not indicative of any pre-existing criminal activity while D. had played a significant role in arranging the deal. In its constant rulling, the Court had insisted on the passivity on the State agent's in committing the crimkinal act by the perpetrator. In this case, D. initiated the whole criminal activity under the direct supervision of the investigation bodies and although she was not a State agent and she had not been authorised to act as an undercover agent, the incriminating evidence obtained because of her intervention led to the prosecution and conviction of the applicant[23].

---

[19] See *supra* note 12.

[20] Case *Matanović v. Croatia*, paras. 131-134, Application no. 2742/12, Judgment 4 July 2017, http://hudoc.echr.coe.int, acessed on 20.06.2019.

[21] Case *Matanović v. Croatia*, par. 135.

[22] Case *Ursu v. Romania*, par. 36.

[23] *Idem*, par. 37.

b. Procedural test of incitement

On the second part of the reasoning, the Court had to determine whether the applicant was able to raise the issue of incitement effectively in the domestic proceedings, and to assess the manner in which the domestic courts dealt with his plea

The Court observed the domestic trial courts had failed to properly answer to the allegation raised by the applicant regarding a plea of incitement rejecting it in a summary manner and had failed to verify all the aspects regarding the undercover operation.

Secondly, the Court observed also that the applicant did not, at any stage of the proceedings, have an opportunity to have D. questioned being thus deprived of the possibility of clarifying to what extent D.'s actions had influenced and determined his behaviour[24].

The Court concluded that the applicant was convicted on the basis of evidence obtained by way of police incitement and that the courts which examined the case did not carry out a careful examination of his assertion that he had been incited to commit the offence imputed to him, art. 6 § 1 ECHD being thus violated.

II.2. Case Cernea v. Romania 2018

The applicant, Mr. Cernea was initially (2006) convicted for bribe taking and his assets were seizured, the criminal investigation starting in 2000. As a matter of fact the applicant was initially sent to trial for bribe taking an abbuse in office and the State Agency for Capitalisation of Banking Assets (*Autoritate Pentru Valorificarea Activelor Bancare*– „AVAB") joined the criminal proceedings against the applicant as a civil party soughting the recovery of 27,863,805,105 Romanian lei (ROL) (approximately 1,758,753 US dollars (USD)), the damage that it had allegedly incurred as a result of the applicant's abuse of office. On 16 August 2002 the prosecutor's office ordered the seizure of the applicant's movable and immovable assets up to the value of the damage allegedly incurred by AVAB. The order was enforced by the Bihor Police Department on 19 December 2002 by seizing part of the immovable properties owned jointly by the applicant and his wife, in particular four plots of *intra muros* agricultural land, a home and annexes.

In 2006 the Bihor County Court acquitted the applicant of abuse of office but convicted the applicant of bribe taking and sentenced him to three years' imprisonment, suspended, maintaining the measure imposed on the applicant's assets. Further, as the applicand had appeald the decision, in 2006 the Court of Appeal quashed the judgment of the County Court and referred the case back to the first-instance court for re-examination on procedural grounds. In 2010 when the County Court examined the applicant's case on the merits, acquitted him of abuse of office, dismissed AVAB's civil claim consequently lifting the seizure measure from his assets, but convicted the applicant, however, of receiving bribes and gave him a suspended sentence of three years' imprisonment. The applicand appealed the decision and, by the final judgment of 2011, the Court of Cassation allowed the applicant's appeal on points of fact and law in part helding that he was guilty of bribe taking, but his criminal liability for that offence had become time-barred.

It was only in 2012 the Bihor Land and Immovable Property Register removed the annotation concerning the seizure measure imposed on applicant's immovable property which had prevented him from freely disposing of it.

---

[24] *Idem*, par. 42.

In this case, there were two main complaints made by the applicant against national authorities: the breach of the principle of celerity under art. 6 § 1 ECHD and breach of the principle of peaceful enjoyment of one' property under Article 1 of Protocol No. 1 to the Convention. In the present study we refere solely to the first complaint.

In its rulling, the Court reafirmed the principles set out in its case-law concerning the assessment of the reasonableness of the length of proceedings. But it is worth to mention that the Court stated before that even if *„it is for the Contracting States to organise their judicial systems in such a way that their courts are able to guarantee the right of everyone to obtain a final decision on disputes concerning civil rights and obligations within a reasonable time"*[25], the reasonableness of the length of proceedings must be assessed *„in the light of the circumstances of the case"*: the complexity of the case, the conduct of the applicant and of the relevant authorities and what was at stake for the applicant in the dispute[26].

In case Cernea the criminal proceedings against the applicant had lasted ten years, five months and ten days over three levels of jurisdiction, neither the complexity of the case, nor the applicant's conduct justifying the overall length of the proceedings. Thus the Court stated that the length of the proceedings in the case did not satisfy the *„reasonable time"* requirement and that there has accordingly been a violation of art. 6 § 1 ECHD.

II.3. Case Tău v. Romania 2019

This case is one of the most recent cases against Romania putting into debate the violation of art. 6 § 1 and § 3 (c) and (d) ECHR.The applicant complained of breaches of the guarantees of fair trial: the applicand had been assisted by an officially appointed lawyer who had also been assisting co-accused persons in spite of the fact that he had requested to be assisted by a lawyer of his own choosing and that he had not been given the opportunity to confront in open court a witness whose statements had been relied upon in convicting him[27].

The applicant was arrested in 2003 and investigated for one of the biggest drug-trafficking cases investigated by the Romanian authorities at the time based on the testimony of two other co-accused, F.D. and P.A. who reached an agreement whereby they would give statements about others involved in drug-trafficking in exchange for a reduced sentence. The first applicant's statement was given in the presence of an officially appointed lawyer, who had also been assisting the other two co-accused, denying any involvement in drug-trafficking. During the hearings before the High Court of Cassation and Justice for the examination of the prosecutor's request concerning applicant's pre-trial detention, the applicant was assisted by the same officially appointed lawyer despite the fact that he insisted to be assisted by a lawyer of his own choosing.

The applicant managed to engage a lawyer only a week later.The applicant's pre-trial detention was repeatedly extended by the Bucharest County Court by interlocutory decisions.

---

[25] Case *Lupeni Greek Catholic Parish and Others v. Romania,* par. 142, Application no. 76943/11, Grand Chamber Judgment 29 November 2016, http://hudoc.echr.coe.int, acessed on 20.06.2019.

[26] Idem, par. 143.

[27] Case *Tău v. Romania,* Application no.56280/07, Judgment 23 July 2019, http://hudoc.echr.coe.int, acessed on 30.07.2019.

The prosecutor issued an indictment concerning twenty-six accused persons, including the applicant, but F.D. had not been indicted although he had recognized his involvement in drug-trafficking.

The co-accused, P.A. stated that the applicant had been his friend since 1994 and had helped him in packing drugs. An under-cover agent, in her statement before the court did not mention anything about the applicant envolvment, although in her initial statement given before the prosecutor had stated that many drug transports had left from the applicant's home. In 2005 the Bucharest County Court found the applicant guilty of taking part in international drug trafficking by facilitating the transport of drugs and convicted him to sixteen years' imprisonment.

His conviction was based on statements given by undercover agent, co-accused P.A. and witness F.D. Following the appeal, the Bucharest Court of Appeal reversed the judgment in respect of the applicant and his sentence was reduced to eight years' imprisonment on the grounds that he was an accomplice, had no criminal record and he was more than sixty years old, but had made no reference to the applicant's complaints that he could not confront in open court the witness F.D. The High Court of Cassation and Justice dismissed in 2007 the appeal on points of law by the applicant. It concluded by stating that the applicant's allegations that he had not committed any offence related to drug-trafficking had been contradicted by the statements of witness, co-accused and the undercover agent.

In this case the Court noted that he right of everyone charged with a criminal offence to be effectively defended by a lawyer, assigned officially if need be (art. 6 § 3 (c) ECHD) does not secure an autonomous right but must be read and interpreted in the light of the broader requirement of fairness of criminal proceedings, considered as a whole, as guaranteed by art. 6 § 1 ECHD[28]. At the same time, the Court recalled that *„the compliance with the requirements of a fair trial must be examined in each case with regard to the development of the proceedings as a whole and not on the basis of an isolated consideration of one particular aspect or one particular incident"*[29] *and* that a person charged with a criminal offence should already be given the opportunity at the stage for the preparation of the criminal proceedings to have recourse to legal assistance of his or her own choosing[30].

But since there was no evidence in the file to corroborate the applicant's allegations that he had requested to be assisted by a lawyer of his choosing and that his request had been ignored by the domestic authorities, the Court dismissed the applicant's complaint that he was prevented from being represented by a lawyer of his own choosing at any of the first two hearings. Further, the Court tryed to establish whether the particular circumstance that the *ex* officio lawyer assigned to him for the first two hearings had been already representing two other suspects who incriminated him, affected the effectiveness of legal assistance provided to the applicant. The conclusions of the Court were against the applicant*: „the overall fairness of the criminal proceedings against the applicant had not been irretrievably prejudiced"* by this fact, since in the first two statements given in the absence of a lawyer of his own choosing, the applicant had not confessed the commission of any offence and the lawyer of his own choice actively participated at all stages in the criminal proceedings (with the except of those two first

[28] *Idem*, paras 38-30.
[29] *Idem*, par. 39.
[30] *Idem*, par. 40.

hearings). Also, the Court emphasized that the applicant had not, at any stage in the criminal proceedings before the domestic courts, raised any complaint concerning the efficacy of the legal assistance ensured by the officially appointed lawyer on the ground that the latter had assisted co-defendants with whom he had conflict of interests[31].

The Court concluded that there had been no violation of art. 6 § 1 in connection with art. 6 § 3 (c) ECHR.

As regards the second complaint, the Court had noted that the guarantees in art. 6 § 3 (d) ECHR represent specific aspects of the right to a fair hearing set forth in § 1 which must be taken into account in any assessment of the fairness of proceedings and had followed specific steps in order to determine if there had been a violation of in art. 6 § 3 (d) ECHR. The Court had found out that there had been indeed such a breach applying the *Al-Khawaja* test[32]:

1. Observed the principle that, before an accused can be convicted, all evidence against him must normally be produced in his presence at a public hearing with a view to adversarial argument.

2. Determined whether there was a good reason for the non-attendance of a witness

3. Examined the sole or decisive rule.

4. Identify eventually sufficient „counterbalancing factors" to compensate for the handicaps under which the defence labored.

Due to the fact that domestic courts admitted the pre-trial statement of witness F.D. in evidence without having him questioned at the applicant's trial, the Court noticed that they had not made all reasonable efforts to secure the witness's presence in spite of the applicant's repeated requests to be confronted with F.D., and did not provid any reasons for the witness' non-attendance[33].

In the following the Court observed that the judgments of the domestic courts listed the witness F.D. statement at the pre-trial stage of the investigation in the evidence substantiating the applicant's guilt and considered that, while the statement of witness F.D. may not have been the sole or decisive evidence on which the applicant's conviction was based, it clearly carried significant weight in the establishment of his guilt.

The last step in the rulling of the Court was to establish whether there were sufficient „counterbalancing factors" to compensate for the handicaps under which the defence labored by analysing relevant elements in the context:

a) whether the trial court approached the untested evidence of an absent witness with caution;

b) whether the domestic courts provided detailed reasoning;

c) whether there was corroborative evidence supporting the untested witness statement;

d) whether the applicant or his defence counsel had been given an opportunity to question the witness during the investigation stage;

e) whether the defence was offered the possibility to put its own questions to the witness indirectly in the course of the trial; *and*

f) whether the defendant was afforded the opportunity to give his own version of the events and to cast doubt on the credibility of the absent witness[34].

---

[31] *Idem*, par. 47.

[32] *Al-Khawaja and Tahery v. the United Kingdom,* Applications nos. 26766/05 and 22228/06, Grand Chamber Judgment 15 December 2011, http://hudoc.echr.coe.int, acessed on 30.07.2019.

[33] Case *Tău v. Romania,* paras. 55-56.

[34] *Idem*, par. 61.

The conclusions of this analisys was that the Court could not identiy a good reason for the non-attendance of the absent witness and that the additional incriminating evidence and procedural safeguards capable of counterbalancing the absence of witness F.D. at the applicant's trial were inssuficient. Thus the criminal proceedings, looked at as a whole, were rendered unfair by the admission in evidence of the pre-trial statement of absent witness[35].

III. Conclusion

The right to a fair trial occupies an important place in democratic society. As stated in the doctrine, the fair trial is a fundamental right, as it represents an ideal of a real justice that respects human rights, its influence being very strong both in the domestic and international legal order[36].

In the interpretation of art. 6, the Court examines the correctness of the procedures as a whole, meticulously verifying all the stages of the trial as well as all the actual possibilities offered to a person to defend himself/herself, avoiding the analysis of a simple isolated procedural defect.The right to a fair trial was explicitly enshrined, in the content of art. 21 paragraph (3) of the Romanian Constitution, when it was revised in 2003. The Criminal Procedure Code of Romania also provides in severall article the general and special guarantees of the riaght to a fair trial as follows: art. 4 – presumtion of innocence, art. 8 – the equitabl character and the reasonable duration of the criminal trial, art. 10 – the right to defense, art. 12 par. 3 – the right to an interpreter.

In spite the proper regulation of the the right to a fair trial by the Romanian law, the Romanian State continues to be condemned by the Strasbourg Court for violating art. 6 of ECHR. In our opinion, this is due to the complexity of the cases in their vast majority, as well as to the logistical difficulties faced by the Romanian judicial bodies in the investigation of the criminal cases.

Bibliography

1. Case *Al-Khawaja and Tahery v. the United Kingdom,* Applications nos. 26766/05 and 22228/06, Grand Chamber Judgment 15 December 2011, http://hudoc.echr.coe.int, acessed on 30.07.2019.

2. Case *Colozza v. Italy*, Application no.9024/80, Judgment 15 february 1985, https://hudoc.echr.coe.int, acessed on 20.06.2019.

3. Case *Demir and Baykara v. Turkey,* Application no. 34503/97, Judgment 12 November 2008, http://hudoc.echr.coe.int, acessed on 20.06.2019.

4. Case *Goddi v. Italy*, Application no. 8966/80, Judgment of 9 April 1984, https://hudoc.echr.coe.int, acessed on 20.06.2019.

5. Case *Khan v. the United Kingdom*, Application no. 6222/10, Final Judgment 20 March 2012, http://hudoc.echr.coe.int, acessed on 20.06.2019.

6. Case *Lupeni Greek Catholic Parish and Others v. Romania,* Application no. 76943/11, Grand Chamber Judgment 29 November 2016, http://hudoc.echr.coe.int, acessed on 20.06.2019.

---

[35] *Idem*, par. 67.

[36] D. Gomien, 1996, *Introducere în Convenția Europeană a Drepturilor Omului*, Editura All, București, p. 40.

7. Case *Marckx v. Belgium,* Application no.6833/74, Judgment 13 June 1979, http://hudoc.echr.coe.int, acessed on 20.06.2019.

8. Case *Matanović v. Croatia*, Application no. 2742/12, Judgment 4 July 2017, http://hudoc.echr.coe.int, acessed on 20.06.2019.

9. Case *Mayzit v. Russia*, Application no. 63378/00, Judgment 6 July 2005, https://hudoc.echr.coe.int, acessed on 20.06.2019.

10. Case *Ramanauskas v. Lithuania (2),* Application no. 55146/14, Judgment 20 February 2018, http://hudoc.echr.coe.int, acessed on 20.06.2019.

11. Case *Ramanauskas v. Lithuania*, par. 51, Application no. 74420/01, Judgment 5 February 2008, http://hudoc.echr.coe.int, acessed on 20.06.2019.

12. Case *Schenk v. Switzerland*, Application no.00010862/84, Judgment 12 July 1988, https://hudoc.echr.coe.int, acessed on 20.06.2018.

13. Case *Tău v. Romania,* Application no.56280/07, Judgment 23 July 2019, http://hudoc.echr.coe.int, acessed on 30.07.2019.

14. Case *Ursu v. Romania* (2018), Application no. 44497/09, Judgment 18 December 2018, http://hudoc.echr.coe.int, acessed on 20.06.2019.

15. Case *Vanyan v. Russia*, Application no. 53203/99, Judgment 15 March 2006, http://hudoc.echr.coe.int, acessed on 20.06.2019.

16. Gomien, D., 1996, *Introducere în Convenția Europeană a Drepturilor Omului*, Editura All, București.

17. Predescu, O., Udroiu, M., 2007, *Conven□ia Europeană a drepturilor Omului și dreptul procesual penal român*, Ed. Ch.Beck, București.

18. Sudre, F., 2005, *Droit Européen et international*, Ed. Presses Universitaire de Rance, 7e édition refondue.

19. Vitkauskas, D., Dikov, G., 2017, *Protecting the right to a fair trial under the European Convention on Human Rights*, Second edition, Council of Europe.

The theories and regulation of criminal liability of legal persons in Hungary

Dr. Dávid TÓTH, PhD*
Assistant Lecturer
Criminology and Penal Law Department
Faculty of Law
University of Pécs

Abstract

The aim of the article is to give a general overview of the criminal liability of legal persons in Hungary. The first part of the study introduces the theories of the criminal liability of legal persons in Hungary. In the next chapter of the essay, analyses the in force regulation with a descriptive method. The contribution also deals with the compliance of the Hungarian regulation with the EU legal sources. The final substantial chapter briefly introduces the practice of the liability of legal persons with statistics and single case. This study only analyses the substantive criminal law and not deals with the criminal procedure regarding this topic.

Keywords: *criminal liability, legal person, legal theory.*

I. Introduction

The criminal liability of legal persons is a controversial area. Is it right to hold responsible a legal person for a criminal act committed by a natural person? Is it necessary? What kind of sanctions shall be applied? Many questions arise from this topic.

In the first part of the study I will introduce legal theories of the criminal liability of legal persons in Hungary. The second part of the contribution analyses the in force regulation with a descriptive method. The third part deals with the compliance with the EU legislation. The aim of the article is to give a general overview of the criminal liability of legal persons in Hungary. The current study only analyses the substantive criminal law and not deals with the criminal procedure regarding this topic.

II. Theories in the beginning in Hungary

At the beginning the Hungarian literature did not have big interest towards the topic of criminal liability of legal corporations. The most important monograph in the 20th century was written in 1922 by Ervin Hacker titled „The associations capacity and criminal liability"[1]. The monograph had a positive review over the time. His proposals

* Email: *toth.david@ajk.pte.hu*

[1] Ervin Hacker, *Az egyesületek büntetőjogi cselekvőképessége és felelőssége - Tanulmány az anyagi büntetőjog köréből [The associations capacity and criminal liability – Study within the substantive criminal law]*. Grill Cs. és Kir. Udvari könyvkereskedése, Pécs. 1922.

are still actual today. According to his views the legal persons shall be punishable[2] for legal dogmatic and legal political aspects.

The most important legal political reasons are the following according to Hacker:

- the effective protection against the big capital bloc. The protection of the legal order is more complicate against organizations that collect many assets and have a big membership. It is an actual fact that there are several crimes which can be mostly committed with a corporation[3].

- It gives the option in many types of crimes to hold responsible the real offender. It is not necessary to punish the innocent who only acted for the order of the legal entity and the real sinner can't avoid punishment. It is not breaching the principle of *„ne bis in idem."* We are not holding responsible the same person but a legal entity and a natural person[4].

- The difficulties of the investigation of the offender natural person. On many occasions it is hard to find the offender. In these cases the criminal punishment won't be avoided if the legal person can take the responsibility[5].

- Every sanction can punish innocents. It is an unjust situation when innocent members from the legal entity suffer the punishment indirectly but this can't be avoided. The person who enters into a company has the privilege to enjoy the profits but should also bear the risks as well[6].

- The balance of the rights and duties are equal. On one hand the natural persons are granted with additional rights but on the other hand duties as well which shall be equal according to their scope of rights. It would be inequitable if we grant them only rights but not sanctions from certain legal relations.

Hacker not argues with the fact that there are difficulties with the guilt of the legal entity. The psychological relation between the criminal act and the offender is a prerequisite of the accountability. Only after this can we talk about criminal liability and imputation. The natural person has the qualified will which is required to declare guilt under the criminal law. Is the same possible with legal persons? Hacker says the answer is no. The legal persons have no qualified will it is not possible to declare guilt[7].

III. Newer theories of criminal liability of legal persons

From the 90s many new articles were published in the legal literature which dealt with the criminal liability of legal persons. The hope for joining the European Union also brought the interest towards to this topic[8]. I would like the highlight the work of Sándor Fülöp. The title of his article is „The criminal legal subject of legal persons"[9].

According to Fülöp the individual responsibility can be hard to clarify. There are three reasons for this. First is the so-called problem of the bad network. Under this he

---

[2] See Laura Stănilă, *To punish or to torture? About inhuman treatment in the recent view of the Strassbourg Court*, in Journal of Eastern European Criminal Law Nr. 2/2017. pp. 257-261.

[3] E.Hacker, Op. cit. p. 118.

[4] E.Hacker, Op. cit. p. 124.

[5] E.Hacker, Op. cit. p. 127.

[6] E.Hacker, Op. cit. p. 118.

[7] E.Hacker, Op. cit. p. 136.

[8] See Laura Stănilă, *The legal person and the tax evasion offenses. From theory to practice,* in Journal of Eastern European Criminal Law Nr. *2/2015,* pp. 153-157.

[9] Sándor Fülöp, *A jogi személyek büntető jogalanyisága [The criminal legal subject of legal persons].* in Magyar Jog 1993/6. pp. 343-351.

means that due to the technical development of production units it is hard to define who is responsible for working and decision mechanism. It is very complicated and hard to control. Sometimes it is impossible to find the real person who was responsible for making the decision. The second problem comes in the case of the so called double omission. For example, environmental crimes (like polluting the air or water) can last for years. It is easier to hold responsible an organization. We can expect from the collective to know and follow the law. Fülöp says that we should follow the so called strict liability which is known in the English law. In this criminal procedure the prosecutor has to only prove the breach of an obligation by the defendant, but not the guiltiness in aspect of the result. Also we can mention here the possibility of a guilty plea which is a cost effective way of solving the case[10].

The civil law and administrative sanctions have low effectiveness. It is well known that the duration of the civil procedure can be delayed with several methods and it is also well known that many administrative sanction – such as fine – eventually are passed on the consumers by the corporations. Compared to these procedures the criminal procedures are relatively fast and a condemnatory verdict can cause great reputation or goodwill loss for the legal person[11].

The legal person can be immoral too and the morality of the legal person can be influenced by the criminal law[12]. The morality philosophy has a concept where they say that legal persons have similar morality levels as natural persons furthermore many urges – due to the abuses of many corporations – the collective legal entities for legal compliance with the criminal law which includes moral aspects[13].

Professor Mihály Tóth in his „Economic crimes and offenses"[14] titled monograph writes that „acknowledging the exceptional justifiability of the breakthrough of the principle of individual responsibility, I think the question can be solved through the acknowledgement of a „limited collective responsibility" having some criminal aspect mostly, but regulated independently on the basis of the following standpoints:

1. in case of an offence committed in the frame of an association we have to strive to define the individual responsibility with all means;
2. with or without it, against a legal person it is possible to apply sanctions ranked in the circle of subject and object defined clearly and precisely in law and listed there;
3. the prejudices are to be applied independently of guilt, considering the company's dangerous activity hurting financial interests and in proportion of this disadvantage; in my view the procedure should be regulated through special administrative proceedings, if possible ensuring the judicial way, guaranteeing the possibilities of excuse and legal remedy."

In the first decade of the 21th century two monographs were written solely about this topic: one from Ferenc Sántha[15] and one from Zsanett Fantoly[16].

---

[10] S.Fülöp, cited, p. 343.

[11] S.Fülöp, cited, p. 344.

[12] See László István Gál, *The criminal law protection of the stock market in Hungary*, in Journal of Eastern-European Criminal Law 2015.2. pp. 43-47.

[13] S.Fülöp, Op. cit. p. 344.

[14] Mihály Tóth, *Gazdasági bűnözés és bűncselekmények [Economic crime and offenses].* KJK-Kerszöv Jogi és Üzleti Kiadó Kft, Budapest 2000. pp. 46-47.

[15] Ferenc Sántha, *A jogi személyek büntetőjogi felelősségéről [About the criminal liability of legal persons].* KjK-Kerszöv Kiadó, Budapest. 2002.

[16] Zsanett Fantoly, *A jogi személyek büntetőjogi felelőssége [The criminal liability of legal persons].* HVG-Orac Kiadó, Budapest 2008.

According to Sántha the sanctions applied against organizations can be considered a special field. „The extension of criminal responsibility onto legal persons can only be justified if the legal behavior can be promoted and increased in this way..." theoretically the introduction of criminal responsibility has no sense if we cannot expect the increase of efficiency: if the criminal sanctions are not more effective than the administrative, civil legal consequences, they are useless in this field." In his opinion when forming the system of sanctions, the following must be considered: In accordance with the Hungarian criminal law penalties suggest guilt, so if we disregard the recognition of the special concept relating to the organizations guilt. These cannot be used against organizations. Thus the problem can be solved by means of either ranging the sanctions applicable against organizations with the circle of provisions or codifying a special, new type of criminal legal consequences. The criminal sanctions have to be clearly separated from the administrative sanctions... In the case of codifying the criminal responsibility of organizations it is more effective to form a system of sanctions consisting of more elements..."[17].

Zsanett Fantoly view is that we need to use criminal law measures against legal persons. The centre of the criminological examination of the criminal liability of legal person is the legal person's crime commitment. These crime consists of the criminal conducts committed for the benefit of the legal person or within the organizational structure and the cases where the legal entity is not the victim[18].

According to László Kőhalmi, The punishability of a legal entity is right regarding legal policy in that case if the commitment of the crime resulted in gaining property advantage in favour of the legal person and member or officer entitled acting or it was committed by its member/employee in the sphere of activity of legal person and the managing director or representative was aware of the crime[19].

IV. The regulation of criminal liability of legal persons in Hungary

1. General provisions

According to Professor Tóth[20] there are three forms of the criminal liability of legal persons in the practice in general:

- The so called objective liability of the organization. This is also called result liability.
- The second when the leader of the organizations takes responsibility,
- and the third liability system when the collective leadership will be held liable for the crime committed with the legal person.

These 3 systems can be combined. The Hungarian criminal law mostly follows the third option[21].

There are two important sources of law regarding criminal liability of legal persons in Hungary. On one hand the Criminal Code of Hungary (Act C of 2012) and on the other hand the Act on measures applicable to legal entities under criminal law (Act CIV of

---

[17] Ferenc Sántha, *A jogi személyekkel szemben alkalmazharó büntetőjogi jogkövetkezmények [Criminal legal consequences applicable against legal persons].* Jogtudományi Közlöny 2000/6. p. 240.

[18] Z.Fantoly, cited, p. 13.

[19] László Kőhalmi, *A jogi személyekkel szemben alkalmazható büntetőjogi intézkedések [The applicable criminal law measures against legal persons]* In: Jura 2006/1. p. 56.

[20] Mihály Tóth, *Az egyes jogkövetkezmények [The sanctions one by one].* in: Balogh Ágnes – Tóth Mihály (editors): Magyar Büntetőjog Általános rész. Osiris Kiadó, Budapest. 2015. p. 368.

[21] See Flóra Józan, László Kőhalmi: *Rule of Law and Criminal Law Thoughts about the criminal justice of the Millennium Era*. in Journal of Eastern-European Criminal Law 2017.1. p. 216.

2001). The Criminal Code only states in Chapter VIII that measures can be used against legal person and refers to the above mentioned separate Act which contains the detailed regulation. The Act CIV of 2001 came into effect in May 1st of 2004 when Hungary joined the European Union. The reason for draft of the law was the legal harmonization with the EU legislation.

Under the Act CIV of 2001 legal entities shall be understood as any organization or organizational units thereof vested with rights of individual representation, which the governing rules of law recognize as legal entities, as well as organizations that can be subject to conditions of civil law in their own right and possess assets distinct from that of their members, including companies active prior to registration pursuant to the Civil Code[22].

It is important to note that legal entities under the Hungarian criminal law can't

- be liable for a crime
- be perpetrators
- be sanctioned with penalties
- and finally can't commit an offense.

The measures can be only applied when someone (a natural person) committed an intentional crime under the Hungarian Criminal Code and a further condition is that the perpetration of such an act was aimed at or has resulted in the legal entity gaining benefit, and lastly the criminal act was committed by

- the legal entity's executive officer, its duly authorized member, employee, officer, managing clerk entitled to represent it, its supervisory board member and/or their representatives, within the legal entity's scope of activity,
- its member or employee within the legal entity's scope of activity, and it could have been prevented by the executive officer, the managing clerk or the supervisory board by fulfilling his or her or its supervisory or control obligations[23].

Other than these cases measures against legal entities shall be applicable even if committing the criminal act resulted in the legal entity gaining benefit, or the crime was committed with the use of the legal entity and the legal entity's executive officer, its member, employee, officer, managing clerk entitled to represent it, its supervisory board member, had a knowledge on the commission of the criminal act.

If these conditions are fulfilled the following measures can be applied:

1. winding up the legal entity,
2. limiting the activity of the legal entity,
3. imposing a fine.

According to Fantoly these sanctions are not within the criminal law. They are civil and administrative law type of sanctions applied by the criminal court on an objective basis. This is different than the traditional criminal law due the separate regulation[24].

Miklós Hollán – in his review[25] of Fantoly's monograph – opinion is that this statement is not well grounded. He thinks that the possible explanation for this statement is that the three above mentioned sanctions do not fit in the scientific definition of the criminal law sanction[26].

---

[22] Act CIV of 2001 Section (1) 1.

[23] Act CIV of 2001 Section 2 (1) a, b.

[24] Z. Fantoly, cited, p. 193.

[25] Miklós Hollán, *Új monográfia a jogi személyek büntetőjogi felelősségéről [New monograph on the criminal liability of legal persons].* in Magyar jog 2009/3. pp. 180-181.

[26] M. Hollán, *op. cit.*, p. 193.

2. Winding up the Legal Entity

There winding has two obligatory case and one facultative case.The court shall wind up the legal entity if, it is not running legal economic[27] activity and

- the legal entity was established for the purpose of covering up a criminal act, or
- the actual activity of the legal entity serves the purpose of covering up a criminal act.

The typical example[28] of these cases when they create a phantom firm or an offshore company and it is obvious in these cases that the court has no discretionary about the winding[29].

According to the facultative case the court may wind up the legal entity in the cases mentioned above even if, it is running legal economic activity. Even though the legal entity shall not be wound up in this case by the court if this would jeopardize the completion of state or local government tasks, or the legal entity

- is a national utility company,
- is considered to be of strategic importance in terms of the national economy,
- carries out national defense related or other special tasks or serves such purposes.

The winding up of the legal entity results in the dissolution of legal person without succession[30].

3. Limiting the activity of the legal entity

The court may limit the activities of the legal entity for one to three years.The duration shall be defined in years. Limitation may extend to the pursuit of all or some of the activities listed. For the duration of the prohibition, the legal entity shall not

- collect deposits based on a public invitation,
- participate in public procurement procedures,
- enter into concession contracts,
- be classified as a public benefit organization,
- receive funding from central or local government budgets, earmarked state funds or targeted support from foreign states, the European Community or other international organizations,
- pursue any other activities, which have been prohibited by the court.

In case the activity is limited, the following shall prevail on the date the court judgment becomes final, subject to the provisions of the court:

- the legal consequences of immediate rescission of contract concluded with legal entity under public procurement procedure,
- the legal consequences of immediate rescission of concession contract concluded with legal entity,
- the procedure involving classification as a public benefit organization is considered terminated, and the legal entity is considered deleted from the registry of public benefit organizations,

---

[27] See László István Gál *Economic Bribery as a Part of Economic Criminal Law and a Concomitant of Political Corruption*. Journal of Eastern-European Criminal Law 2014.1., pp. 22-25.

[28] See Csaba Szilovics: *About the causes of corruption in the hungarian public procurement system*. in: Journal of Eastern-European Criminal Law 2014.2., pp. 101-103.

[29] M. Tóth, cited, 2015. p. 370.

[30] Miklós Hollán, *Az intézkedések [The measures].* In: Kis Norbert – Hollán Miklós, Büntetőjog I. Általános rész. Dialóg Campus Kiadó, Budapest. 2013, p. 335.

- the procedure involving the granting of subsidies under paragraph (2) point e) is considered terminated, and any subsidy received in conjunction with the criminal act shall be repaid.

4. Imposing a fine

Fine is a pecuniary sanction and within that is a payment obligation. The highest fine that can be imposed on the legal entity shall be three times the financial advantage gained or intended to be gained through the criminal act, but at least 500,000 Hungarian Forints. The Court may estimate the rate of the financial advantage if the financial advantage gained or intended to be gained could only be established at unreasonably high cost or not at all.

If the benefit gained or intended to be gained through the criminal act is not financial advantage, the court imposes the fine considering the financial situation of the legal entity, but at least HUF 500,000 (Which is around 1609 Euros when the article was written). The fine is recovered according to the rules of the court order in the case the fine is not paid.

V. Compliance of the Hungarian regulation to the EU legislation.

The European Union requires from the Member States to ensure the possibility of sanctioning legal persons involved crimes. Many EU legal sources (directives and council framework) contains the criminal liability of legal persons with very similar regulation. The regulated crime types are such as:

1. Counterfeiting;
2. Fraud and counterfeiting non-cash means of payment;
3. Environmental offenses etc.

In my current study I will compare the Hungarian regulation with the Directive[31] regarding counterfeiting for as an example.

The Directive prescribes that the Member States shall take the necessary measures to ensure that legal persons can be held liable for the counterfeiting offences committed for their benefit by any person acting either individually or as part of an organ of the legal person who has a leading position within the legal person based on

- 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[32].

The Directive also requires from the Member States that to ensure that the legal person can be held liable where the lack of supervision or control by a person… has made possible the commission of an offence… for the benefit of that legal person by a person under its authority[33].

It is also important to note that the liability of a legal person shall not exclude criminal proceedings against natural persons who are perpetrators, instigators or accessories in the counterfeiting offences[34].

---

[31] Directive 2014/62/EU Of The European Parliament and of the Council of 15 May 2014 on the protection of the euro and other currencies against counterfeiting by criminal law, and replacing Council Framework Decision 2000/383/JHA.

[32] Directive article 6. 1.

[33] Directive article 6. 2.

[34] Directive article 6. 3.

As for the sanctions against legal entities the Directive prescribes that Member States shall take the necessary measures to ensure that a legal person held liable with effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines. The Directive also contains facultative sanctions with examples like:

- exclusion from entitlement to public benefits or aid;
- temporary or permanent disqualification from the practice of commercial activities;
- placing under judicial supervision;
- judicial winding-up;
- temporary or permanent closure of establishments which have been used for committing the offence[35].

The Hungarian regulation complies with the EU Directive in both aspects. Firstly it gives the option to sanction legal persons. Secondly the Hungarian regulation contains the one compulsory sanction: fine. The sanctions contained in the legal sources are summarized in the following table:

The Hungarian regulation (Act CIV of 2001)	**The EU Directive on counterfeiting currency (2014/62/EU)**
imposing a fine.	criminal or non-criminal fines (compulsory)
winding up the legal entity,	judicial winding-up (facultative)
limiting the activity of the legal entity,	temporary or permanent disqualification from the practice of commercial activities (facultative)
	exclusion from entitlement to public benefits or aid (facultative)
	placing under judicial supervision (facultative)
	temporary or permanent closure of establishments which have been used for committing the offence. (facultative)

In my opinion the Hungarian regulation should have more sanctions than the existing ones so the courts have more discretionary in these cases. All of the facultative sanctions should be considered in the future legislation.

VI. The Szegedi Paprika case and statistics

Since the criminal law measures were introduced there were not many cases where the legal persons were actually sanctioned. The following table contains the statistic[36] where the prosecutor office proposed sanction against legal persons from 2007 to 2013:

[35] Directive article 7.

[36] http://kimittud.atlatszo.hu/request/2642/response/4308/attach/3/attachment2.pdf (accessed on 30.10.2017).

	In the indictment the prosecutor proposed criminal law measures against legal persons						
	2007	***2008***	***2009***	***2010***	***2011***	***2012***	***2013***
Total Number	1	6	6	8	4	4	8

The next table[37] consists the yearly numbers where the court decided to sanction the legal person from 2007 to 2013:

	The court applied a criminal law measure against legal persons in the conviction						
	2007	***2008***	***2009***	***2010***	***2011***	***2012***	***2013***
Number of convictions	0	3	1	1	0	3	2

We can conclude from the figures that the numbers are very low it is almost close to non-existent statistically.

Until the essay was written one of the most famous of these few cases was the Szegedi Paprika case.

The case[38] can be summed up as the following. The accused natural persons of the case were convicted of misuse of harmful consumer goods and was awarded with a fine penalty. The legal person was also fined by 15 million Forints by the Szegedi Törvényszék (Szeged Regional Court). The crime can be accomplished when a person who prepares or possesses any consumer goods for the purpose of distribution that is harmful to health.

As legal persons the main actors of the case were the Szegedi Paprika firm and the Kotányi GmBH firm. These two firms were in a business relationship. The Kotányi GmBH bought 20 ton of spicy pepper (paprika) from the Szegedi Paprika firm in 2004. The paprika contained more than 5 micrograms per kilogram aflatoxin which is a poisonous carcinogen that are produced by certain molds. This number exceeded the permissible level and can be harmful to humans when its consumed. The Kotányi GmBH noticed this to Szegedi Paprika and the assistant from it transmitted these to the Quaility Control Department. The Department confirmed this claim and reported this to the company leaders as well. They bought back the 20 ton of spicy pepper and after that they sold more than 3.5 ton of these as gourmet meal. They also sold the other parts of the paprika as so called diluted meal.

The accused natural persons, the leaders of the Szegedi Paprika firm decided over the resale of the spicy pepper. With this decision they put back harmful to human health goods on the market.

The Szegedi Paprika firm also gave a deceptive information about the origin of the spicy pepper and they were not allowed to use the label „Szegedi" which means from the

[37] http://kimittud.atlatszo.hu/request/2642/response/4308/attach/3/attachment2.pdf (accessed on 30.10.2017).

[38] http://szegeditorvenyszek.birosag.hu/targyalasi-jegyzek/20140616/artalmas-kozfogyasztasi-cikkel-visszaeles-buntette-es-mas-buncselekmeny (accessed on 30.10.2017).

Hungarian city of Szeged due to the fact that most of the spicy pepper were from Spain. It was solely an imported good. In some goods they also labelled with a trademark as „Perfect Hungarian Food" or „Grand Prize Winning Hungarian Product" which was also misleading.

The second instance court increased the sanctions compared to the first instance court due to the crime dangerous nature and the accused personal circumstances.

VI. Summary and conclusions

According to Professor Tóth[39] the obligatory conditions for applying criminal law measures against legal persons are:

1. the crime committed with intent.
2. The criminal act resulted or aimed to gain assets for the legal person or was committed with the legal person or with the use of the legal person.
3. A natural person was liable for the crime. or the offender was not (or not yet) identified.
4. Not the accused or suspected committed the crime or this cannot be declared.
5. The offender could not hold liable due to death; or his or her mental disorder; or clemency, or duress or threat.
6. The procedure was suspended due to absence sickness.

Facultative conditions:

1. the leader committed the crime as the leader of organization or as operative a member committed the crime and the offender could be stopped by the leader.
2. An outsider (*extraneus*) committed the crime for assets and the leader know about.

The possible measures:

1. winding up the legal entity,
2. limiting the activity of the legal entity,
3. imposing a fine.

The criminal legislature and the science of criminal law had long fights and debates and possibly there will be more in the future to improve the legislation.

Overall the Hungarian regulation complies with the EU legislation by giving the option of sanctioning and containing the sanction of fine.

References

1. Fantoly, Z., *A jogi személyek büntetőjogi felelőssége* [The criminal liability of legal persons]. HVG-Orac Kiadó, Budapest 2008.
2. Fülöp, S., *A jogi személyek büntető jogalanyisága* [The criminal legal subject of legal persons]. Magyar Jog 1993/6.
3. Gál, L.I., *The criminal law protection of the stock market in Hungary.* Journal of Eastern-European Criminal Law 2015.2. Hacker, E., *Az egyesületek büntetőjogi cselekvőképessége és felelőssége - Tanulmány az anyagi büntetőjog köréből* [The associations capacity and criminal liability – Study within the substantive criminal law]. Grill Cs. és Kir. Udvari könyvkereskedése, Pécs. 1922.
4. Gál, L.I., *Economic Bribery as a Part of Economic Criminal Law and a Concomitant of Political Corruption*. Journal of Eastern-European Criminal Law 2014.1.

[39] M.Tóth, cited, 2015. pp. 368-369.

5. Hollán, M., *Az intézkedések* [The measures]. In: Kis Norbert – Hollán Miklós, Büntetőjog I. Általános rész. Dialóg Campus Kiadó, Budapest. 2013.

6. Hollán, M., *Új monográfia a jogi személyek büntetőjogi felelősségéről* [New monograph on the criminal liability of legal persons]. Magyar jog 2009/3.

7. Józan, F., Kőhalmi, L., *Rule of Law and Criminal Law Thoughts about the criminal justice of the Millennium Era.* Journal of Eastern-European Criminal Law 2017.1.

8. Kőhalmi, L., *A jogi személyekkel szemben alkalmazható büntetőjogi intézkedések* [The applicable criminal law measures against legal persons]. Jura 2006/1.

9. Sántha, F., *A jogi személyek büntetőjogi felelősségéről* [About the criminal liability of legal persons]. KjK-Kerszöv Kiadó, Budapest. 2002.

10. Sántha, F., *A jogi személyekkel szemben alkalmazharó büntetőjogi jogkövetkezmények* [Criminal legal consequences applicable against legal persons]. Jogtudományi Közlöny 2000/6.

11. Stănilă, L., *The legal person and the tax evasion offenses. From theory to practice*, Journal of Eastern European Criminal Law Nr. 2/2015.

12. Stănilă, L., *To punish or to torture? About inhuman treatment in the recent view of the Strassbourg Court*, in Journal of Eastern European Criminal Law Nr. 2/2017.

13. Szilovics, C., *About the causes of corruption in the hungarian public procurement system.* Journal of Eastern-European Criminal Law 2014.2.

14. Tóth, M., *Az egyes jogkövetkezmények* [The sanctions one by one]. In: Balogh Ágnes – Tóth Mihály (editors): Magyar Büntetőjog Általános rész. Osiris Kiadó, Budapest. 2015.

15. Tóth, M., *Gazdasági bűnözés és bűncselekmények* [Economic crime and offenses]. KJK-Kerszöv Jogi és Üzleti Kiadó Kft, Budapest. 2000.

The relationship between *Habeas Corpus* and robot technology in criminal proceedings

PhD Balázs Elek[1]
Associate professor
Debrecen University
Faculty of Law Abstract

Abstract

In law enforcement activities, the most common restriction on fundamental rights is the limitation on personal freedom – that is, the apprehension and preliminary detention of suspects. With developments in technology, it is conceivable that robots will be able to carry out these measures instead of (or alongside) human beings in the near future. The question is: Is it legally or technologically feasible for robots to assume the role of police patrols in the coming decades?

There is no legal dogma that prevents the use of robots to apprehend people, since there are already numerous examples of machines or installations carrying out activities that have the effect of limiting personal liberty, even without human intervention.

Keywords: *fundamental rights, robot, habeas corpus, arrest, criminal procedure, European Court of Human Rights, robotic cop car, War on Terror*

I. Introduction

Habeas corpus proceedings are generally understood to be cases in which an individual in custody files an urgent petition to a court with the aim of obtaining his release[2]. The principle is closely related to the accused party's right to a hearing before the bench and right to judicial review. The law on criminal procedure seeks to ensure that the accused shall be detained exclusively within the framework of an adversarial process. During the investigation, the investigating judge makes the decision; during the preparatory phase, this can only be accomplished at a hearing at which the defendant is present[3].

However, questions about the restriction of personal freedom go much further in the present day. The time may be ripe to ask whether the apprehension and detention of suspects during enforcement activities can be performed by robots rather than humans[4]. We already take it for granted that traffic lights and automatic gates restrict our freedom of movement. In Hungarian law, the codification of rules on legal

---

[1] President of the Chamber, consultant on European law, Debrecen Court of Appeals; Department head, associate professor, University of Debrecen Faculty of Law.

[2] László Blutman (1993), *„A fogvatartás bírói felülvizsgálata: a habeas corpus az európai alapjogok között"* („Judicial Review of Detention: *Habeas Corpus* Among European Fundamental Rights"), *Jogtudományi Közlöny*, August-September 1993, pp. 309-317.

[3] Law XIX (1998) on criminal procedures, Article 210 §(1)a, Article 272 §(2)a

[4] Zoltán Székely (2014), *„Habeas Corpus Machinima. Avagy elfoghat-e engem egy robot?"* (*Habeas Corpus Machinima*; or, Can a Robot Arrest Me?") *Hadmérnök*, IX(1) (March 2014), pp. 291- 303.

preventive defense has opened the possibility for the apprehension of unlawful attackers through automatic installations.

In law enforcement activities, the most common restriction on fundamental rights is the limitation on personal freedom – that is, the apprehension and preliminary detention of suspects. With developments in technology, it is conceivable that robots will be able to carry out these measures instead of (or alongside) human beings in the near future. The question is: Is it legally or technologically feasible for robots to assume the role of police patrols in the coming decades[5]? Furthermore, how might an individual who is arrested or detained by robots exercise his right to a court hearing on the legality of his arrest?

„The basics of robotics are one of the rare subjects to be handled as a whole in a due to the extreme diversity of scientific technologies it incorporates. It uses quite many fields of technology, for example; mechanical engineering, electrical engineering, computer sciences, electronics, sensors, actuators and artificial intelligent. It is a multidimensional area which takes advantage of all engineering studies that exist in our life besides a hard mathematical module application which is required to be applied"[6].

In years, maybe decades, the officer could be replaced by a robotic cop car. The robot will scan the driver's license, decide whether to issue a warning or ticket, and inform of its decision[7].

II. The origins of the principle of *habeas corpus*

Habeas Corpus is a legal principle that derives from English law. *„The writ of habeas corpus has its origins in the early common law courts of medieval England. Some legal historians have found a reference to the writ in Article 39 of the Magna Carta, which in 1215 provided that 'no Freman shall be taken, or imprisoned…but by lawful Judgement of his Peers, or by lawful Judgement of his Peers, or by the Law of the Land.' Whether this refers to the writ of habeas corpus (or something like it) is disputed, but the prohibition against unlawful imprisonment or detention has always been at the heart of the writ"*[8].

Habeas corpus is the greatest safeguard of personal freedom, guaranteeing that an individual can only be deprived of liberty for a short period of time unless he is formally charged or arraigned before a judge. The principle first appeared in the 13th Century as a means of preventing the arbitrary restriction of personal freedom during the war between England's barons and the king. An individual detained at the king's behest could receive a writ of *habeas corpus* from a judge, which would then be handed to the arresting authorities. In this manner, the detainee could demand that the authorities disclose the reasons for his arrest, grant him a court hearing and allow a judge to review the legality of the arrest. By sending back the writ, the authorities would confirm that they had fulfilled these conditions. The development of the *habeas corpus* principle

---

[5] Zoltán Székely (2014), *„Habeas Corpus Machinima. Avagy elfoghat-e engem egy robot?"* (*Habeas Corpus Machinima*; or, Can a Robot Arrest Me?") *Hadmérnök*, IX(1) (March 2014), pp. 291- 303

[6] Lahden Ammattikorkeakoulu Tekniikan ala Kone – ja tuotantotekniikka Mekatroniikka Opinnaytetyö Syksy 2011 Fareed Shakhatreh (Lahty University of Applied Siences). https://www.theseus.fi/bitstream/handle/10024/37806/Shakhatreh_Fareed.pdf?sequence=2.

[7] Steven Nelson, *Are robot cops the future of efficient, bias-free policing?* February 06, 2018.

[8] James Landman, *You Should Have the Body Understanding habeas Corpus.* Social Education 77(2) pp 92-105, 2008 National Council for the Social Studies, https://www.americanbar.org/content/dam/aba/images/public_education/05_mar08_habeascorpus_landman.pdf.

covers several important milestones, including the prohibition on arbitrary detention enshrined in the Magna Carta[9].

The very first written source of law in Hungary, the Golden Bull, shows that the Hungarian legal system was developing in parallel to that of England. Proclaimed in 1222 by King András II, this document qualifies the detention of suspects as the most basic restriction on the individual right to liberty. According to Ferdinandy, the Golden Bull represents „the basic code of personal freedom in Hungarian public law" since it mandates the state to respect the individual and, by extension, personal freedom[10]. The Bull deals with arrest and detention in Article II: „We also desire that neither [the current monarchy] nor any king that succeeds us shall arbitrarily arrest or oppress any nobleman unless he is previously convicted in a court of law and through proper procedure".

In Anglo-Saxon law, the most critical juncture in the development of the *habeas corpus* principle occurred during the era of the English Civil War. In 1627, Parliament issued a Petition of Rights in response to legal violations by the King's Bench, the supreme royal court. It stipulated that a free person could only be deprived of liberty through formal charges and lawful proceedings, not by royal decree. At first, King Charles I deemed the Petition to be a violation of his royal prerogative, but Parliament forced the monarch's hand by refusing to pass tax legislation until he signed it. On 28 July 1628 Charles I approved the Petition, which stated that nobody should be subject to arrest by royal order in the absence of a clear reason for the arrest and formal charges[11].

The struggle between the monarch and Parliament continued. According to the Habeas Corpus Act of 1640, every arrested individual would have the right to submit a writ. However, this institution was swept away by the ensuing English Civil War. During the reign of King Charles II, Parliament passed the Habeas Corpus Act of 1679, which required the court to issue an order based upon a written complaint or petition submitted by the individual in custody (or on his behalf). This order enjoined the arresting authority to disclose the time of the detention and the reason for it; to grant the detained individual a court hearing; and to fulfill the provisions of the judge's ruling. The Habeas Corpus Act of 1679 expressly addresses the requirement to bring the arrested individual's „body" before a magistrate[12]. At the order of a judge, the prison warden had to produce a report that spelled out the reasons for the detention as well as a certification that he would bodily release the imprisoned person[13]. The Latin term *habeas corpus* literally means „that you have a body". It implies that authorities are required to „bodily" produce a detained person or bring him before a judge. Ultimately, a *habeas corpus* order is a written legal formula that makes it possible to examine whether an individual's detention is legitimate.

The British Habeas Corpus Act of 1816 extended these legal guarantees to all types of deprivations of liberty – not just those pertaining to criminal cases.

---

[9] Barna Mezey (2015), *„A Runnymede-i carta, 1215"* („The Carta of Runnymede, 1215"), *Ügyvédek Lapja*, 2015/3, pp. 2-6.

[10] Gejza Ferdinandy (1899), *Az arany bulla* (*The Golden Bull*), Hungarian Academy of Sciences, Budapest, p. 169.

[11] Lajos Hajdú, Pál Horváth, József Ijjas, Katalin Szegvári Nagy, János Zlinszky, István Stipta (1991), *Általános Jogtörténet* (*General History of Law*), Tankönyvkiadó, Budapest, pp. 178-180.

[12] János Poór (ed.) (2000), *Kora újkori egyetemes történeti szöveggyűjtemény* (*Early Modern Universal Historical Document Collection*), Osiris Kiadó, Budapest, pp. 87-88.

[13] Lajos Hajdú, Pál Horváth, József Ijjas, Katalin Szegvári Nagy, János Zlinszky, István Stipta (1991), *Általános Jogtörténet* (*General History of Law*), Tankönyvkiadó, Budapest, p. 179.

The principle later underwent additional developments. The United States of America's Declaration of Independence cites British authorities' violations of the *habeas corpus* principle as one of the root causes of the War of Independence. The US Constitution as well as American legal practice place great emphasis on upholding and defending this principle. *Habeas corpus* was a cornerstone of legal challenges to the George W. Bush administration's policy of detaining prisoners without trial at the Guantánamo Bay military base during the War on Terror. In 2006, Congress passed the Military Commissions Act, which denied „enemy combatants" the right to use *habeas corpus* to challenge their detention in federal courts, including the Supreme Court. However, a majority of Supreme Court justices opined that denying a prisoner the right to a *habeas corpus* review was, in fact, a violation of the constitutional principle of separation of powers. If the president and Congress can decide whether the Constitution applies in a given area of law, then ultimately it is not the judiciary, but the executive and legislative branches that interpret the Constitution. Writing for the majority, Justice Anthony Kennedy affirmed that the Constitution extends the right of *habeas corpus* petitions to Guantánamo prisoners. In other words, these detainees would be able to mount legal challenges to the state's decision to restrict their liberty, the Military Commissions Act notwithstanding[14].

It is worth mentioning that the 1789 Declaration of the Rights of Man and of the Citizen also codified *habeas corpus.* The Universal Declaration of Human Rights, adopted in 1948 by the United Nations, makes the principle mandatory. *Habeas corpus* also constitutes a significant part of the European Convention on Human Rights, signed on 4 November 1950 in Rome with the aim of defending human rights and fundamental freedoms.

Article 5 of the Convention lists the circumstances under which it is possible to deprive an individual of liberty. The Convention not only details the scope of circumstances, it also discusses the most important procedural necessities, such as the requirement that court proceedings be overseen by a judge. An arrested or detained individual must, with all deliberate speed, appear before a judge or other public official who is legally vested with commensurate powers. Throughout the period of arrest or detention, every individual who is deprived of liberty has the right to a hearing during which the court will decide on the legality of the detention; in case of unlawful detention, the court will order the petitioner released[15].

---

[14] Orsolya Salát (2008), *„Az Egyesült Államok Legfelső Bíróságának döntéseiből"* („From the Decisions of the Supreme Court of the United States"), *Fundamentum*, 2008/3, pp. 101-104.

[15] Hungarian Act XXXI of 1993, the Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, Rome; *Article 5, Right to Liberty and Security*

„1. Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law:

(a) the lawful detention of a person after conviction by a competent court;

(b) the lawful arrest or detention of a person for non- compliance with the lawful order of a court or in order to secure the fulfilment of any obligation prescribed by law;

(c) the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so;

(d) the detention of a minor by lawful order for the purpose of educational supervision or his lawful detention for the purpose of bringing him before the competent legal authority;

(e) the lawful detention of persons for the prevention of the spreading of infectious diseases, of persons of unsound mind, alcoholics or drug addicts or vagrants;

The Convention's clause on arrests is supplemented by other recommendations. These include Resolution 11 (1965) of the Council of Europe's Committee of Ministers, which suggests that detention of suspects should not be an automatic requirement, but rather a decision made by a court of law following an examination of the facts and circumstances of the particular case. Arrest should be regarded as an exceptional measure that can be ordered and sustained only when absolutely necessary.

III. Constitutional considerations in Hungarian *habeas corpus* proceedings

Hungarian procedures on the restriction of personal liberty also use the technical term *habeas corpus.* This is particularly notable in the practice of the Constitutional Court. Preliminary detention, orders of house arrest and extensions thereof are all known as „*habeas corpus*-related procedures"[16]. The Constitutional Court determined that §55 of the Constitution guarantees the right to freedom and personal security: „This provision is the Constitution's *habeas corpus* rule, which states that nobody can be deprived of liberty except when such action is based upon legally determined reasons and court proceedings, and the individual must be brought before a judge as speedily as possible"[17].

In constitutional democracies, special enforcement provisions or legal remedies apply in the case of healthcare or medical operations that might result in a restriction of, or a clear threat to, fundamental rights. Special *habeas corpus* procedures apply in the case of mental patients who pose a threat to themselves or others and are therefore committed to mandatory psychiatric treatment. The court must order the treatment or review its rationale in an expedited process[18].

Naturally, a good part of the Hungarian Constitutional Court's rulings took shape before the current constitution, known as the Fundamental Law (*Alaptörveny*), went into force in 2012. But the Fundamental Law has generally preserved the previous rules on *habeas corpus.*

The Fundamental Law's Article 4(2) constitutionally mandates that a person can be deprived of liberty only through legal procedures. Article 4(3) of the Fundamental Law states, „Any person suspected of having committed a criminal offense and taken into detention shall, as soon as possible, be released or brought before a court. The court shall be obliged to hear the person brought before it and shall forthwith take a decision

---

(f) the lawful arrest or detention of a person to prevent his effecting an unauthorized entry into the country or of a person against whom action is being taken with a view to deportation or extradition.

2. Everyone who is arrested shall be informed promptly, in a language which he understands, of the reasons for his arrest and of any charge against him.

3. Everyone arrested or detained in accordance with the provisions of paragraph 1 (c) of this Article shall be brought promptly before a judge or other officer authorized by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release pending trial. Release may be conditioned by guarantees to appear for trial.

4. Everyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful.

5. Everyone who has been the victim of arrest or detention in contravention of the provisions of this Article shall have an enforceable right to compensation."

[16] Constitutional Court decision 166/2011 (XII. 20)

[17] Constitutional Court decision 67/2011 (VIII. 31)

[18] Constitutional Court decision 39/2007 (VI. 20)

with a written reasoning to release or to arrest that person." This is a word-for-word duplication of the corresponding passage in the old constitution.

The text of the Fundamental Law's Article 4(2) is similar to that of Articles 5(1) and 5(3) of the European Convention on Human Rights. With respect to coercive measures, the Constitutional Court decided that the rules of the constitution and the Fundamental Law should be interpreted in harmony with the European Convention on Human Rights.

In line with Article 46(1) of the Convention, Hungary considers any final judgment by the Strasbourg-based European Court of Human Rights (ECtHR) binding in cases to which is it a party. In other words, Hungary, as a signatory to the Convention, is only required to eliminate legal violations in cases where the Court establishes a violation of the Convention. During a judicial review, Hungary's highest court, the Kúria, stressed that „although Hungarian law (Law XXXI/1993) promulgates the provisions of the European Convention on Human Rights, and the ECtHR's interpretation of the Convention's provisions takes precedence over all others, the principle of subsidiarity remains unrealized in signatories' judicial practice. The signatory states do not directly apply the judgments of the ECtHR. When domestic norms are at variance with the Convention, the courts disregard the Convention's provisions, even though the sources of law (our domestic laws) are on the same level"[19].

The Constitutional Court regularly cites the ECtHR's practice as confirmatory arguments in the explanations that accompany its rullings.

IV. The European Court of Human Right's Practice with Respect to the System of Guarantees with Respect to Coercive Measures

The European Court of Human rights has, in numerous judgments, addressed the legality of detention in light of the guarantee of due process enshrined in Article 5 of the European Convention on Human Rights.

In harmony with the provisions Article 5 (1c), every person who is arrested or detained must be brought promptly before a judge (or other public officer authorized by law to exercise judicial power); the arrested or detained individual has a right to a hearing on his case within a reasonable amount of time, or must be released until the hearing takes place. His release must take place under conditions that will guarantee his appearance at the hearing.

The European Court of Human Rights has held that under Article 5 (1c), the goal of the hearing that takes place during detention is to supplement the criminal investigation with data that confirms or refutes the reasons for the arrest. (*Murray v. the United Kingdom*, judgment of 28 October 1994, §55-56). The European Court of Human rights listed these same criteria in §53 of its judgment in the case of *Goussinski v. Russia* on 19 May 2004.

According to the European Court of Human Rights, the system of guarantees with respect to detention and arrest rests upon on three conditions: The action should be prompt, should be automatic, and should be handled by an independent judicial body that is authorized to release individuals from custody. (Judgment in the case of *Zervudacki v. France* of 27 July 2006, §33-35)[20]. In *Zervudacki*, the Strasbourg court also

[19] Kúria Bfv.II.1812/2014/18. In this case the Chief Prosecutor's Office argued that a motion by the defense counsel inaccurately stated that all ECtHR decisions were binding upon Hungary.

[20] Constitutional Court Decision 3/2007 (II/13), in an accompanying explanatory statement by Constitutional Court Judge Dr. Péter Kovács.

established a violation of Article 5(3) of the Convention because the petitioner (who was later sentenced to 18 years and nine months in prison) was not brought promptly before a judge or other public official legally vested with judicial powers following his detention[21].

In *Gábor Nagy v. Hungary* (2014), the European Court of Human Rights ruled that „in the present case, the Court is not persuaded that the applicant was heard as to the justification of his detention at reasonable intervals, all the more so since his request for release was adjudged in solely written procedure. In particular, the period of some four months cannot be regarded as a reasonable interval"[22].

It is especially worthwhile to mention that, in the Strasbourg court's practice, a particularly important part of the system of guarantees regarding coercive measures is the detailed completion of the justification for legal action[23]. The explanatory statement must take experiences into account. This can perhaps be illustrated in cases where it is not possible to launch new proceedings against a given individual due to the principle of *ne bis in idem*, hence it is impossible to apply coercive measures if another European country has already held the accused person responsible for the same act[24]. When databases are not readily available and information is incomplete, it is sometimes only possible to shed light on this during a hearing where the accused is present.

V. The Right to a Hearing in Relation to Coercive Measures

In a 2007 ruling, the Constitutional Court struck down certain provisions of Hungary's law on criminal procedures (Act XIX of 1998) on grounds that they were unconstitutional and incompatible with the right to a fair trial. These rules made it possible to order a defendant's arrest in his absence and without a court hearing.

The Constitutional Court's ruling, which examined the constitutionality of procedural requirements applicable to investigating judges, used the Strasbourg court's practice as a starting point. Under Article 5(3) of the Convention, the requirements are fulfilled „if the judge (or other officer authorized by law to exercise judicial power) grants the detained individual a hearing; and, when it is necessary to review the circumstances militating for or against detention, decides whether there are reasons to justify detention; and, if there are no such reasons, to order the accused released." (*Schiesser v. Switzerland*, 4 December 1979, §31)"[25] The European Court of Human Rights stuck to this test in the following decades, stressing the importance of these

---

[21] Ágnes Czine, Sándor Szabó, József Villányi, p. 255: Judgment in the case of *Soysal v. Turkey*, 3 May 2007, petition no. 50091/99.

[22] *Gábor Nagy v. Hungary* (2014); *Erisen and Others v. Turkey*, no. 7067/06, § 51, 3 April 2012

[23] See the European Court of Human Rights judgment in *Hunvald v. Hungary,* petition no. 68435/10, 10 December 2013, and the European Court of Human Rights judgment in *Maglódi v. Hungary*, petition no. 30103/02, Strasbourg 2004.

[24] Marek Kordik (2011), *„Ne bis in idem: The role of national criminal law in the European Union area and the alternative resolutions of criminal procedure,"* Collection of Papers from the International Scholastic Conference Law as a Unifying Factor of Europe – Jurisprudence and Practice, Comenius University Faculty of Law, Bratislava, pp. 221-226.

[25] Constitutional Court ruling 166/2011 (XII/20) [For the supporting theses from *Schiesser v. Switzerland*, see *Assenov v. Bulgária*, October 28, 1998, §146-149; *McKay v. United Kingdom*; *Medvedyev and others v. France* (Main Chamber), §119 and §124; *Moulin v. France*, §57-58.] For the Schiesser case, see Vincent Berger (1999), *Az Emberi Jogok Európai Bíróságának Joggyakorlata* (*The Legal Practice of the European Court of Human Rights*), Budapest, Károly Tóth (ed.), ISBN 963 03 811192.

judicial guarantees, even if the expectations under Article 5(4) are not the same as under Article 6(1) (Judgment in *Wesolowski v. Poland,* 22 September 2004, §60). At such times, a hearing is indispensable (Judgment in *Kampanis v. Greece,* 13 July 1995, §47) and it is generally necessary to ensure that both sides – that is, the prosecutor and the arrested person – possess „equal firepower." (Judgment in *Wesolowski v. Poland,* 22 September 2004, §61). „Equal firepower" means the state is required to provide the complainant the opportunity to appear at the same time as the prosecutor so that the complainant can reflect upon his conclusions. (Judgment in *Wesolowski v. Poland,* 22 September 2004, §66)[26].

In several cases the Constitutional Court has examined the regulations surrounding coercive measures in the case of misdemeanours. The contents of these rulings can also offer direction in criminal proceedings, since the two types of procedures are similar in many ways. The responsibility for both misdemeanour violations and criminal offenses is the perpetrator's subjective, guilt-based responsibility, which the state may punish with retaliatory, repressive sanctions, including deprivation of liberty. The difference between misdemeanour and criminal responsibility does not lie in the repressive nature of the punishment, but in the fact that punishments for misdemeanours are less severe. Responsibility for misdemeanour offenses – whether the violations are administrative or criminal in nature – is in essence criminal responsibility: It corresponds to a violation of law committed by a natural person, and, based upon culpability, authorities apply a defined legal sanction that is repressive in nature[27].

Although misdemeanour procedures significantly differ from criminal procedures, they are related in terms of content. Misdemeanour cases are simpler and do not fully include the fundamental principles of criminal procedures. It is not possible to draw a parallel between criminal and misdemeanour cases in terms of gravity, danger to society, or system of sanctions. Misdemeanours cannot be handled with the same considerations or with the same legal guarantees that apply in criminal procedures[28]. At the same time, the Constitutional Court has held – in line with the practice of the European Court of Human Rights – that due to the criminal character of misdemeanour proceedings, misdemeanour trials must also meet the requirements that apply to criminal proceedings, as spelled out in the constitution[29].

The Constitutional Court struck down part of a law on misdemeanours specifically because it did not include the right to a court hearing in cases where a perpetrator was sentenced to imprisonment because he was unwilling or unable to pay a monetary fine. The Constitutional Court held that a fine could only be transmuted into loss of liberty after the perpetrator had been granted a hearing[30]. A hearing for the perpetrator is indispensable; without it, a procedure directed at the temporary deprivation of personal freedom cannot be fair. The restriction on personal liberty is based upon the court's ruling on transmuting the punishment. No fine for an administrative offense, no order to perform public service in lieu of a fine, and no on-the-spot fine can serve as a basis for

---

[26] Constitutional Court ruling 1/2008 (I/11), separate opinion by Constitutional Court Judge Dr. Péter Kovács.

[27] Constitutional Court ruling 1/2008 (I/11), ABh1., ABH 1997, 371., Constitutional Court ruling 1/2008. (I/11).

[28] Constitutional Court ruling 3/2007 (II/13) 1284/B/1990, ABH 1991, 562, 563-564.

[29] Constitutional Court ruling 63/1997 (XII/12), ABH 1997, 365, 368-369.

[30] 1/2008. (I. 11.) AB határozat.

the restriction of personal freedom. This only can occur by virtue of a court decision. The court cannot hand down such a decision without first granting the subject a hearing (i.e. without a trial); otherwise, the court cannot possibly conduct a fair procedure that truly examines the legal conditions for applying imprisonment. Since the restriction of liberty touches on a fundamental right, it can only be put into practice constitutionally if the court gives the perpetrator a hearing. In these questions, the Constitutional Court stressed that there is a significant difference between transmuting a monetary fine for a misdemeanour into imprisonment and taking the same action with respect to a fine imposed for a criminal act: In the case of a criminal act, the establishment of facts (and the assessment of responsibility that rests thereupon) is carried out by an official judge, not by an administrative authority or judicial employee (court secretary.)

All this highlights another significant difference that arises during the various phases of the procedure in relation to coercive measures that deprive a person of freedom. The vast majority of the Strasbourg cases are related to preliminary-arrest orders stemming from an established suspicion. The procedural-law situation is different if an order of preliminary arrest is determined to be necessary in a first-instance proceeding; a still different situation arises if a court of first instance takes a position on the question of a defendant's guilt and establishes proof thereof, and the second-instance court issues an order for coercive measures.

VI. The Subjects of Arrest and Preliminary Detention in Light of the Legal Environment

Under current legal regulations, arrests and preliminary detention are carried out by the police, which obviously means any person officially on police staff. The situation is the same in the case of national-security services, the National Tax and Customs Office, and the Parliamentary Guard. In the sphere of private security, those assigned to protect people and property also have the right to detain perpetrators. According to the Fundamental Law, it is possible to authorize an independently operating robot to apprehend people in Hungary, but this would require a legislative amendment. Under current Hungarian law, a robot cannot carry out such activities. Police can use robots as tools during the apprehension process. Hence robots, like handcuffs or police dogs, can help ensure a successful apprehension so long as a law-enforcement official is present[31].

In his study on robotics, Zoltán Székely points out that the main challenge is as follows: After we have designed the ideal robot, made of heavy-duty material, whose motions are governed by flawless factory software, and equipped with superhuman sensory organs, we must also provide that which governs the body – the brain, the central computer, the artificial intelligence. A rookie robot lacks life experience, ethics and morals, habits and norms. It has no intuition, no sense of suspicion, zero feeling of empathy, and has no way of determining whether someone is lying or simulating an act[32].

The consequence of the arrest may be the hearing. The robot shall not do the hearing. As the **Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States sayes**

[31] Zoltán Székely (2014), „Habeas Corpus Machinima. Avagy elfoghat-e engem egy robot?" (*Habeas Corpus Machinima*; or, Can a Robot Arrest Me?") *Hadmérnök*, IX(1) (March 2014), pp. 291- 303.

[32] Zoltán Székely (2014), *„Habeas Corpus Machinima. Avagy elfoghat-e engem egy robot?"* (*Habeas Corpus Machinima*; or, Can a Robot Arrest Me?") *Hadmérnök*, IX(1) (March 2014), pp. 291- 303.

Where the arrested person does not consent to his or her surrender as referred to in Article 13, he or she shall be entitled to be heard by the executing judicial authority, in accordance with the law of the executing Member State[33].

VII. Conclusion

At present, robots cannot independently arrest people because only law-enforcement officials are authorized to carry out apprehension activities. However, the law permits police to use them as tools.

There is no legal dogma that prevents the use of robots to apprehend people, since there are already numerous examples of machines or installations carrying out activities that have the effect of limiting personal liberty, even without human intervention.

„In some cases, the use of police robots may increase the safety of policing, for both officers and the public. In other cases, however, the use of police robots to detain or subdue a suspect may raise challenges to the conventional ways in which we have regulated the police"[34].

The technical realization of this goal is possible through several steps: First, by having robots assist in arrests, then using them „partners" in police patrols, and finally, if necessary, allowing robots to independently apprehend human beings under strict security and quality-control requirements. Anyone detained by a robot would have to be brought before a judge promptly. No machine can ever replace a judge under any circumstances.

References

1. Berger, Vincent (1999), *Az Emberi Jogok Európai Bíróságának Joggyakorlata* (*The Legal Practice of the European Court of Human Rights*), Budapest, Károly Tóth (ed.), ISBN 963 03 811192.

2. Blutman, László (1993), *„A fogvatartás bírói felülvizsgálata: a habeas corpus az európai alapjogok között"*, Judicial Review of Detention: *Habeas Corpus* Among European Fundamental Rights, *Jogtudományi Közlöny*, August-September 1993.

3. Czine Ágnes, SZABÓ Sándor, VILLÁNYI József, p. 255: *Judgment in the case of Soysal v. Turkey*, 3 May 2007, petition no. 50091/99.

4. Ferdinandy, Gejza (1899), *Az arany bulla* (*The Golden Bull*), Hungarian Academy of Sciences, Budapest.

5. Hajdu, Lajos, HORVÁTH. Pál, IJJAS, József, SZEGVÁRI Katalin, ZLINSZKY, János, STIPTA, István (1991), *Általános Jogtörténet* (*General History of Law*), Tankönyvkiadó, Budapest.

6. Joh, Elizabeth E. 64 UCLA L. Rev. Disc. 516-543 (2016) https://www.uclalawreview.org/wp-content/uploads/2016/11/Joh-D64.pdf.

7. Kordik, Marek (2011), *„Ne bis in idem: The role of national criminal law in the European Union area and the alternative resolutions of criminal procedure,"* Collection of

[33] 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision (*Official Journal L 190, 18/07/2002 P. 0001 – 0020).*

[34] Elizabeth E. Joh 64 UCLA L. Rev. Disc. 516-543 (2016), https://www.uclalawreview.org/wp-content/uploads/2016/11/Joh-D64.pdf.

Papers from the International Scholastic Conference Law as a Unifying Factor of Europe – Jurisprudence and Practice, Comenius University Faculty of Law, Bratislava.

8. Lahden *Ammattikorkeakoulu Tekniikan ala Kone – ja tuotantotekniikka Mekatroniikka Opinnaytetyö Syksy 2011 Fareed Shakhatreh,* Lahty University of Applied Siences, https://www.theseus.fi/bitstream/handle/10024/37806/Shakhatreh_ Fareed.pdf?sequence=2.

9. Landman, James, *You Should Have the Body Understanding habeas Corpus*. Social Education 77(2) pp 92-105, 2008 National Council for the Social Studies (https://www.americanbar.org/content/dam/aba/images/public_education/05_mar08_habeascorpus_landman.pdf.

10. Mezey, Barna (2015), *„A Runnymede-i carta, 1215"* („The Carta of Runnymede, 1215"), *Ügyvédek Lapja*, 2015/3.

11. Nelson, Steven, *Are robot cops the future of efficient, bias-free policing?* February 06, 2018.

12. Poor, János (ed.) (2000), *Kora újkori egyetemes történeti szöveggyűjtemény* (*Early Modern Universal Historical Document Collection*), Osiris Kiadó, Budapest.

13. Salat, Orsolya (2008), *„Az Egyesült Államok Legfelső Bíróságának döntéseiből"* („From the Decisions of the Supreme Court of the United States"), *Fundamentum*, 2008/3.

14. Szekely, Zoltán (2014), *„Habeas Corpus Machinima. Avagy elfoghat-e engem egy robot?"* (*Habeas Corpus Machinima*; or, Can a Robot Arrest Me?") *Hadmérnök*, IX(1) (March 2014).

Accreditation and standardization in forensic science - present and future of reliability of forensics examination and expertise

Dr. Aleksandar B. Ivanović*
Associate Professor of criminalistics
Forensic Center Police Direktorate of Montenegro, Danilovgrad

Abstract

The author deals with the issue of standardization and accreditation in forensic science as a key factor in achieving the reliability of forensic evidence. In this regard, the author gives a concise summary of the application of the international standard ISO 17025, which refers to the accreditation of forensic laboratories. The paper presents forensic institutions in Europe that are accredited to ISO 17025. With tending of assurance of the reliability of forensic work, as one of the cornerstones of a fair judiciary, autor in the paper also points on that what is considered as future in the field of accreditation and standardization of forensic work. That is mosty related on the work of the technical committee TC 272, which is based on the development and application of forensic standards, which will include a complete forensic process from finding on-site material traces to the presentation of findings and opinions by forensics at the court room.

Keywords*: forensic science, accreditation, standard ISO 17025, reliability of forensic evidence, technical committee TC 272.*

I. Introduction

For the last 30 years role of forensic examinations and expertise is of great importance for the work of the judiciary system. Namely, at the end of the twentieth century, analytical methods were developed using primarily DNA testing (deoxyribonuclearic acid), chromatographic methods (gas mass and liquid chromatography), scanning electron microscopy (which could increase up to 300,000 times), and in particular the development of information technology (computers, internet, mobile telephony), lead us to the situation that even small traces can be faunded on the crime scene, identified by using of modern technology, and presented at the court by forensic experts. The use of identification forensic methods, such as DNA analysis and fingerprint analysis and the creation of applicable and operational databases with more than a million search patterns (for example, the DNA Database DNA Database - NDNAD National DNA Database, contains about one million ipo DNA profiles), classified as forensic evidence as an indisputable means of illuminating and prosecuting criminal offenses. This is because modern forensic methods meet high quality criteria of evidence, namely: relevance and credibility. In forensic expert circles, for the DNA realm of DNA testing, it is commonly said that only sky is the limit of their potential, and for the domains of digital forensics, it is commonly said, neither sky is the limit of their ability!

* E-mail: ialeksandar@t-com.me.

However, in the time of expansion and (non) justified optimism of the forensisation of science and their application in the judiciary, there is anxiety and caution. Persons who possess expertise and skills gain unusual power. Engaged by the judiciary, protected by the authority of science, provide testimony that justice participants simply can not understand. There is a paradox similar to Juvenal's critique of Plato's state who will guard the guardians? That is, who can establish the probative value of the findings and opinions of the forensic who is called before the court precisely because of its knowledge, which court and the parties not posess? Furthermore, are the tests, measurements, calibration, etalonization used in contemporary forensic examinations scientifically valid? Are forensic laboratories performing sophisticated examinations and expertises, staffed and technically trained and equipped to produce technically valid results? As mentioned in the text so far, there is a clear and important role for forensic examinations and expertises in order to illuminate criminal offenses and prosecute their perpetrators. However, in the proper sense, the Forensic Laboratory has demonstrated that the tests and expertise carried out by competent and scientifically based must be accredited in accordance with the international standard ISO 17025. In contemporary judicial systems in the European Union and the United States, confidence in the forensic forensic examinations and the expertise is based on the application of ISO 17025 as the most important single standard for standardization and testing[1].

II. Application of ISO 17025 standard in forensics

Confidence, reliability, precision, accuracy and other activities for forensic examinations and expertises in the EU and candidate countries are carried out by the European Network of Forensic Science Institutes (ENFSI)[2]. The most important activity of this reference and respectable netwokr is the impleement of ISO 17025 quality standard in forensic laboratories in European countries. This is best described in the ENFSI Quality Policy[3] (Policy on standards for accreditation), where, among other things, it states that one of the aims of the ENFSI is to forensic evidence preforming in laboratories accredited to ISO 17025.

The ISO 17025 standard is intended for the use of the development of laboratory quality management systems, administrative and technical operations (Majstorović & Majkic-Sing, 2006:5). The use of this standard will, among other things, help, in cooperation between laboratories of different countries, which is of great benefit in illuminating criminal offenses of cross-border crime, terrorism and corruption. The purpose of applying the ISO 17025 standard in forensic laboratories is to achieve reliability of testing and results obtained in the laboratoryes.

The quality of analysis and the results of judicial expertise are important for the judicial system, law enforcement, crime prevention and health policy, as well as international harmonization, exchange and coordination of information and forensic data in the world.

---

[1] ISO / IEC 17025 was first mentioned in 1999 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), (Calibrate Inc./The Pipet People, 2014).

[2] www.enfsi.eu.

[3] http://enfsi.eu/wp-content/uploads/2016/09/160727_qcc-acr-001-006_policy_on_standards_for_accreditation.pdf.

Compatibility and acceptability of laboratory results between the countries has been facilitated by their compliance with ISO / IEC 17025: 2005 - an International Laboratory Quality Test and Calibration Standard, in relation to the recommendations of the ILAC-G 19: 2002 International Laboratory Accreditation Association for Forensic Scientific Laboratories. Compliance with ISO 17025 also ensures compliance with ISO 9001, which in itself is not a substitute for ISO 17025 compliance, ie is not sufficient for the technical competence of the testing lab.

Quality devotion is the functional principle of forensic testing and expertisation. Standrad quality ISO 17025, pays attention to the technical conditions (including the importance of expert training, adequate accommodation of their necessary equipment and environmental conditions, validation methods, access to the required equipment and reference standards, quality control and reporting of results) and management requirements (including document control, response to customer needs, preventive and corrective action, the need for regular audits, compliance with the quality management system and continuous improvement). In the following, we will present on which way application of certain parts of the standard contributes to the reliability of forensic testing and expertisation. Also, since standard ISO 17025, as a rule, covers the entire work of the forensic laboratory, this description of all the parts of the standard greatly overcomes the scope of this work, and hereafter we provide a description of the pieces of standards relating to the reliability of forensic application in order to illuminate criminal offenses and prosecute their perpetrators.

1. Log Control / Chain of Evidence

Accredited forensic laboratory according to ISO 17025 standard, it has systems for making, marking, managing, storing, moving, locating and destroying all records in paper and electronic form.

The technical records include all written case-related materials, including sample layout description, document dossier, case files (including drawings and diagrams), photographs, telephone conversations, spectrums, calibration and other quality control data, working parameters instruments and records, reports, statements, etc., records and records on the maintenance of instruments and training of a court expert, records of competencies and authorizations.

Technical records shall be kept in a safe and secure place, to avoid damage, decay, unauthorized access or loss, for a period depending on the needs of the applicant / investigator (police, court and / or prosecutor) and relevant regulations under the jurisdiction of forensic laboratories. In this way, by applying the aforementioned standard part, in a forensic laboratory accredited according to ISO 17025, the possibility of modification, contamination, subsequent changes and replacement of the test material for testing is excluded (Simonović, 2009:237).

2. Staff-forensics

The greatest treasures of a forensic laboratory are people who work in it! The forensic laboratories and forensics employed in them have policies and procedures for identifying training needs and providing training to staff-forensics in order to assist in achieving and maintaining skills (eg through defined training programs at the workplace, participation in scientific and expert meetings, seminars, conferences and workshops, technical training, courses by suppliers for instrument work and maintenance, and further education and training). While training is being done, the staff-forensics have been closely

monitored, in a way to monitor and evaluate the effect of the training. If the training effect is tested or verified, check criteria should be determined (eg by tracking the appropriate tests or by an expert's analysis, or by comparing the results of individual tests with the results obtained from other training forensics). When needed, training programs also include training on the development of evidence in court.

For each forensic expert, a record of his / her education, qualification and training is kept, together with a list of jobs for which he has been trained and authorized (eg for conducting certain types of tests, issuing test reports, giving opinions and interpretations, and working with a particular type equipment). This information should include a date, responsibilities and authorizations, so that all forensics clearly understand the scope of their duties and responsibilities. By applying this part of the standard, the full reliability of the forensic experts who performed the examinations / expertises in the same field of examinations / expertise is provided.

3. Forensic staff specifics

When it comes to so-called. Forensic staff, regardless of whether they are doing fieldwork (on the scene of a criminal event) or in a lab, it is necessary to have certain skills related to the evidence material such as: detection, identification, protection, documentation (written and photo / video, packaging, labeling, safe transport, to ensure that it does not change the evidence material by proper handling, which could make it partially or completely unsuitable for the analysis and thus negatively affect the results of the analysis.

Personnel should be trained to ensure that no material changes (physical, chemical or biodegradable nature) occur to prevent material loss or contamination, to avoid sampling, both when locating and sampling, as well as during transport or disposal (if necessary fridge / freezer), and handling the same during laboratory work and storage after completing the analysis.

In this respect, it is necessary to know the basics of handling different materials (liquid, solid, powdery, volatile, chemically aggressive, poisonous, biologically dangerous) and be aware that many materials may have latent nature (invisible) or are present in very small quantities microtracks) and to find the necessary knowledge of optical detection methods (eg use of lupe or light sources of different wavelengths - commercial products: UV lamp or forensic light).

Forensic staff must also have sufficient knowledge in the area of application of legal regulations relating to drug-related material handling, treatment of persons face-to-face when encountering such material, with persons related to the particular case and must be trained for teamwork (eg. with a prosecutor, medical staff, etc.).

In many countries, laboratory forensics have the task of appearing as expert witnesses in court proceedings, ie, at the main trial, elaborate and interpret the results of the analysis and answer the questions of all participants in the proceedings (prosecution, defense, judges, accused and injured parties).

In this regard, appropriate staff must have the necessary education, knowledge and experience to carry out this responsible job.

4. Methods of testing and analysis, validation of methods and procedures

Forensic laboratory accredited according to standard ISO 17025, use appropriate methods and procedures for all tasks: sampling, handling, transport and storage of evidence, use of equipment, testing, evaluation and interpretation of results and

reporting. Methods and procedures are fully documented and easily accessible to all parties in a judicial procedure.

The documented method contains the following:

– Method name, method reference number;

– Scope of the methods (eg analytes, matrices, concentrations, ranges, known interferences - the interactions of the individual components that the analysis material may contain);

– Theoretical principles of the method;

– A set of validation parameters and reference to a document containing validation data;

– Chemicals, appliances and equipment, including technical specifications; Reference standards, required materials, required ambient conditions (eg room temperature) and some stabilization time (eg setting time for GC);

– Description of the step by step process, including:

a) any special precautionary measures taken;

b) requirements for sampling, marking, packing, transport and preservation of samples;

c) preparation of samples, reference materials, standards for control and calibration of the analysis;

d) requirements for checking and calibration of equipment (eg standard sample release, adjustment and mass spectrometer calibration);

e) process of analysis / test procedure and quality control (eg use of blind tests, control and calibration standards);

f) recording and processing of results (eg calculations, preparation of calibration curves and scales), including acceptance or rejection criteria (for example, if the results out of the calibration range or the control of the quotient are unacceptable);

g) results report requirements;

h) requirements for the Report on the Unreliability of the Method.

5. Development and validation of forensic methods, used for testing and expertisation

The methods and procedures used for forensic examinations and examinations are based on papers published in reviewed scientific journals (for example, Forensic Science International, Journal of Forensic Sciences, Journal of Analytical Toxicology, Journal of Chromatography and UNODC / LSS publications based on published papers[4]) and needs

[4] Following the Dauber case, the Supreme Court of the United States agreed that the provisions of the Ordinance on Evidence (Federal Proofs) should not apply to the admission of scientific evidence in the case (1993), rather than a „Fixed Test". Thus, after a full 70 years, the „Fret test" is replaced by the rule that the evidence presented in a particular case must meet the following five conditions: a) Can the theory or technique on which a critical scientific testimony is based can be verified? b) Does the technique involved have a known error rate in its application? The professional expression for the mentioned measurement uncertainty and the same implies the percentage of error in performing some forensic examinations, analyzes and expertises; c) Is the relevant theory or technique discussed in the professional circles and whether it is published in the form of reviewed books and / or in the form of reviewed scientific work; e) What is the level of acceptance of the theory or technique in the relevant scientific community; f) To what extent are there standards for determining the acceptable use of the subject technique? There is also a sixth criterion that needs to be fulfilled in the court's evidence presented (*General Electric Co.* v. *Joiner*, 522 U.S. 136), reads: - Relevance, which implies examining the

to meet client needs. If published methods are unavailable, methods developed in the laboratory may be authorized, provided they meet the intended purpose and meet the needs of the client. In that case, the examination record should contain sufficient details of the method applied so that the other qualification analyst understands the method and the results obtained.

Validation is by confirming, reviewing and providing objective evidence that certain conditions for a particular purpose are met. Guidelines on what is appropriate in different circumstances and for different methods can be found in many publications.

Verification is similar to validation and shows that forensics are applied according to the foreseen specification, and is used when the method is validated at another location.

When computers or automated equipment for collecting, processing, recording, reporting, storing or finding test or calibration data are used, a forensic engineer in the accredited laboratory ensures that the software developed by the users is fully documented and validated in an acceptable manner.

The accredited forensic laboratory possesses the documented forensic records that were involved in the validation affairs, the dates, the results obtained, the procedures used, the statement that the method corresponds to the intended use and the authorization to the place, signed the approval.

When the forensic laboratory introduces a method validated in another (accredited) laboratory, it must first demonstrate the reliability of the method in its own laboratory, in addition to any performance characteristic of the method published in the literature. The record of this performance verification is kept for future reference.

6. Equipment

Forensics and / or accredited laboratory in which they work, have procedures and instructions, whose application guarantees the reliability and performance of the equipment being used. The list of equipment owned by accredited laboratories is maintained with the record of its location, date of purchase, service history and maintenance. The main items of equipment (eg instruments such as spectrometers, chromatographs etc.) should have their own log for recording this information, kept close to the instrument.

Forensics in the accredited laboratory are trained in the use of equipment, and are handled only by authorized personnel when assessing that they are trained. Training and authorizations in the accredited laboratory are documented and archived.

In an accredited forensic laboratory, equipment is regularly inspected during use, using documented procedures, thus proving that its performance is still acceptable (eg, the instrument can be checked before each set of samples for assay to be sure of correctness). This may include temperature, gas pressure, adjustment, calibration, etc. depending on the instrument. For test purposes, test samples are also analyzed. Updated instructions on how to use and maintain equipment (eg abbreviated internal operating instructions as well as manuals supplied with the manufacturer) are available (preferably with the instrument) to appropriate laboratory personnel.

Equipment that has a significant impact on the accuracy of the test results is calibrated according to schedule, using documented procedures available to authorized

---

validity of conclusions drawn between theoretical analysis and practical examples of the aforementioned problem. This rule is also interpreted in a way that the judge must reject the conclusions made by the expert, which have not been accepted by the relevant scientific community.

users. All equipment in the accredited laboratory is marked (eg label with calibration status data: date of the previous calibration and expiration date or other criteria for calibration) to avoid replacement with non-calibrated equipment. The calibration of important equipment (eg scales, thermometers, pipettes) is recorded, including certificates, if available, to be kept.

Forensic who is responsible for the equipment, ie the procedures and records that follow from it, who is in charge of a specific device, should identify deficiencies and propose taking corrective actions. If the defect is serious, the concrete device must not be used until the problem is resolved and the way in which the problem is resolved, the time and date are documented in the defined form and deposited in the equipment log. Similarly, the equipment that does wrong, so that it no longer provides reliable results or is found to be defective, should be withdrawn from use. To prevent its use, it should be insulated, clearly marked or labeled as „out of use" as long as it is calibrated or calibrated or tested to work properly.

7. Work with subject-testing, sampling, labelling and packaging

The accredited forensic laboratory has procedures to exclude samples of all types of material trace in place at the laboratory, and these procedures are available and located at locations where the samples are excluded. The sampling procedure ensures that part of the sample taken for analysis is representative of the whole sample.

Sampling materials, all kinds of material evidence submitted for forensic testing, analysis and/or expertise, are recommended for sampling plans and procedures published by internationally recognized organizations such as UNODC[5], ENFSI or SWGDRUG[6].

The general principles of sampling of submitted material traces in accredited forensic laboratories are:

– In the case of a small number of suspicious items (typically 10 or less) all items should be taken. If large individual items are to be homogenized before taking samples or taking multiple samples from the total quantity of that item;

– In the case of a large number of items, it is impractical to take them all, and the sampling strategy needs to be adjusted to ensure that the samples taken are representative of all items. If the material is not homogenized, it must first be separated into homogeneous groups I then define and then document (make and approve appropriate procedures and guidelines) the appropriate sampling plan for each group.

The accredited forensic laboratory has instructions that ensure that the materials to be tested are properly sampled, labeled, packaged, and stored before being delivered to the laboratory. The labeling is so organized (of course, following the documented procedures and instructions) to allow a unique identification of samples and sub-samples and their connection to the original source. The manner of packing the delivered material traces in the accredited laboratory (acting according to the definitions and by approved laboratory management, procedures and instructions) prevents unauthorized access and loss or contamination of samples during transport (Ivanović & Ivanović, 2016:95).

---

[5] United Nations Office on Drugs and Crime. https://www.unodc.org/.

[6] Scientific Working Group for the Analysis of Seized Drugs. http://www.swgdrug.org/.

8. Laboratory Reception, Handling and Treatment

The accredited forensic laboratory has documented procedures for receiving and retrieving the relevant incriminated material traces or samples. The documents accompanying the submitted material include each item and sufficient information for the laboratory to understand what is required by the application. Each item is assigned a unique number, the corresponding details are entered into the lab system of case records.

In the laboratory, an authorized person (defined by appropriate procedure and instructions) receives and carefully checks the samples and documents.

The accredited forensic laboratory has an efficient and documented system for safe storage of samples before and after the test, which links the sample to other information submitted to the same (eg, an analysis request) identifies each sub-sample prepared from the sample and shows the course of the analysis, the date of issue of the report on the analysis, as well as the date and manner of disposal of all remaining samples after analysis. The work system in the accredited laboratory is so organized and functional that it ensures that the submitted samples for testing, analysis and / or analysis can not be physically replaced by inspecting the records or other documents, also by documented procedures, the accredited laboratory ensures the absence of opportunities to reach loss and / or damage of samples during storage, handling and analysis.

9. Results report

The results of the analysis in the accredited forensic laboratory are presented in a precise, clear, unambiguous and objective manner and meet the requirements of the applicant. The format of the report is defined to suit all kinds of analyzes that are being made and minimizes the possibility of misunderstanding and misuse.

III. Application of forensic accreditation in the countries of Europe

Accreditation of forensic jobs in European Union countries started for practical reasons. Namely, cross-border crime and terrorism forced the European states to intensify and operational police cooperation. This cooperation includes, among other things, operational forensic cooperation, which is mostly and mainly seen in the exchange of interstate exchange of forensic data, such as DNA profiles, fingerprints, traces of passenger cars, traces of footwear, traces of narcotics, traces of explosives and other forensic biometric and other data.

In order to highlight criminal offenses in the area of cross-border crime, there is often a practical and pragmatic situation, namely forensic data obtained in one state, used as evidence in the police and in the court of another state. The mentioned has led to the need to introduce common forensic standards in European countries. Of course, the European Union was first reacted in that direction as an inter-state space that guarantees high standards in the area of rights and security. With this aim, the Council of the European Union, 23.06.2008. adopted Decision 208/615 / JHA „Strengthening cross-border cooperation, particularly in the fight against terrorism and cross-border crime". This Decision, inter alia, provided that the states of the European Union would more effectively begin exchanging forensic databases and identifying perpetrators suspected of terrorist offenses and interstate crime. Soon after the Council of Europe Decision No 208/615 / JHA was adopted, it was necessary to make the same modification, the

manager of its reliability, operability, eligibility and legal norms[7]. The Council of the European Union did so by adopting Decision 2009/905 / JHA, 30.11.2009, years, which refers to the accreditation of forensic institutions in the European Union. This Decision is aimed at securing the integrity, compatability and usability of forensic data (now DNA profiles and fingerprints) from one country to another.

In order to provide the objective set out in the Council of Europe Decision 2009/905 / JHA[8], it obliges all EU member states to have at least one forensic institution accredited according to the international quality standard ISO / IEC 17025. Article 5 of the said EU Council Decision strongly suggests that in order to recognize forensic testing, analysis, research and expertise, each Member State must adhere to the stringent requirements required by the ISO / IEC 17025 quality standard. The implemen- tation of the EU Council Decision under item 7, imperative for Member States, requires the following (Ivanović & Rump, 2011:163):

a) Accreditation of the DNA Laboratory until 30.11.2013. years;

b) accreditation of dactyloscopic laboratories up to 30.112015. years;

c) inclusion in the national legislation of the EU Council Decision 2009/905 / JHA, by 30.05.2016. years;

d) The Council will, by the end of 2018, monitor the application of this Decision in the Member States.

Implementation in practice, Council of Europe Decisions 2009/905 / JHA, is entrusted to the ENFSI Association. Since ENFSI full members are not only forensic institutions from the European Union but also candidate countries for accession to the European Union[9], the condition for retaining membership in ENFSI was accreditation by 2013 (except for three forensic institutions, which were members of the ENFSI project-EMFA-2[10], The European mentoring for forensic accreditation and for these institutions deadline was the 2014. Year was forensic institutions from Montenegro, Serbia and the Russian Federation.

Quality Control, Quality Standards and Accreditation, Quality Management and Compensation Committee (QCC[11]) is responsible to the ENFSI. The following table gives the data of the ENFSI Quality and Competency Committee, which outlines the current situation in the area of application of forensic standards in the countries of Europe, members of ENFSI (Enfsi members are not forensic institutions from Bosnia and Herzegovina, Albania, Moldova and Belarus It should be mentioned that Portugal has not yet managed to accredit its forensic laboratory !?) (Rakočević, Ivanović & Maver, 2017:301).

---

[7] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014459%202010%20INIT

[8] Council framework Decision 2009/905/JHA of 30 November 2009 on Accreditation of forensic service providers carrying out laboratory activities. https://publications.europa.eu/en/publication-detail/-/publication/9c1f8a74-4287-4f2a-bf02-0df5f9a8f01f.

[9] Constitution ENFSI (statut ENFSI-a). http://enfsi.eu/wp-content/uploads/2017/06/181107_ENFSI-Constitution_181107-approved.pdf.

[10] It is about the EMFA-2 project, European mentoring for forensic accreditation and for these institutions the guard was 2014. year. They were forensic institutions from Montenegro, Serbia and the Russian Federation).

[11] The Quality and Competence Commitee. http://enfsi.eu/about-enfsi/structure/standing-committees/ qcc/.

Table 1. Overview of European states accredited by their forensic institutions according to SIO 17025, ISO 17020 and others (ISO 9001, ISO 17065, ISO 17043), as well as an overview of accredited DNA analysis and Dactyloscopic analyzes[12].

	Forensic institution accredited (by what standard)	**Accredited DNA analysis method**	**Accredited method of dactyloscopic analysis**
Armenia	ISO 17025, ISO 9001, ISO 17065	Not	Ne Not
Austria	ISO 17025	Not	ISO 17025
Bulgaria	ISO 17025	ISO 17025	ISO 17025
Cypar	ISO 17025	ISO 17025	ISO 17025
Croatia	ISO 17025	ISO 17025	ISO 17025
Ches Republic	ISO 17025	ISO 17025	ISO 17025
Danmark	ISO 17025	Not	ISO 17025
Estonia	ISO 17025, ISO 17020	ISO 17025	ISO 17025
Finland	ISO 17025	ISO 17025	ISO 17025
France	ISO 17025	ISO 17025	ISO 17025
Georgia	ISO 17025	ISO 17025	ISO 17025
Germany	ISO 17025, ISO 17020	ISO 17025, ISO 17020	ISO 17025, ISO 17020
Ireland	ISO 17025	ISO 17025	ISO 17025
Italy	ISO 17025, ISO 9001	ISO 17025	ISO 17025
Latvia	ISO 17025	ISO 17025	ISO 17025
Lithuania	ISO 17025	ISO 17025	ISO 17025
Macedonia	ISO 17025	ISO 17025	Not
Montenegro	ISO 17025	ISO 17025	ISO 17025
Netherlands	ISO 17025	ISO 17025	ISO 17025
Norway	ISO 17025	ISO 17025	ISO 17025
Poland	ISO 17025	ISO 17025	ISO 17025
Romania	ISO 17025	Not	ISO 17025
Russian Federation	ISO 17025	Not	Not
Serbia	ISO 17025	ISO 17025	Not
Slovenia	ISO 17025	ISO 17025	ISO 17025
Slovakia	ISO 17025	ISO 17025	ISO 17020
Špain	ISO 17025, ISO 9001, ISO 17043	ISO 17025	ISO 17025
Sweden	ISO 17025	ISO 17025	ISO 17025
Switzerland	ISO 17025, ISO 17020	Not	ISO 17025
Turkey	ISO 17025	ISO 17025	Not
Great Britain	ISO 17025, ISO 17043	ISO 17025	ISO 17025

[12] ENFSI/QCC survey 2016.

Ukraine	ISO 17025	ISO 17025	Not

Table 1 shows that virtually all European countries have accredited their forensic institutions, mostly and mostly according to the international standard ISO 17025, and by ISO 17020[13], ISO 9001[14] and ISO 17043[15].

IV. Conclusion

The quality of analysis and the results of forensic examinations depends to a great extent on the efficiency and effectiveness of the judicial system, with the aim of fair and equitable implementation of legal norms, further crime prevention, international harmonization, exchange and coordination of information and forensic data in the world. The above-mentioned, contemporary judicial procedure puts in front of the imperative forensic institutions, the results of the analysis, testing and expertisation performed in forensic laboratories:

– reliable,

– valid,

– based on standard procedures,

– compatible with results in other countries, other scientific and professional circles, internationally recognized institutions,

– in accordance with the evidentiary standards of the appropriate judicial, administrative and legal systems,

– get in the required timeframes, in an effective and efficient manner.

The guarantor of the mentioned factors in forensic work and treatment is accreditation according to the international ISO 17025 quality standard. This standard regulates all segments of the work and procedures of a forensic laboratory. In addition, accreditation according to ISO 17025, implies the compatability and applicability of forensic evidence obtained in one country during the conduct of an evidentiary proceeding in another country, particularly in cross-border crime, terrorism and corruption cases.

Accreditation as a factor for the reliability of forensic post-work and work is of great importance for the implementation of the Council of Europe Conclusions on the forensic scientific area and forensic infrastructure EFSA 2020 (Council conclusions on the European Forensic Science 2020 forensic science infrastructure in Europe[16]). Priority of the goals of the Council of Europe's mentioned document is the accreditation of forensic laboratories by 2020, but also, among other things, the development of European forensic databases, why the conditions for the creation of European forensic databases of DNA and Dactyloscopy have already been achieved. However, by pursuing the goals of meeting the Conclusions of the Council of Europe, EFSA 2020, it is necessary by 2020 to create a database of illegal drugs, firearms, manuscripts and documents, footprints and so on, and to fulfill the aforementioned goal, it is necessary to accredit

[13] Inspection Standard Application document. http://www.fnovi.it/sites/default/files/old_fnovi/userfiles/files/ISO-IEC-17020-Inspection-Standard-Application-Document.pdf.

[14] Quality Management System. https://www.iso.org/standard/62085.html.

[15] Proficiency Testing Provider Accreditation Documentation Kit. https://www.globalmanagergroup.com/Products/PTservices-17043-accreditation-documents-manual.htm?.

[16] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/126875.pdf.

these forensic methods according to ISO 17025 standard.

As mentioned above, the international ISO 17025 quality standard refers to forensic work and treatment in a forensic laboratory. However, as forensic examinations, analyzes and expertises are based on on-site forensic work, which involves finding traces of material, further fixing, exclusion, packing and sending forensic examination. This part of the forensic treatment from a person's point to a forensic laboratory implies accreditation according to ISO 17020. However, both standards currently regulating and controlling the reliability of forensic treatment are not strictly forensic standards. For example, the ISO 17025 standard applies mostly and mainly to a (basically) chemical and / or toxicological laboratory, while the ISO 17020 standard has the name Requirement for the work of inspection bodies (Bencivenga, 2015:341). Since accreditation is a process that is constantly changing, supplementing and supplementing, the forensic community through the ISO organization (International Standardization Organization[17]), within which the Australian Standardization Organization[18], has joined the organization of the Technical Committee for the Adoption and the subsequent application of international standards that will standardize forensic work from detecting material traces on the scene of crime and to interpreting (reporting) the results of court forensic work! The aforementioned Technical Committee (TC 272) has hitherto made three standards:

– ISO 18385 Reduction of the risk of human DNA contamination in products used in the collection, storage and analysis of biological material for forensic purposes. (Minimizing the risk of human DNA contamination in products used to collect, store and analyze biological material for forensic purposes);

– ISO 21043-1 Forensic Science - Part One, Concepts and Definitions (Forensic Sciences - Part 1: Terms and Definitions);

– ISO 21043-2 Forensic Science - Part Two, Recognition, Recording, Collection, Transportation and Storage of Items (Forensic Sciences - Part 2: Recognition, Recording, Collecting, Transport and Storage of Items).

In addition to constructed and aggressive standards, TC 272, there are currently four more forensic standards in operation, namely:

– ISO 20964 Specification of consumable material used in forensic procedure-requirements for sampling whales. (Specification for consumables used in forensic process;

– ISO 21043-3 Forensic Science Part 3: Analysis (Forensic Sciences - Part 3: Analysis);

– ISO 21043-4 Forensic Science Part 4: Interpretation (Forensic Sciences - Part 4 Interpretation);

– ISO 21043-5 Forensic Science - Part 5 Reporting (Forensic Sciences - Part 5 Reporting).

The completion and enhancement of standards, which are under the scope of TC 272, is expected in May 2020. The standardization of standards and their implementation in forensic laboratories will make a big contribution to the reliability of forensic testing, analysis and expertise, and thus the righteousness as one of the fundamental foundations of a society that strives to be righteous and right as the finest of the democracies.

---

[17] International Organization of Standardization. https://www.iso.org/home.html.

[18] Standards Australia. https://www.iso.org/member/1524.html.

References

1. Bencivenga, P. (2015) *Which Standards Are Standard? Differences between ISO/IEC 17025 and 17020 for forensic agencies*. Forensic Magazine 10/22/2015. Publishing, 2007 (p. 338-356)

2. Council of the Europe (2009) *EU Council Framework Decision 2009/905/JHA* of 30th November 2009: Accreditation of forensic service. http://eclan.eu/en/eu-legislatory/council-framework-decision-2009-905-jha-of-30-november-2009-on-accreditation-of-forensic-service-providers-carrying-out-laboratory-activities

3. Council of the Europe (2011). EFSA 2020 (Council conclusions on the vision for European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/126875.pdf

4. ENFSI-EA (European co-operation for Accreditation9. (2008). Guide for the implementation of ISO/IEC 17020 in the crime

5. ILAC (2014) Modules in a Forensic Science Process. http://ilac.org/latest_ilac_news/ilac-g19082014-published/

6. Ivanović, A., Merike Rump (2011), *ACCREDITATION PROCESS FORENSIC CENTER OF MONTENEGRO TO THE MENTORSHIP OF THE EUROPEAN UNION* (Projects EMFA-2). 10th Symposium of forensic sciencies. Bratislava. Symposium Journal. Kriminalisticky a expertizny ustav Policajneho zboru. (p. 159-164)

7. Ivanović, B. A., Ivanović, R. A., (2016) *Current issues with the criminalistics investigations managing with a focus on standardization and accreditation*, Legal issues vol. 4, no. 8. International university of Novi Pazar, pp. 85-99.

8. Majstorović, V., Majkić-Singh, N. (2006). *Accredited laboratory as a model for quality improvement in the organization*. Yugoslavia Med Biohem 2006. 25. Pp 1-9 2006.

9. Rakočević, V., Ivanović, A., Maver, D. (2017). *Forensic Accreditation in European Countries: Current Situation. Revija za kriminalistiko in kriminologijo*. Letnik 68, številka 3. Ljubljana.

10. Simonović, B. (2009). *Standardization and Accreditation as one of the ways of professionalizing police and criminal services*. Safety No 1-2 / 2009. Belgrade. MUP Serbia. Pp 236-254.

Criminological and criminal legal aspects of discrimination, violence, abuse and neglect of school-age children

Prof. dr. Osman Jašarević[1]
Faculty of Law of the University of Travnik
Farah Fazlagić, Bachelor[2]

Abstract

The topic of this paper is the criminological aspects of discrimination and violence against school-age children. In the introductory part of the paper, the criminological aspects of discrimination, the definition of violence, the rate of occurrence and causes of violence among school-age children, the conditions and motives that lead to discrimination and violence against school-age children are considered, followed by the criminological aspects of discrimination and violence against children in the course of historical development in the family and in school, the discriminatory and violent aspects of parents' behaviour, the risk factors and protective factors with regard to abuse, who discriminators, bullies and abusers are, the types of discrimination, violence and abuse, and how to protect children from discrimination, violence and abuse.

Discrimination, violence and abuse are heavily widespread phenomena in the world and also in Bosnia and Herzegovina and the wider South Eastern European region. On a daily basis, we hear about witness discrimination, violence and abuse of children in schools, families and peer violence. Discrimination, teasing, insulting, ridiculing, provoking, blackmailing, violent attacks and forcible deprivation of cell phones and other objects are the most common forms of peer violence among school-age children. The victims are mostly modest, withdrawn, peaceful, well-brought-up, peaceful and often insecure children. The topic of discrimination, violence and abuse of children is debated, spoken about and written about every day in various tabloids, through the „crime news" in daily newspapers. Discrimination, violence, neglect, sexual abuse, emotional abuse and corporal punishment of children are, unfortunately, always present in society, even though it is difficult to accept. Discrimination, violence, abuse and neglect of children happens in all areas and can, to a great extent, affect the development of children and leave lasting consequences.

Regardless of the statistics on discrimination, violence, abuse and neglect of children, scholars, experts, analysts and others claim that these phenomenological forms of criminal aspects against school-age children increase year after year. The final part of the paper addresses the rights of children and the prevention of discrimination, violence, abuse and neglect of children and among children.

Keywords: *discrimination, violence, abuse, neglect of children, protection, rights of the children.*

---

[1] e-mail:dr.osmanjasareic@hotmail.com.
[2] e-mail: farahfazlagic@hotmail.com.

I. Introduction

It is important to emphasize that the last few decades of the twentieth and twenty-first century have seen an increase in criminological forms of discrimination, violence, abuse and neglect of school-age children by teachers, educators, school counsellors, parents, educational and other pedagogical institutions. Most citizens witness discrimination, violence, abuse and neglect of children, on a daily basis in different places and at any time of the day. Certain categories of children, mostly children of wealthy families tease, discredit, insult, ridicule and humiliate in various ways their chosen victims, leading eventually to physical violence.

Discrimination, violence, abuse and neglect of children in general, including school-age children, had always been recorded, but not to a such degree, during the historical development of society in various epochs, until it began to be spoken about this phenomenon publicly. Even then, people felt anxious and concerned about this issue and attempted to find ways to prevent it through general and special prevention measures taken by state authorities. Victims, i.e. school-age children, are mostly silent about all deviant forms of attacks, humiliation, psychological and physical maltreatment, fearing for their lives and what would happen to them if they speak out, resist or fight back. Therefore, this paper discusses discrimination, violence, abuse and neglect of school-age children. Some parents are increasingly allowing themselves to impair both the psychological and physical well-being of their children, and the children imitate their parents by copying these behaviour patterns in their interactions with other children thus committing various forms of peer violence.

Therefore, it is important to recognize the inappropriate behaviour of parents towards children, and to be aware of how to encourage children to speak without fear about their problems, how the schools, teachers, educators can help children facing discrimination, violence, abuse or neglect in order to develop properly and what can be done to protect such children regardless of whether they are experiencing violence at home or in school.

What children see and hear on television, the radio, the Internet and other networks, encourages them to various destructive forms of deviant behaviour in terms of discrimination, aggression and violence, and makes them satisfied with their actions.

Various forms of corporal punishment of children are applied in some countries as a methods of work, order and discipline. This is the reason why certain schools, even schools in foreign states, consider corporal punishment as a measure of upbringing. In the age of science, technology and digitalization, the corporal punishment of children is seen as unacceptable.

Practice shows that discrimination, violence, abuse and neglect in the family most frequently occurs after a parent experienced discrimination, forcibly alienated from the family or abused (i.e. physically or psychologically punished) and these methods of punishment are passed on to other children, and in turn transferred through imitation to their peers who are school-age children[3].

This paper consists of several parts which discuss the criminological and historical overview of discrimination and violence against children in the family, and discrimination, violence and abuse of children in schools, as well as the Convention on

[3] https://zir.nsk.hr/islandora/object/ufzg:402/preview, Marija Lujić was born on 22/11/1993 in Sisak.

the Rights of the Child. The paper then addresses the issue of violent parents and what encourages them to conduct domestic and violence against their child. Previous analytical reports show that there are various theoretical models of violent parental behaviour towards children, but also protective factors for abuse that will be discussed in the paper.

II. Discrimination

Discrimination (lat. *discriminare*) means separating, making a difference on the grounds of social, wealth, racial, ethnic, religious, individual, sexual, linguistic, age or other characteristics of a person.

Discrimination results in difficult or impossible exercise of certain human rights. Unfortunately, the worst part of stereotypes and prejudices is their consequences in behaviour, which is discrimination. The very realization that a person is stigmatized causes discomfort, or feelings such as anger, sorrow and loneliness. An even greater injustice is loss of work or inability to work, poor housing conditions or low income resulting from discrimination[4].

Discrimination[5] is any act of distinguishing and unequal treatment of a person or a group of persons due to personal characteristics that make them different from others. It can be based on gender, national, religious identity, sexual orientation, disability, political conviction, skin colour, property, etc. The labour market is one of the areas where discrimination often occurs in Bosnia and Herzegovina, based on gender, nationality, disability.

III. Violence

Today, violence is a well-known and widely discussed subject. It is by itself a highly complex social phenomenon and a state in a society, which, in terms of emotion, motivation and action, manifests itself as an internal instinct, fury, rage, anger, hostility and increased aggressiveness in attacking a particular person, object, geo territory, groups of people and wider. Therefore, it can be said that violence is a characteristic use of force, threat, blackmail or other ruthless act directed against someone. Violence aims at controlling another person by using power in a varying intensity. Hence, violence is an inhuman act that is to be condemned but is often expressed in milder or more severe forms that can also be permanently harmful and difficult[6].

Bilic et al., 2012[7], cites the World Health Organization's definition (WHO, 2006) of violence: *„all forms of physical and/or emotional ill treatment, sexual abuse, neglect or negligent treatment or commercial or other exploitation, resulting in actual or potential harm to the child's health, survival, development or dignity in the context of a relationship of responsibility, trust or power".*

---

[4] https://hr.wikipedia.org/wiki/Diskriminacija#cite_note-1.

[5] http://www.diskriminacija.ba/%C5%A1ta-je-diskriminacija.

[6] Vrgoč, H. (1999). *Aggressiveness (violence) in school*. Zagreb: Hrvatski pedagoško-književni zbor. Zagreb: Naklada Slap.

[7] Bilić, V., Buljan Flander, G., Hrpka, H. (2012). *Violence against children and among children*. Zagreb: Naklada Slap.

The definition is used as a basis for defining individual types of abuse. It is important to emphasize that there are different definitions of abuse: medical, legal and scientific definitions that are not identical, which makes research and practical treatment more difficult. Regardless of the specificities of each individual definition, all have in common an emphasis on the damage and suffering often inflicted by parents through their actions or lack of actions, i.e. neglect of the children's needs, whether physical or psychological[8].

When defining abuse, it is usually pointed out it involves: permanent or frequent exposure; deliberately violent means; which occurs in the context of a relationship of responsibility, trust and power; the consequences of which can be clearly visible in the form of injuries and endangerment or less noticeable emotional injuries and injuries to internal organs.

One of the important elements of abuse is permanent or frequent exposure, but it is necessary to emphasize that individual acts characterized as highly cruel, insolent and ruthless that endanger the child's health and life can also be identified as violent and abusive. One powerful blow can cause serious injuries, or sexual abuse can occur once, but the consequences will be long-term[9].

Discrimination, violence and abuse among children occurs when one or more children repeatedly or deliberately provoke, attack or injure another child who is unable to defend himself/herself based on his or her race, colour, ethnicity. Thus, violence can take the form of threatening, causing bodily harm, rejection from a peer group, humiliating on grounds of family or personal stigma, as well as teasing, gossiping, destroying and forceful taking of objects and belongings. The abuser or abusers often comment negatively about the family of the child which is who is faced with discrimination and violence[10].

In their textbook, the authors Bilic and Zloković (2004) cite the conceptual definition of a neglected and abused child: any child younger than eighteen, not cared for by his or her parents, manifested as lack of care for the upbringing, well-being, encouragement, social adaptation, education or other responsibility about the child's welfare.

The authors Bilic and Zlokovic also cite Polansky who defines child neglect as „a condition in which a care-taker responsible for the child either deliberately or by extraordinary inattentiveness permits the child to experience avoidable present suffering and/or fails to provide one or more of the ingredients generally deemed essential for developing a person's physical, intellectual, and emotional capacities."

The abuse of children as an immoral and inappropriate behaviour, regardless of whether it is in the form of discrimination, violence, abuse or neglect of a child, endangers and prevents the healthy and normal development of children and prevents the development of adaptive skills in the environment or family in which the children stay and live[11].

Bilic and Zlokovic (2004) cite two conceptual definitions of child abuse, as follows: a) child abuse is aggressive and usually rough behaviour to the child; b) abuse is any direct or indirect trauma or indirect exposure to discrimination and violence, primarily to family members.

---

[8] Bilić et al., cited, 2012.

[9] Bilić et al., cited, 2012.

[10] Kovačević, H., Buljan-Flander, G. (2005). Why me? Zagreb: Znanje.

[11] Bilić, V., Zloković, J. (2004). The phenomenon of maltreatment of children. Zagreb: Naklada Ljevak.

IV. Discrimination, violence and abuse during the historical development of society in family and school

4.1. Violence in the family during the historical development of the society

Physical, psychological and other types of punishment and abuse of children in the family have a long history. Physical punishment, which often transformed into psychological abuse as well, has been justified for decades as an educational method used for disciplining and teaching family and educational values and principles, whereas emotional abuse was considered to be normal. A large part of treatment that is now considered as discrimination, violence and abuse was not deemed to be inadequate or unacceptable during the historical development of society. Sometimes the children were considered personal property, and the parents had great power over them[12].

Zaninovic (2008) states that children in ancient Greece were raised by using harsh disciplinary methods, which was a characteristic of the Spartan culture at the time. These methods were applied to train children to fight with enemies, and to become strong and accustomed to various difficult and hardly tolerable living conditions such as very cold conditions, severe pain, suffering, hunger and thirst. Such an upbringing was aimed at strengthening their obedience and endurance. Apart from being exposed to violence, they were also trained to be harsh to others. They were encouraged to kill slaves they would encounter on the streets, and the Athenian women would take the young children to war so the children could see what awaits them through life's struggles, but also what they will do after they grow up. For preparing children for war and other Spartan activities in ancient Greece, children were starved, as most often decided by the father. In Sparta, this decision was made by a group of commanding elders. These acts and similar acts were not considered murder as they believed that the children would be saved by the gods.

In ancient Rome, there was a somewhat different upbringing, but not any gentler than in ancient Greece. In ancient Rome, all members of the family, including the elderly, were owned by their father. The father had absolute power over the whole family and the right to decide about life and death. New-borns would be placed before the father's feet, and if his father raised the baby, it had the right to life, otherwise it was sentenced to death. In old Rome, the father had all the powers, which meant that he could kill, sell or cripple a child, especially if the child had a weak constitution, was in poor health or had a physical injury, and the father would not be punished for that[13].

Children were killed not only in ancient Rome, but in various cultures, social classes and ethnic groups. During historical development of society, children were killed mostly by their own parents. New-borns and older children were killed for centuries in various civilizations and cultures. Biological mothers killed their new-borns motivated by fear of shame or condemnation by the society.

Embarrassment and fear would force the mother to commit such an act if the mather was not certain who the father was, or if the father was already married, or if the child was a great material burden, or due to infidelity in marriage (Lonza, 2001). Pediatrician Henry Dwight Chapin wrote during the 20th century that children who experienced physical and emotional neglect were placed in institutions during their first

---

[12] Tomison, A. M. (2001). A History of Child Protection. Back to the Future? Melbourne: The Australian Institute of Family Studies: Family Matters, 60.

[13] Bilić et al., cited, 2012.

year of life. Unfortunately, despite improved food and hygiene conditions, children died in 31.7 to 75% of cases due to infections and failure to thrive.

Pediatrician Henry Dwight Chapin began to place children without parents in foster homes in the United States. Studies consistently showed that children who were placed in institutions had an increased susceptibility to infections, as well as severe deficits in social development and control of behaviour and emotions. Even then it was understood that the cause was the emotional lack of the mother[14].

Scholars cite two types of child killing:

a) Passive killing – failure to properly care for the umbilical cord, failure to properly clean the respiratory tract, not giving the child sufficient food or exposing the child to cold.

b) Active killing - disabling the passage of air to the lungs due to blocking of airways caused by strangulation or choking, throwing the child or hitting the child on a hard surface, causing fractures and internal bleeding, ultimately leading to the death of the baby.

In the Dubrovnik Republic, new-borns were killed by drowning in the sea or in a well, thrown into the toilet or thrown from high altitudes (Lonza, 2001). It was not any different in other countries. For example, in feudal Japan, new-borns were killed by suffocation, while in China new-borns were drowned in cold water bins, and in India, in bottles filled with milk[15].

The reasons that led to the killing of children were: poverty, birth defects, superstitions and ignorance. The methods used by parents to kill their children are surprisingly cruel. One of the methods was abandoning the children and leaving them to die from hunger or animal attacks. Parents most often left those children who were weak or unwanted.

4.2. Violence in schools during the historical development of society

Violence against school children has existed during the historical development of society since schools have existed. The type of violence against school children has most often been corporal punishment that was considered an educational method. Children were punished in countries such as Egypt, Greece, Rome and others. The goal of these methods of corporal punishment was building and strengthening of the children's will and physical strength as recorded in Spartan schools[16].

In Yugoslavia, in the nineteenth and twentieth century, drastic methods were also applied in certain schools such as slapping children on the face on both sides, hitting the children's palms with a compass, bar, school ruler, etc. pulling students' sideburns or hair by twisting a tuft and even pulling out, and pulling the girls' braids by teachers along with slapping. There was also the method of kneeling with hands raised in the air, with grain of wheats, corn or other berries under the knees, applied in order to discipline children who would be late to school, who did not write their homework, prepared a recitation or children who were not obedient in class/school.

Miljkovic (2009, p. 35) describes Spartan disciplining methods as follows: „Until the age of seven, children were raised in families, but even then they were taught not to cry much as it was considered shameful to show pain. At seven years old, the boys went to

---

[14] Polyclinic for Protection of Children and Youth of the Zagreb City, Zagreb 2008., http://www.poliklinikadjeca.hr/publikacije/zanemarivanje-djece/ (accessed on 29.11.2018).

[15] Milner, J. S., Robertson, K. R., Rogers, D. L. (1990). *´Childhood history of abuse and adult child abuse potential´*. Journal of Family Violence, 5 (1), pp. 15-34.

[16] Bilić et al., cited, 2012.

state-owned schools. The schools were run by managers. All boys had to have closely shaved hair, and they slept on straw, without any covers. Both in summer and winter, they were barefoot and lightly dressed, and the food they received was very simple and - insufficient. In order to boost courage, the children were allowed to steal food, but if they were caught in the act, they would be severely punished. The manager had his own floggers who followed him everywhere, always ready to act. In order to help children become accustomed to pain, public flogging was organized every year in the town hall. Boys who would endure the flogging without crying out would be praised in front of the altar"[17].

These examples of the Spartan practice demonstrate cruelty, disrespect and strictness which are still associated with Spartan upbringing today. In the middle Ages, children were expected to be fully obedient based on the principle of „Magister dixit" (the teacher has said it), which would now be deemed as emotional punishment of children[18].

In Norway, the issue of abusers/victims were a subject of interest to the media, parents and society, but schools did not attach much importance and attention to this issue, until the end of 1982, when the newspapers announced that three boys between 10 and 14 years of age committed suicide because of peer violence. Not only did this event cause increased discomfort, attracted media attention and led to public tension, it also triggered a series of reactions that led to campaigns to resolve the problems related to bullying in all Norwegian primary and lower secondary schools initiated by the Ministry of Education in autumn 1983[19].

Bilic et al. (2012) argue that physical and psychological punishment in schools all over the world used to be justified as the best way to maintain order and discipline, by preventing children to violate the rules, in terms of respecting authority and as an aid in building character. The psychological and physical punishments included methods such as hitting children with a rod, strap or belt, books and hands, beating, immersion of children's heads in a container with cold water, and kneeling on corn or glass, or standing in front of a pillar of shame. All the punishments were made public so that everyone else would see the child's sin and shame him or her.

There are few scientific data on the use of physical and psychological punishment of children in schools. There is not a single recorded example of a teacher who kept records on how often and how he or she punished children by writing down how he or she used beatings, floggings, hitting by hand, hitting the children's palms, lips, heads, behind the ears, and hitting with books. These are statistical facts, or methods of teacher Haberle who worked for fifty years in a smaller German town[20]. The physical and psychological punishment methods in schools were so terrifying in nature and so widespread that the Prussian Minister of Culture announced in the media in 1899 that he demanded a decrease in the application of corporal punishment in schools because corporal punishment had already transformed into abuse[21].

---

[17]Miljković, D. (2009). *Pedagogy for Sports Coaches*. Zagreb: Faculty of Kinesiology of the Zagreb University.

[18] Bilić et al., cited, 2012.

[19]Olweus, D. (1998). *Peer violence in schools*. Zagreb: Školska knjiga.

[20] Tauš and Munjiza 2006; according to Bilić et al., cited, 2012.

[21] 24. Singer, M., Mikšaj-Todorović, Lj., Poldrugač, Z. (1985). *Criminality to the detriment of minors*. Zagreb: Školska knjiga.

V. Abusers of school-age children

The maltreatment of school-age children is characterized by aggressive and usually deliberately harsh actions towards the child. Any direct psychological and physical trauma or indirect exposure to violence, primarily within the family, is considered abuse[22]. In order to expose the causes, conditions and motives why a person abuses a child or children of school age, various etiological factors and characteristics of the abuser must be considered: how the bully and abuser behaves, what made him or her an abuser, whether there was domestic violence, how much influence his or her financial power has, what is the level of stability and support in the environment, and what is the abuser's marital status. All these factors are interwined and it is difficult to express their individual influences[23].

The US Department of Health and Human Services (USDHHS, 2010) defines abusers as persons who have caused or who possessed information on child abuse[24].

This definition of abusers seems very simple, but it is important to emphasize that USDHHS considers to be an abuser any person who has committed any methodological form of violence against children, including school-age children, but also any person who possesses any information on violence against a child, even only as an eyewitness or a direct participant. Every eyewitness is a type of abuser, since he or she has directly seen that a crime has been committed but failed to inform anyone or report the crime to competent institutions.

In addition, this definition applies to the person who has indications or assumes that violence is occurring but does nothing to help the abused child in the family, at school, in public and elsewhere[25].

We are witnesses to the problem of child abuse which is part of the basic value system of a modern society. A large number of humanitarian organizations in the world and in our country are active in combating and preventing the abuse and neglect of children, and the media are increasingly reporting on individual cases in which children become victims of the immediate or wider family, friends or another person[26].

VI. Types of abuse

A frequent type of abuse is physical punishment. The term physical punishment implies the application of physical force with the intention of inflicting physical pain and/or discomfort or psychological discomfort, but not injury, for the purpose of correction and control of the child's behaviour[27].

Physical abuse is inflicting injuries which may be „unintentional" or „unconscious" as a consequence of „disciplining a child" or different punishments which are inappropriate considering the child's age and physical development[28].

It is important to mention the fact that physical violence in some schools is so widespread and such a great problem that schools install video surveillance cameras and

---

[22] Bilić, Zloković, 2004, cited, p. 20.
[23] Bilić et al., cited, 2012.
[24] Bilić et al., cited, 2012, p. 66
[25] Bilić et al., cited, 2012.
[26] Šarić, 2011; according to Velki, Bošnjak, 2012.
[27] Straus, 2000; Pećnik, 2003; Gershoff, 2008; according to Bilić et al., cited, 2012, p. 82.
[28] Cicchetti, D., 1997, 38; Bilić and Zloković, 2004, cited.

metal detectors to prevent carrying of firearms and knives. There are even schools that employ armed guards (Field, 2004). Field (2004) lists the physical behaviors of bullies: a) pushing and knocking over, kicking and hitting; b) stealing various things from other students, from books and food to items from students' lockers; c) throwing the victim's belongings from one child to another; d) pulling a chair back while a student is trying to sit on it; e) hair pulling; f) carrying weapons; g) throwing erasers and papers at the victim etc.

There are various forms of physical abuse, including instrumental corporal punishment in which some parents use corporal punishment in a peaceful, thought-out and planned manner, without strong emotions, and impulsive corporal punishment caused by parents' anger, aggression, loss of control, and ultimately leads to a sense of guilt. It is important to note that corporal punishment is not only hitting a child's bottom or hitting with objects, but also includes some other physical forms:

a) Direct physical forms of punishment (pinching and shaking; stretching a child's ears and hair; hitting with hands or feet and various objects);

b) Forceful consumption of harmful substances (forcing a child to consume hot spices such as pepperoni and pepper; rinsing a child's mouth with baby soap);

c) actions involving excessive physical discomfort (forcing a child to sit in a painful position; kneeling on hard objects, for example, corn or pebbles; depriving a child of water or food; forcing a child to exercise excessively, for example 50 squats, push-ups or other exercises for punishment).

It is very important to distinguish protective restrictions, i.e. a parent's warning or quick reaction in the event of a child being in danger. Protective restrictions include sudden pulling and lifting of a child so it does not burn itself on a hot stove or does not run out on the street[29].

Parents are still unaware of the possible negative consequences of physical and psychological punishment and other forms of violence against children, and therefore it is necessary to continue to educate parents during parental meetings and various workshops on modern principles of upbringing, and what is good and bad for children[30].

Regarding the difference between discipline and corporal punishment, it is important to instruct parents to take a series of preventive and corrective actions to help their children regulate their behaviour. It is important to accept the reactions of the child, understanding the child's wishes and encouraging the child to make decisions and achieve better results.

Punishment and discipline are not synonyms, the more so because discipline involves upbringing. Upbringing methods, means and actions towards children achieve a positive discipline benefit indicating where the limits of acceptable or unacceptable behaviour are, thus developing awareness, character and morality about acceptable actions in the family, but also in society and the wider community.

VII. Neglecting children

Neglecting is failure to meet a child's needs to an extent that significantly affects the physical and psychological development of the child. It is not always deliberate, and the limit when neglect begins is not completely clear[31].

---

[29] Bilić et al., cited, 2012.

[30] Velki, T., Bošnjak, M. (2012). *The connection between parental upbringing methods and corporal punishment of children.* Život i škola: časopis za teoriju i praksu odgoja i obrazovanja.

[31] Bačan, 2006; Bilić et al., cited, 2012, p. 179.

Neglect, as a rule, is widely defined as failure of parents to care for and satisfy the emotional and developmental needs of the child, including the need for adequate nutrition, clothing, housing, health care, education, intellectual stimulation and emotional understanding[32].

Unlike child abuse, neglect is failure to do something, rather than directly causing injury or harm to a child. It is important to note that neglect only happens if lack of parental care endangers the healthy development of the child and his or her psychological/social balance[33].

Neglect represents 35 to 65% of all forms of abuse, and most of the victims are under three years of age. About 40% of deaths from abuse and neglect are the exclusive result of neglect due to failure to help the child, failure to provide medical treatment and drowning.

Children who are neglected were most often exposed to other types of abuse, and in a large number of cases, this was emotional or sexual abuse[34].

There are numerous causes[35] of neglect, and one of them is an inadequate parent-child relationship that does not depend only on the parent, but also on the child whose characteristics significantly influence the mutual relationship. The needs of each child are individual, as are the psychological and physical capacities of parents, therefore it is very difficult to explain in a few sentences what it is meant by failure to satisfy a child's needs. A parent who treats every child equally is not a good parent; a good parent is one who treats every child exactly as the child needs. People whose parents could not recognize their needs are often unable to recognize the needs of their own children, which, of course, leads to problems with children. It is important to know that failure to satisfy some of a child's needs can help the child to understand that the child cannot have everything in life immediately, which will contribute to him or her better coping with difficulties later in life. It is certainly neglect if one or more of the needs of a child are not satisfied for a long time or this situation is often repeated.

VIII. Peer violence

„Peer violence is defined as exposure to deliberately negative, repeated actions by one or more students of school age, of disproportionate real or perceived power, due to which a child suffers physical and/or emotional harm and is not able to resist such actions" (Olweus, 1993, 1998; Bilic et al., 2012, p. 266).

„Violence among children is every intentionally physically and psychologically violent behaviour directed towards children and young people by their peers, intended to cause harm, and which, regardless of where it occurs, can be distinguished by its phenomenological form, severity, intensity and duration, and which involves repetition of the same form and reflects an unbalanced relationship of strength (stronger against the weaker or groups against the individual)[36].

---

[32] White et al., 1987; Ajduković, Pećnik, 1994.

[33] Ajduković, Pećnik, 1994.

[34] Bilić et al., 2012.

[35] Jašarević, O., Kustura, M., *Criminology (Etiology and Phenomology of Criminality)*, Travnik, 2013, pg. 61-71.

[36] Jaman, A. (2009). *Violence among children in orphanages*. Školski vjesnik: časopis za pedagogijsku teoriju i praksu, 58 (3), 301-313. https://hrcak.srce.hr/82601, accessed on 27.11.2018,

Peer violence is often defined as a form of aggressive behaviour in which there is an imbalance of power between the victim and the bully, where the abuser has greater power, and such behaviour is often repeated[37].

Experience shows that violence among peers, particularly the child is exposed to violence for a long period of time, has very harmful consequences for further education, but also for the child's physical and psychological development. It is important to distinguish violence among peers from an attack or a common conflict among children. Peer violence can be direct such as through hitting and teasing, or indirect such as through exclusion from a group, gossiping or manipulating peers[38].

Peer violence as well as violence in schools have gained attention in recent years in many countries of researchers and scholars who deal with educational practices. Children who are exposed to abuse in school will very likely develop a negative attitude toward school and other students, and it will be increasingly more difficult for them to concentrate on fulfilling school-related obligations, tasks and learning the materials. In addition, in case of a lack of timely intervention by institutions through general and special prevention measures, it is possible that a child's physical and mental health will be endangered.

Children who are victims of violence show greater anxiety, depression and loneliness, and often express suicidal ideas that can lead to rejection by peers and worsening of relations with teachers[39].

IX. Protection of children and prevention in Bosnia and Herzegovina

Scientists and experts in the pedagogical field, regardless of where they work, whether in educational, health or other institutions dealing with children, have an obligation and responsibility to promptly report to the competent authorities and institutions any discriminatory, violent or abusive forms and actions towards children.

All institutions, according to their expert assessment, are obliged to report any suspicion of child abuse[40].

The Constitution of Bosnia and Herzegovina and the constitutions of other states in the region and wider treat children as a particularly vulnerable group which is entitled to all the rights to special social and political protection, i.e., the protection of society and the state. Therefore, the protection of children is regulated by numerous legislation: a) Convention on the Rights of the Child; b) Law on Social Protection; c) Family Law; d) Criminal Law; e) Law on the Protection of Patients' Rights; f) Law on Protection against Domestic Violence; g) Law on Primary Education; h) Law on Secondary Education.

Bosnia and Herzegovina is also a signatory to important international documents regulating the assistance to children and protection of children's rights, including the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, and the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse.

Constitutional provisions also stipulate that *„no one shall be subjected to any form of abuse (...)",* and the constitutional right to life without violence is determined by special

---

[37] Rigby, K. (2006). *Bullying in schools and what can we do?* Zagreb: Mosta. Rigby, 2002; according to Velki, Vrdoljak, 2013.

[38] Bilić et al., cited, 2012.

[39] Marušić, Pavin Ivanes cited, 2008.

[40] Bilić et al., cited, 2012.

regulations. In addition to the constitutional provisions, the legislation in Bosnia and Herzegovina stipulates that parents and other family members must not expose the child to humiliating circumstances or any type of violence or abuse. Each person who notices any violence against a child is required to inform the Social Welfare Center which is in turn obliged to examine each application and take all measures to protect the rights of the child.

X. Conclusion

Discrimination, violent behaviour, abuse and neglect of children of school age are an integral part of numerous criminological and criminal legal aspects of everyday life, and they occur in the family, kindergarten, school, media, politics and other institutions. Discrimination, violence, abuse and neglect of children most often take forms of discrimination based on national, religious, racial, ethnic grounds in terms of provocation, harassment, threats, causing bodily harm, mental pain in the form of rejection, teasing and forcible alienation, injuries and destruction of personal things. Discrimination, violence and abuse often include vulgar, embarrassing, provocative comments related to the child, but also to the child's family. Discrimination, violence and abuse among peers are most common in kindergartens and schools, but beyond the control of teachers and other professional educators. Discrimination, violence, abuse and neglect of children of school age may occur at any place where children live, socialize, play and spend leisure time.

There are several phenomenological forms of discrimination, violence, abuse and neglect of children in terms of physical and psychological harm, such as: intellectual, emotional, verbal, sexual, physical, cultural, economic and other criminological or criminal legal forms. Regardless of the phenomenological form of discrimination, violence, abuse and neglect, it is important to publicly expose the problems related to discrimination, violent behaviour and abuse among peers. It is thus highly important to talk with school-age children in a timely manner and to inform them that, in any case of any phenomenological form of discrimination, violence or abuse, the children can talk to their parents, parental councils, educators, kindergarten or school managers and teachers, but also police officers in the area where children stay, play, socialize and go to school.

With regard to discrimination, violence, abuse and neglect, it is important to communicate with parents as soon as a child has been enrolled in kindergarten or first grade of primary or secondary school. It is therefore important that educators, teachers and other pedagogical workers achieve a good relationship with parents, so they can cooperate during the educational process. Organizing educational workshops and professional programs will greatly assist parents, professionals but also school children to learn about the dangers and possible consequences of discrimination, violence, abuse and neglect. Such education programs can teach school children how to protect themselves from future forms of discrimination, violence and abuse, by developing mutual respect and tolerance. Kindergartens, schools, sports clubs and other educational institutions are not just spaces for transferring knowledge, but also spaces for learning and acquiring intellectual, social and practically dual life skills. It is therefore important to inform children in a timely manner who they can talk to in such cases, but also to educate parents to recognize discrimination, violence or abuse against their children so that they can talk to school teachers and other professionals as well as police officers in order to prevent any form of discrimination, violence or abuse in the most adequate manner possible. A good method of resolving these issues and gaining an

insight of what is happening is organizing an anonymous survey for school-age children. Given the honesty of children and anonymity, the chances are that the teachers and educators will know exactly what is happening and, in accordance with the information provided, can act in many ways through an institution or means of information.

Working with school-age children in groups and individually can be beneficial as children can be taught to what extent discrimination, violence and abuse are dangerous social phenomena, and how much they can damage the victims but also the discriminators, bullies and abusers. During professional trainings and workshops, parents, educators and other teaching staff can learn how to achieve positive communication with school-age children, how to provide support to children, how to solve conflicts painlessly and creatively, and how to develop a great level of trust and understanding among the children. It is important that school-age children know that they always have the support of adults, but it is especially important to include them in the decision-making processes, according to their interests and capabilities.

All deviant phenomenological forms of criminality[41], i.e., discrimination, violence and abuse of peers and school-age children should be approached in a very thorough, professional and serious manner, and the information to be taken into account includes absence of children from kindergarten, school and university lessons, poorer results and behaviour, damaged clothing, hunger, bruises or other injuries. It should be kept in mind, however, that there are often deeper injuries which are truly invisible but are painful and bear severe consequences. Some of the often visible signs in victims (school-age children) are the child's withdrawal or refusal to participate in working in a group in which the discriminator, bully or abuser is participating. The behaviour of the latter is terrorizing, hateful and aggressive, causing panic to the victim and thus affecting the child's healthy development.

Noticing these unusual gesticulated and mimicked signals can to a great extent prevent and reduce the occurrence of all etiological and phenomenological types and forms of discrimination, violence, abuse and neglect of school-age children.

Reference

1. Ajduković, M., Pećnik, N. *Abuse and neglect of children in the family*. Croatian Social Policy Review, 1 (3), 269-273. Taken from 27 studenog 2018, iz: https://hrcak.srce.hr/29726, (1994).

2. Bilić, V., Buljan Flander, G., Hrpka, H. *Violence against children and between children.* Zagreb: Naklada Slap, (2012).

3. Bilić, V., Zloković, J. *Phenomenon of maltreatment of children*. Zagreb: Naklada Ljevak, (2004).

4. Bulatović, A. *Consequences of abuse and neglect of preschool children. Life an school*, Journal of Theory and Practice of Education, 58 (27), 211- 221. Taken at 27 November 2018, from: https://hrcak.srce.hr/84275, (2012). 5. Centre for Social Welfare, Novi Marof at adress https://www.czss-novimarof.hr/2017/04/12/zastita-djece-braka-i-obitelji-i-skrbnistvo/ (accessed on 29.11.2018).

6. Field, E. M., *Living without violence*. Zagreb: Naklada Kosinj, (2004).

7. Forward, S., Buck, C. *Poison parents*. Zagreb: library Anima, (2002).

[41] Jašarević, O., Kustura, M., *Kriminologija (etiologija i fenomenologija kriminaliteta),* Univerzitet u Travniku, Pravni fakultet, 2013, pp. 163-184.

8. Hrabar, D. *Rights of children in the family*. Croatian Social Policy Review, 1 (3), 263-267. Taken at 29 November 2018, from https://hrcak.srce.hr/29717(1994).

9. Jaman, A. *Violence among children in homes for children without adequate parental care.* School Magazine: Journal of Pedagogical Theory and Practice, 58 (3), 301-313. Taken at 27 November 2018, from https://hrcak.srce.hr/82601, (2009).

10. Jašarević, O., Kustura, M., *Kriminology (etiologiy i fenomenology of kriminality),* Law university of Travnik.

11. Knežević, M., Baradić, *Information on a student behavioral questionnaire conducted among students. Life and school*, Journal of Theory and Practice of Education and Education, 50 (12), 76-86. Taken at 29 November 2018, iz: https://hrcak.srce.hr/25508, (2004).

12. Kocijan-Hercigonja, D., Hercigonja-Novković, V., *Children, youth and violence in family.* Medicus, 18 (2), 181-184. Taken at 28 November 2018, iz: https://hrcak.srce.hr/57167, (2009).

13. Kovačević, H., Buljan-Flander, G. *Why me?* Zagreb: Knoweladge, (2005).

14. Marušić, I., Pavin Ivanec, T. *Monitoring peer violence in primary schools: gender differences in frequency and types of violent behavior*. Annual of Social Work, 15 (1), 5-19. Taken at 27 November 2018, from: https://hrcak.srce.hr/23095, (2008).

15. Miljković, D., *Pedagogy for sports trainers*. Zagreb: Faculty of Kinesiology, University of Zagreb, (2009).

16. Milner, J. S., Robertson, K. R., Rogers, D. L. *´Childhood history of abuse and adult child abuse potential´*. Journal of Family Violence, 5 (1), 15-34., (1990). 17. MSD Manual for Diagnosis and Therapy at adress http://www.msdprirucnici.placebo.hr/msd-prirucnik/pedijatrija/zlostavljanje-djece (accessed on 29.11.2018.)

18. Olweus, D., *Violence between children at school*. Zagreb: Schools book.

19. Pećnik, N., *Intergenerational transmission of child abuse*. Zagreb: (1998). Naklada Slap, (2005).

20. Clinic for the Protection of Children and Young People of the City of Zagreb http://www.poliklinikadjeca.hr/publikacije/zanemarivanje-djece/ (29.11.2018.)

21. Rigby, K., *Violence at school, what we can do?* Zagreb: Mosta, (2006).

22. Sanderson, G. *Infliction of the child*. Zagreb: V. B. Z.,(2005).

23. Singer, M., Mikšaj-Todorović, Lj., Poldrugač, Z., *Crime against juvenile delinquency.* Zagreb: Schools book, (1985).

24. Singer, M., Grozdanić, V., Ljubin, T., Mikšaj-Todorović, Lj. *Criminology of Delicate Violence.* Zagreb: The Naked Bureau Globus, (2005).

25. Tomison, A. M., *A History of Child Protection. Back to the Future?* Melbourne: The Australian Institute of Family Studies: Family Matters, 60., (2001).

26. Velki, T., Bošnjak, M., *Relationships of parental educational practices with bodily punishment of children. Life and school*, Journal of Theory and Practice of Education, 58 (28), 63-81. Taken at 29 November 2017, from: https://hrcak.srce.hr/95244,(2012).

27. Velki, T., Vrdoljak, G., *The role of some peer and school variables in predicting peer violence.* Social Research, Journal of General Social Issues, 22 (1), 101-120. Taken at 27 November 2018, https://hrcak.srce.hr/101010, (2013).

28. Vrgoč, H. *Aggression (violence) in school.* Zagreb: Croatian Pedagogical-Literary Choir, (1999).

29. Zaninović, M., *The general history of pedagogy.* Zagreb: Schools book, (2008).

30. Zloković, J., *Violence among peers-the problem of family, school and society.* Pedagogical research, 1 (2), 207-219. https://hrcak.srce.hr/139356,(2004). Accessed on 29.11.2018.

Terrorism: between the need for funding and obtaining funding sources

Phd. Viorel Pașca[1]
Faculty of Law
West University Timișoara, Romania

PhD candidate Daniela Simona Orza
Faculty of Law
West University Timișoara, Romania

Abstract

The beginning of the 21-st century is characterized by globalization, instability, uncertainty, but also by the recrudescence of terrorism, which has become one of the main threats to human society and democracy.

An analysis of the evolution of international terrorism reveals that the actions taken are more and more dangerous due to the easier access of terrorist groups to financial resources, resources that enable them to acquire more and more sophisticated weaponry, technological and propaganda tools.

The number and severity of acts of terrorism varies depending on the financial infrastructure of the terrorist organization, which is why finding and attracting new sources of funding, new money-laundering methods and new ways of transferring funds has become an important objective.

The ways in which terrorist groups collect and transfer funds needed to fund their operations reveal that modern technologies that are in line with new trends (cryptovalute and darknet) but traditional means (zakat and hawala) are also used.

This paper examines the dependence of terrorists on financial funds, the methods of collecting and transferring these funds, and the efforts of the international community to counteract the phenomenon, for the fight against terrorism means, among other things, fighting in order to stop its funding.

Keywords: *terrorism, financing, financial funds, financing sources, legal instruments.*

I. Methods of Setting up and Transferring Funds used by Terrorist Organizations

We can talk about the financing of terrorism when someone, by any means, directly or indirectly, with illicit and intentional purpose, provides or collects funds in order to use them or knowing they will be used to commit a terrorist act.

As a result, investigating terrorism financing means tracking funds from the starting point to the destination, in other words, from the origin and up to those who use them to commit terrorist attacks, namely terrorist organizations or groups, lone terrorists or terrorist cells.

[1] Contact: viorel.pasca@e-uvt.ro

In terms of obtaining financial funds, terrorists can use both legal sources, such as: charities, nonprofit organizations, business sources, or even self-financing, but also illegal sources such as drug trafficking, oil trafficking, credit card frauds, extortion, kidnapping for ransoms, various taxes, and so on.

The success of a terrorist group means building and maintaining a strong financial infrastructure that can be achieved by finding sources of funding, money laundering and, last but not least, by finding methods for these funds to be used in order to obtain the necessary logistics for committing terrorist acts.

As a result, in the constant attempt to prevent and combat terrorism, stopping its funding could be one of the most powerful weapons.

That is why dismantling the financial networks of terrorist organizations and blocking their sources of funding has become the number one priority of anti-terrorism experts. Instead of intelligent bombs, explosive materials, commando troops and unmanned drones – economic sanctions, financial restrictions, and cyber-programs to detect and block money can be the most powerful weapons. This is the reality of the modern financial war[2].

In 2003, Dr. Rachel Ehrenfeld, a researcher in the terrorism funding field and director of the American Centre for Democracy, published the book entitled *„Funding Evil - How Terrorism is Financed - and How to Stop It,"* which for many years became the subject of intense legal controversy at international level and which has generated a series of libel judicial proceedings against the author. The book described the activities of various individuals, charitable organizations, banks, drug trafficking networks, or money laundering schemes. The book also discussed the involvement of certain groups, organizations and individuals, but also mentioned officials that were bribed in order to obtain the funds needed to finance the „evil".

Rachel Ehrenfeld paid special attention to the involvement of Iran, Hezbollah and Al-Qaeda organizations in drug trafficking, claiming that *„Bin Laden managed the drug trafficking profits for the Taliban and arranged money laundering operations with the Russian Mafia."* The author urged the entire international community to take firm measures against terrorist financing, including imposing economic sanctions on states that fund or encourage terrorism, such as Saudi Arabia, Iran, Syria, Sudan, Indonesia, Libya, North Korea and Malaysia[3].

It is clear that the commission of international terrorist acts requires important financial resources that terrorists, terrorist groups and organizations have to obtain by

---

[2] *Tom CW Lin, „Financial War Weapons", Minnesota Law Review, volume 100, p. 1377, Temple University, article available on papers.ssrn.com - accessed on May 20, 2019.*

[3] In *„Funding Evil - How Terrorism is Financed – and How to Stop It",* Rachel Ehrenfeld claimed that the Saudi billionaire Khalid bin Mahfouz has funded al-Qaeda through the bank and his charitable organization. Mahfouz denied the allegations and filed a lawsuit for libel. Although Rachel Ehrenfeld was a US citizen residing in New York, he was sued in London and although he refused to recognize the jurisdiction of the British courts, the British Court delivered a decision against her. In December 2004, before the end of the libel trial in London, Ehrenfeld sued bin Mahfouz at the District Court of the United States for the South District of New York on the grounds that the English court decision could not be enforced in the US, and that the allegations claimed could not be considered as „defamatory" under American law. In his complaint, she claimed that the rights conferred by the first amendment to the Constitution of the United States had been violated. As a result of these disputes, on April 29, 2008, the „*Rachel's Law*" was adopted, its goal being to provide to New York citizens greater protection against libel lawsuits settled in countries whose laws are incompatible with the freedom of expression granted by the Constitution of the United States. https://www.amazon.com/Funding-Evil-Terrorism-Financed, accessed on May 20, 2019.

various methods, given that each operation means costs that may be higher or lower depending on its magnitude.

On the other hand, terrorist organizations need large budgets to function as such. And because nowadays terrorism has become „global", its sources of funding have also acquired a global coverage.

1. The Need for Funds

The terrorist organizations have a constant need for funds, starting with the propaganda of ideology, recruitment of volunteers, preparing terrorist attacks, helping families of those who died in terrorist operations or those in prison, and so on.

Thus, the preparation of terrorist attacks (so-called pre-operational surveillance) involves the purchase of vehicles, weapons, explosive devices, the purchase of false identity documents, and travel and subsistence expenses.

Then, the terrorist organizations invest important funds in complex propaganda operations such as the publication of magazines and newspapers, or the acquisition of Internet domains and the management of web sites for the production and distribution of recruiting materials in order to disseminate their ideology and to attract new volunteers.

Other terrorist organizations use television and radio to promote their messages and ideas around the world. By way of example, *As-Sahab Media Foundation* represented, since 2000, the production facility dealing with the recording and transmission of Al Qaeda messages[4]. All these productions are either in English or subtitled in English, which shows that the terrorist organization is targeting a broader audience.

It is obvious that terrorists are willing to invest in the media to undermine the security of the population, to shortcircuit the daily routine of the people, but also to direct public opinion to state leaders, exerting pressure to meet or promote terrorist wishes and demands[5].

Another segment of the activity of terrorist organizations that requires serious financial resources is that of training and instructing the operational members in the use of weapons, the manufacture of craft bombs or clandestine communication. Also, the money is spent on buying buildings and land for training camps, for virtual training of members via the Internet, paying salaries for the leaders of groups and terrorist organizations, providing assistance to the families of those in prison or providing compensations for the families of the deceased[6].

At the same time, many terrorist organizations, in order to modernize their methods of action and to use the latest technologies, hired specialists such as: engineers, cybernetics, IT experts, economists, managers, physicians, former officers, which also, implied other costs.

Furthermore, a number of reports noted that Al-Qaeda and its affiliated groups use the anonymity provided by TOR encryption protocols[7].

---

[4] https://news.siteintelgroup.com/Jihadist-News/al-qaedas-as-sahab-media-launches-website.html, accessed on May 23, 2019.

[5] Cristian Delcea, *Ad Terrorism - The Relationship of Symbiosis between Terrorism and the Media, A.S.CT Publishing House, Cluj Napoca, 2007,* p. 22.

[6] FATF Report, Emerging Terrorist Financing Risks, Paris Cedex, October 2015, pp. 9-10.

[7] Software tool that provides the highest degree of anonymity on the Internet and allows anonymity to be maintained using a routing algorithm across a worldwide network of 5000 servers to

Last but not least, terrorist organizations need financial resources to support different social institutions that provide health and education services to population. With such actions, they seek to obtain local population support for the recruitment of new members within the terrorist organization.

In conclusion, it can be argued that terrorists have a permanent need for financial means to carry out their plans and to support the full range of activities that these plans involve and the destruction of terrorist financial resources is one of the most effective means of counteracting acts of terrorism.

I would also like to mention that on 12 February 2019, in a press release, the European Commissioner Dimitris Avramopoulos said the following: *„In order to catch criminals and terrorists, we must be able to track their money (...) fast access to financial information and better cooperation throughout Europe, makes any offender or suspect unable to evade our vigilance or hide away dirty money"*[8].

2. The Sources of Terrorism Financing

In regard to the sources of terrorism financing, they are also very diverse, and they may be legal or illegal.

2.1. Illegal Sources of Financing

Money for terrorist financing may come from a range of illegal activities, from minor crime to organized crime, such as drug trafficking, arms or human trafficking, extortion (threats, blackmail, use of violence) on the population in the areas in which they operate, or credit card frauds.

Another source of funding is the kidnapping activity, for ransom. The ransom value is based on the size of the terrorist group that the kidnappers are part of and the economic conditions in the geographical region where the terrorist operations are organized[9].

However, it is possible that the „origin" of money is sometimes legitimate in the sense that funds can be provided by means of donations of charitable organizations and non-profit organizations, given that such organizations benefit from public confidence, have large sources of funds, manage large amounts of cash and provide the necessary framework for financial transactions, both at national and international level.

Often, terrorists divert donor money and direct them to finance terrorist activities.

2.2. Obtaining Sources of Funding Through Means Specific to the Muslim Culture

Monetary practices embedded in Muslim culture, such as donating a portion of income to charities and various informal bank transfer centers, have complicated the already difficult task of tracking terrorist financial ties.

Thus, one of the pillars of Islam, *zakat*, refers to the mandatory granting of a certain percentage of each person's wealth for charity[10].

---

hide source and destination - Raphael Cohen-Almagor, *In Internet's Way*, International Journal of Cyber Warfare and Terrorism, 2, no. 3, July-September 2012, pp. 39-58.

[8] *12 February 2019 Brussels; Security Union: The Commission welcomes agreement on strengthening anti-terrorism financing rules - europa.eu/rapid/press-release_IP-19-1049_en.pdf; accessed on May 12, 2019.*

[9] Financial Action Task Force –FATF-, Groupe d'action financière-GAFI-, Terrorist Financing, Paris Cedex, pp. 11-19.

[10] *Zakat* is a voluntary charity tithe, normally 1/40 of income, paid as a religious obligation - *Tracking Down Terrorist Financing | Council on Foreign Relations https://www.cfr.org/.../tracking-down-terrorist-financing* - accessed on May 22, 2019.

In the Islamic world, there are tens of thousands of charitable organizations and among them only a few hundred may sponsor terrorism, but these are some of the richest charitable organizations[11].

While most of these Muslim world charitable organizations are created to help the poor and to spread the message of Islam, they have also been used, especially in the rich Middle East countries, to finance jihad.

2.3. Financing Terrorism by the use of Modern Technology

In recent years, terrorist organizations have discovered that they can also make money in the online environment, so they have begun to emerge themselves into the virtual environment.

Thus, US security services discovered a global financial network in 2017 that collected money, even from the US, to support „jihad."

Joseph Fitsanakisn, a security expert at Carolina University, highlighted the fact that, as of now, terrorist organizations have learned to use the crypto-currencies and the so-called darknet and to develop creative means to collect as much money as possible[12].

Today, modern technologies allow fast money transfers outside the international banking system and the use of virtual identities with a high degree of anonymity.

This has attracted the attention of many terrorist organizations interested in concealing illicit financial transactions and activities.

Therefore, the virtual decentralized currency or „crypto" are not only a new method of payment but also a potential instrument for terrorist funding entities due to anonymity, the absence of a centralized supervision body and global coverage.

At the same time, as I have shown above, the crypto currencies such as Bitcoin are a very modern method of transferring funds, making it almost impossible to track the financial flow of such funding[13].

Another method used for financing terrorism is „crowdfunding".

Crowdfunding is an alternative form of financing that creates a direct link between those who can give, borrow or invest money and those who need funding for a particular project. It usually refers to online public calls to help fund a personal project or adventure and consists in requesting the public openly to deposit funds online. Being an alternative way of financing, terrorists can easily access the money due to the fact that crowdfunding platforms rely on the anonymity of online presence and the global coverage of these platforms[14].

---

[11] J. Millard Burr, Robert O. Collins, *Alms for Jihad: Charity and Terrorism in the Islamic World*; Cambridge University Press, 2006.

[12]https://www.coastal.edu/academics/facultyprofiles/humanities/politics/josephfitsanakis/facultyprofile.php - accessed on 17-th May 2019.

[13] Bitcoin (BTC) was created in January 2009 by Satoshi Nakamoto and consists of 64 digits. Any interested person can create this coin on specialized sites using a specialized program and performing computers. In order to obtain the BTC, a virtual wallet (Bitcoin wallet) must be created and the transmission of the currency is made via the Internet as simple as sending an e-mail to anyone who has a bitcoin address. Transactions with BTC are not recorded at any central bank or brokerage firm, the currency being created by a peer to peer (peer-to-peer) computer network, so that the BTC does not depend on a central bank but on the importance which people attach to this coin - N. Malik, *„Terror in the Dark - How Terrorists Use Encryption, the Darknet, and Cryptocurrencies*" - article available at http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf, accessed on April 5, 2019.

[14] https://ec.europa.eu/info/business-economy-euro/growth-and-investment/financing-investment/crowdfunding_en, accessed on 21-st May 2019.

3. The Transfer of Terrorist Funds

Funding of terrorist activities often requires the transfer of money and values within states or between different jurisdictions.

There are three main ways in which terrorists transfer money or transfer values, namely: by using the financial system, by official channels of the financial market or by unregulated channels, respectively, by using couriers for cash - which implies the physical movement of money through the international trading system.

The diversification and multiplicity of the organizational structures of terrorist networks and the continuous evolution of the techniques used by them in response to international actions to stop fund transfers for terrorist purposes makes it difficult to identify a preferred or common method for organizations of this kind.

In most cases, in order to transfer funds, terrorist organizations alternately use all three methods of money transfer.

However, as a rule, the funding of a terrorist group is easier to achieve through the conventional banking system – so that money sent from one country to another can go into accounts with false names, charitable organizations or other enterprises meant to hide the final recipient.

Furthermore, the identification and discontinuation of terrorist financing are naturally more difficult to achieve when authorities face „informal" support networks. In such circumstances, the links between the financial activity and terrorism become more opaque and the disruption of funding by the authorities more difficult to achieve. On the other hand, the links between funds and terrorism can be extremely difficult to find in the country of origin, when the terrorist activity occurs in a whole other part of the world.

3.1. Transferring Funds by Means Specific to the Muslim Culture

Since many terrorist groups operate in areas with poor infrastructure, where modern technology and telecommunication tools penetrate harder, and given that terrorists need physical currency, they often use a traditional muslim money transfer method called *hawala*.

In Arabic, „*hawala*" means „*transfer*," and in certain contexts, the word *„hawala"* is synonymous with „*trust*", usually expressing the personal link between the participants and the informal nature of transactions that are not officially documented.

In essence, hawala is a transfer or hand-over of money from one side to another without the use of a formal financial institution such as a bank or exchange office, as it is an „informal" transaction[15].

Thus, the client contacts the hawala broker and gives him an amount of money to transfer it to a beneficiary in a particular country, along with the beneficiary's identification data. The hawala broker contacts his counterpart in that country and asks him to remit that amount to the beneficiary. The hawala operator in that country contacts the beneficiary on the same day and hands over the amount sent, usually in local currency or another currency accepted by both parties, with a course different from the official one, and the beneficiary is not being identified, being used only a recognition code. The transfer takes from a few hours to a day or two. Usually the

---

[15] Remus Jurj-Tudoran, *Terrorism Financing - Judicial Theory and Practice* in ProLege Magazine Oct. 10 2018, article available on revisleprolege.ro/finantarea-terorismului- teorie-si-practica-judiciara/ - accessed on 25-th May 2019.

customer is in touch with the beneficiary and sends him the contact person's name, that is, the name of the hawala broker. For this transfer, the hawala broker charges a fee from the amount so transferred, which is lower than the bank fee and which is usually paid on the spot because the costs are minimal[16].

What is specific to *hawala* is that these transactions cross international borders, usually involve more than one currency and involve middle men who usually hold financial positions[17].

3.2. The Reaction at the European Level

In response to these traditional forms of transfer of funds or to unofficial value transfer systems, the European Parliament and the Council are to adopt a new Regulation on the control of cash entering or leaving the Union and repealing the Regulation (EC) no 1889/2005 of the European Parliament and of the Council of 26 October 2005[18] which establishes an obligation for agents carrying out such transactions to declare to the competent authorities each significant operation carried out through such systems.

In this respect, any middle man and/or person involved in this type of activity (supervisors or exchange agents, middle men and distributors, coordinators, collectors and transmitters) will be required to register with the competent national authority; all operations must be declared and documented in a way that facilitates the transfer of information upon request, and dissuasive sanctions for those middle men and/or other persons involved in undeclared activities are to be instituted and applied. It remains to be seen, however, whether the regulation will have the expected result.

II. Legal Instruments in the Field of Combating Terrorism Financing at International Level

1. The Palermo Convention Against Transnational Organized Crime

At international level, the transatlantic countries, reunited either in the United Nations or in the „Group of Eight" (G8), have been the main factor in uniting global and regional instruments to optimize actions to prevent and combat terrorism financing[19].

---

[16] *Idem*.

[17] Robert Looney, *Hawala: mecanismul financiar informal al teroristului*; nr.1, Volumul X Hawala: The Terrorist's Informal Financial Mechanism | Middle East... Politici Council, *https://www.mepc.org/ .../hawala-terrorists-informal-financial* - accesat la 7 mai 2019.

[18] Published in the Official Journal of the European Union 238-32005R - 1989, L.309 / 9) COM / 2016/0825 final - 2016/0413 (COD) - European Parliament legislative resolution of 12 September 2018 on the proposal for a regulation of the European Parliament and of the Council on the control of cash entering or leaving the Union and repealing Regulation (EC) No. 1889/2005 (COM(2016)0825 – C8-0001/2017 – 2016/0413(COD).

[19] The Group of Eight „(G8) is an international forum of governments of economically, technologically and militarily developed countries. The G8 includes Canada, France, Germany, Italy, Japan, the United Kingdom and Northern Ireland, the United States and Russia, which, although accounting for about 14% of the world's population, account for 60% of gross domestic product worldwide, accounting for about 72% of the world's military spending. France, Russia, the United Kingdom and the United States hold more than 95% of the world's nuclear weapons. In March 2014, after the annexation of Crimea, Russia was suspended temporarily; currently the international forum refers to 7 states, the G7; available on: https://en.wikipedia.org/ wiki/Group_of_Eight, accessed on May 29, 2019.

On 13 December 2000, the United Nations issued the Palermo Convention[20] against transnational organized crime[21] the goal of which was to promote cooperation of states in order to prevent and combat organized crime more effectively.

In this regard, article 7 of the Convention, entitled *Measures to combat money laudering*, provides, among others, that each state party shall institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions and, where appropriate, other bodies particularly susceptible to money-laundering, within its compe- tence, in order to deter and detect all forms of money-laundering.

2. Financial Action Task Force on Money Laundering (FATF)

An important role in combating global terrorism financing is the FATF International Financial Action Task Force[22].

The Financial Action Task Force on Money Laundering (FATF) is an intergovernmental organization founded in 1989 to develop anti-money laundering policies and, since 2001, it has also been involved in combating terrorist financing.

FATF issues international standards and recommendations in the field of countering global terrorism financing, monitors the legislative, financial and law enforcement activities taken at national and international level. The issued recommendations cover the criminal justice system and law enforcement, international cooperation, the financial system and its regulation.

3. The International Convention on the Suppression of Terrorist Financing

The International Convention on the Suppression of the Financing of Terrorism was adopted under the aegis of the United Nations in New York on 9th December 1999[23].

In the Convention, the offense of terrorist financing is defined in art. 2 par. 1 and refers to *„any person who by any means directly or indirectly illegally and deliberately provides or collects funds with intent to use them or knowing that they will be used, in whole or in part, to the commission of: (a) an act constituting an offense within the framework and as defined in one of the Treaties listed in the Annex[24]; (b) any other act that*

---

[20] Published in the Official Gazette no. 813/8 November 2002.

[21] Available on *www.cdep.ro/pls/legis/legis_pck.htp_ act_text? Idt = 38601*, Accessed on May 18, 2018.

[22] The FATF is an intergovernmental structure, founded in 1989, headquartered in Paris, which sets international standards, develops and promotes policies to combat money laundering and terrorist financing. It currently has 33 members: 31 countries and governments and two international organizations; 20 observers: five FATF regional structures and more than 15 other international organizations or bodies. A list of all members and observers can be found on the FATF website at http://www.fatf-gafi.org/Members.en.htm, acessed on 30 May 2019.

[23]Available at https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-11&chapter=18&clang=_en.

[24] The Annex to the International Convention on the Suppression of Terrorist Financing includes the following conventions: 1. Convention for the Suppression of Illegal Hijacking of Aircrafts (The Hague, 16 December 1970); 2. Convention for the Suppression of Unlawful Acts against Civil Aviation Security (Montreal, 23 September 1971); 3. Convention on the Prevention and Suppression of Offenses against Persons enjoying International Protection, including Diplomacy Agents, adopted by the General Assembly of the United Nations on 14 December 1973; 4. The International Convention against the Taking of Hostages, adopted by the United Nations General Assembly on 17 December 1979; 5. International Convention on the Physical Protection of Nuclear Material (Vienna, 3 March 1980); 6. Protocol on the suppression of illicit acts of violence at airports serving international civil aviation, complementary to the Convention for the Suppression of Unlawful Acts against Civil Aviation Security (Montreal, 24 February 1988).

may cause the death or serious injury of a civilian or any other person not directly involved in hostilities in an armed conflict when, by its nature or context, that act is aimed at intimidating the population or forcing a government or an international organization to fulfill or refrain from performing any act".

On May 16, 2005, in Warsaw, the Council of Europe issued the Convention on the Prevention of Terrorism[25]. The objective of the Convention, according to its Article 2, was to *„intensify the parties' efforts to prevent terrorism and its negative effects on full respect for human rights, and in particular the right to life, both by means of measures taken at national level, as well as in the framework of international cooperation, taking into account bilateral or multilateral treaties or agreements between contracting states"*[26].

4. The additional Protocol to the Council of Europe Convention on the Prevention of Terrorism[27]

The Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism[28] was adopted in Riga on 22 October 2015 in order to complement the provisions of the Council of Europe Convention on the Prevention of Terrorism as regards the criminalization of the deeds described in Articles 2 to 6, thereby enhancing the efforts of states parties to prevent terrorism and its negative effects on the full exercise of human rights, in particular the right to life.

Article 5 of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism criminalizes the act of financing travel abroad for terrorist purposes as follows:

For the purposes of the Protocol, *„financing the travel abroad for terrorist purposes"* refers to the provision or collection in any way, directly or indirectly, of funds which, wholly or in part, facilitate the travel of any person for terrorist purposes abroad as defined in Article 4, paragraph 1, of the Protocol[29], being aware of the fact that the funds are wholly or partly intended to serve this purpose, and according to paragraph 1, each Party shall take the necessary measures to regulate as an offense according to its domestic law to fund the travel abroad for terrorist purposes as defined in paragraph 1, when committed with intent.

5. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing the Council Framework Decision 2002/475 / JHA and amending the Council Decision 2005/671 / JHA

Article 11 of EU Directive 2017/541 of the European Parliament and of the Council[30] regulates anti-terrorist financing measures as follows: *1. The Member States*

---

[25] Published on 22.06.2018 in the Official Journal of the European Union.

[26] Article 2 of the Convention on the Prevention of Terrorism.

[27] Adopted at Riga on 22 October 2015; Published in the Official Journal of the European Union no. L 159/17 of 22 June 2018.

[28] Available on the website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217, accessed on May 27, 2019.

[29] Article 4, paragraph 1 of the Additional Protocol to the Convention of the Council of Europe on the Prevention of Terrorism. *For the purposes of this Protocol, „traveling abroad for terrorist purposes" means traveling to a state which is not the state whose national citizen or resident is the person who is traveling, for the purpose of committing or contributing to committing or participating in a terrorist act, or providing or acquiring training for terrorism.*

[30] Published in the Official Journal of the European Union L88 / 6 EN of 31.03.2015, available at https://publications.europa.eu/en/publication-detail/-/publication/.../language-ro accessed at 31 May 2019.

shall take the necessary measures to ensure that the provision or collection of funds by any means directly or indirectly, with the intention of using them or knowing that they will be used wholly or in part to commit any of the offenses referred to in Articles 3 to 10 or to contribute to committing any of those offenses, shall be criminalized as a criminal offense when committed with intent.

2. If the financing of the terrorism referred to in paragraph (1) of this Article relates to any of the offenses referred to in Articles 3, 4 and 9, it shall not be necessary for the funds to be used, in whole or in part, with the purpose of committing or contributing to the commission of any of the offenses concerned, nor is it obligatory for the author to know the offense or specific offenses for which the funds are to be used.

6. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directives 2009/138 / EC and 2013/36 / EU

The main legal instrument to prevent the use of the European Union's financial system for the purpose of money laundering and terrorist financing is the Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018.

The Directive establishes *„more effective and comprehensive measures for the financing of terrorism, measures to be taken while complying with the fundamental right to the protection of personal data and complying with international commitments and the application of the proportionality principle"*[31].

The preamble to the Directive states that trends in how terrorist groups finance and carry out their operations reveal that modern technology services have become increasingly popular as alternative financial systems and, in keeping up with the new trends, further steps should be taken to ensure greater transparency of financial transactions, corporate entities and other legal entities, as well as trusts and legal constructions with a structure or function similar to trusts, (...) in order to improve the current prevention framework and to combat in a more effective manner the financing of terrorism. It is important to note that the measures taken should be proportionate to the risks[32]. The Directive defines terms such as „electronic money", „virtual currency", „digital wallet provider"[33].

The objective of the Directive, namely the protection of the financial system by preventing, detecting and investigating money laundering and terrorist financing, can not be achieved individually by the Member States, as the measures adopted by them to protect their financial systems may be incompatible with the functioning of the internal market, the principles of the rule of law and the Union's public policy. This desirability can therefore be better achieved at Union level, which can adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union.

---

[31] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directives 2009/138 / EC and 2013/36 / EU, published in the Official Journal of the European Union at 9 06 2018, L 156/43.

[32] Paragraph 2 of the preamble to the Directive.

[33] Article 3 (c) point 16; art. 3 (d) pt.18; art. (EU) 2018/843 of the European Parliament and of the Council amending Directive (EU) 2015/849 and amending Directives 2009/138 / EC and 2013/36/EC (3) (d).

Article 4 of the Directive specifies that the Member States are required to bring into force the laws, regulations and administrative provisions necessary to comply with the Directive by 10th January 2020.

III. The Terrorist Financing Offense in Domestic Law

In domestic legislation of Romania, the financing of terrorism is criminalized in art. 36 par. (1) of the Law no. 535/2004 on preventing and combating terrorism as follows: *„it is a terrorist financing offense to collect or make available, directly or indirectly, licit or illicit funds, knowing that they are to be used, in whole or in part, for committing acts of terrorism or for supporting a terrorist entity „.*

At the same time, paragraph 2 of art. 36 of Law no. 535/2004 establishes that *„The commission of a crime for the purpose of obtaining funds with the intention of being used or knowing that they are to be used wholly or partly for the purpose of committing acts of terrorism or for supporting a terrorist entity is punishable by the punishment specified by law for that offense, the maximum of which is increased by 3 years."*

As far as *„terrorist entities"* are concerned, they are defined in art. 4 point 1 of the Law no. 535/2004 as a person, grouping, structured group or organization that: a) commits or participates in terrorist acts; b) is preparing to commit terrorist acts; c) promotes or encourages terrorism; d) supports, in any form, terrorism.

„The terrorist actions" are defined in art. 4 point 7 of Law no. 535/2004 as *„the preparation, planning, favoring, commissioning, directing, coordinating and controlling the terrorist act, as well as any other activities carried out after its committing, if related to the terrorist act".*

It should be noted that, following the review of Recommendation no. 5 and the FATF Glossary of October 2016, it is recommended that the provisions on terrorist financing offense also apply to the provision or collection of funds or other assets that explicitly include economic resources, including oil and other natural resources, dividends and asset income and any other assets that are not funds but could be used to obtain funds, goods or services[34].

Law no. 535/2004, defines, at art. 4, point 8, the term „funds" as „goods of every kind, tangible or intangible, movable or immovable, acquired by any means and documents or legal instruments in any form, including electronic or numerical form, property rights or interest in such goods, bank credits, traveler's checks, bank checks, mandates, shares, securities, bonds, special drawing rights and letters of credit, without being enumerated as limiting.

The active subject of the offense can be any person who is criminally liable, including a legal person, and this offense can be committed in all forms of participation: co-sponsorship, instigation and complicity.

The primary passive subject of the offense may be the state as the holder of protected social values and secondary passive subjects may be charitable organizations, banks and financial agencies by which transfers of funds are made to finance terrorist acts or organizations.

The *actus reus* consists of an action, namely to collect or make available, directly or indirectly, funds.

---

[34] FATF Guidance, *„Criminalising Terrorist Financing (Recommendation 5*) - available at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Criminalising-Terrorist-Financing.pdf, accessed on 25-th May 2019.

In order to be considered a terrorist financing offense, it is not necessary for the financing of terrorist organizations to result in the commission of a terrorist act but may have any purpose designed to support the capacity of the terrorist organization to prepare and organize such attacks.

The immediate consequence is the state of danger created for socially protected relations and implicitly derives from the commission of the offense.

As regards the subjective side of the terrorist financing offense, the perpetrator's guilt takes the form of direct or indirect intent.

No law is immutable, and Law no. 535/2004 even less. It has undergone changes following the entry into force of Law no. 58/2019 which amends and complets Law no. 535/2004 on preventing and combating terrorism[35] and will probably be followed by others in order for its provisions to comply with those contained in Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, the deadline being 10th January 2020**.**

However, it is clear that, in countering the terrorist phenomenon, it is important to reduce the sources of income of terrorist entities, which must be achieved only by legal instruments, by clear and transparent regulations in line with technological developments, a unique definition of terrorism, and of terrorist offenses, both in the Member States of the European Union and in the other countries of the world.

IV. Conclusions

As W. Lacqueur states, *„Modern terrorists, unlike their predecessors, do not subsist only with enthusiasm but need a lot of money"*[36].

As a result, discontinuing funding flows, dismantling or banning these flows may, over time, limit the ability of terrorist groups to launch attacks, because in the absence of funds, risks of failure of planned operations are increasing.

Even if some terrorist acts do not require high costs, terrorist organizations need financial resources for propaganda, recruitment, to buy weapons and information to create a favorable environment for their activities. In other words, the destruction of the funds needed for terrorist activities leads to diminishing the capacities of action, limiting their impact and effect.

Moreover, knowing how terrorist groups and networks finance their activities is essential both for understanding their functioning and for taking measures to dismantle financial networks and stop their funding sources.

Although financial information alone is not enough to combat terrorism, however, when combined with other counterterrorism measures, financial information can greatly increase the ability of a country to identify and counteract terrorist activity. And as terrorist financing offenses are cross-border, it is necessary that strategies in the field be based on cooperation and exchange of information between services specialized in combatting terrorist financing.

With the specific purpose of enhancing the capacity of law enforcement, prevention and response to terrorist financing, the European Parliament issued the

---

[35] Published in the Official Gazette no. 271/10 April 2019.

[36] W. Lacqueur, *The Age of Terrorism. A Completely Revised and Expanded Study of National and International Political Violence, Based on the Author's Classic Terrorism,* Ed. Little, Brawn & Co, New York, 1987, p. 96.

Recommendation of 1 March 2018 to the Council, the Commission and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy on cutting sources of the Jihadists' income. It was considered that the establishment of a system for monitoring worship places and religious schools, institutions, charitable foundations and cultural associations where there is reasonable suspicion that they are related to terrorist groups may provide details on the source of the funds they receive and how the funds are distributed.

This is why finding and eliminating the financial sources of terrorist networks should become an essential component of all anti-terrorist investigations.

References

1. *Lin, Tom C.W., „Financial War Weapons", Minnesota Law Review, volume 100, p. 1377, Temple University, article available on papers.ssrn.com - accessed on May 20, 2019.*

2. Ehrenfeld, Rachel, *Funding Evil - How Terrorism is Financed – and How to Stop It",* https://www.amazon.com/Funding-Evil-Terrorism-Financed, accessed on May 20, 2019.

3. https://news.siteintelgroup.com/Jihadist-News/al-qaedas-as-sahab-media-launches-website.html, accessed on May 23, 2019.

4. Delcea, Cristian, *Ad Terrorism - The Relationship of Symbiosis between Terrorism and the Media, A.S.CT Publishing House, Cluj Napoca, 2007.*

5. FATF Report, Emerging Terrorist Financing Risks, Paris Cedex, October 2015.

6. Cohen-Almagor, Raphael, *In Internet's Way*, International Journal of Cyber Warfare and Terrorism, 2, no. 3, July-September 2012.

7. *europa.eu/rapid/press-release_IP-19-1049_en.pdf; accessed on May 12, 2019.*

8. Financial Action Task Force – FATF, Groupe d'action financière-GAFI-, Terrorist Financing, Paris Cedex, pp. 11-19.

9. Council on Foreign Relations, *Tracking Down Terrorist Financing,* https://www.cfr.org/.../tracking-down-terrorist-financing, accessed on May 22, 2019.

10. Millard Burr, J., Collins, Robert O., *Alms for Jihad: Charity and Terrorism in the Islamic World*; Cambridge University Press, 2006.

11. https://www.coastal.edu/academics/facultyprofiles/humanities/politics/josephfitsanakis/facultyprofile.php, accessed on 17-th May 2019.

12. Malik, N., *Terror in the Dark - How Terrorists Use Encryption, the Darknet, and Cryptocurrencies* - article available at http://henryjacksonsociety.org/wp-content/uploads /2018/04/Terror-in-the-Dark.pdf, accessed on April 5, 2019.

13. https://ec.europa.eu/info/business-economy-euro/growth-and-investment/financing-investment/crowdfunding_en, accessed on 21-st May 2019.

14. Jurj-Tudoran, Remus, *Terrorism Financing - Judicial Theory and Practice* in ProLege Magazine Oct. 10 2018, article available on revisleprolege.ro/finantarea-terorismului- teorie-si-practica-judiciara/ - accessed on 25-th May 2019.

15. Looney, Robert, *Hawala: mecanismul financiar informal al teroristului*; nr.1, Volumul X, Hawala: The Terrorist's Informal Financial Mechanism | Middle East... Politici Council, *https://www.mepc.org/.../hawala-terrorists-informal-financial*, accessed on 7 mai 2019.

16. https://en.wikipedia.org/wiki/Group_of_Eight, accessed on May 29, 2019.

17. *www.cdep.ro/pls/legis/legis_pck.htp_ act_text? Idt = 38601*, accessed on May 18, 2018.

18. FATF website, http://www.fatf-gafi.org/Members.en.htm, acessed on 30 May 2019.

19. https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-11&chapter=18&clang=_en.

20. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217, accessed on May 27, 2019;

21. Official Journal of the European Union L88 / 6 EN of 31.03.2015, available at https://publications.europa.eu/en/publication-detail/-/publication/.../language-ro, accessed at 31 May 2019.

22. FATF Guidance, *Criminalising Terrorist Financing (Recommendation 5*) - available at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Criminalising-Terrorist-Financing.pdf, accessed on 25-th May 2019.

23. Lacqueur, W., *The Age of Terrorism. A Completely Revised and Expanded Study of National and International Political Violence, Based on the Author's Classic Terrorism,* Ed. Little, Brawn & Co, New York, 1987.