UNIVERSITY OF TIMISOARA
FACULTY OF LAW

UNIVERSITY OF PÉCS
FACULTY OF LAW

JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW

No. 1/2020

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

2020

Universul Juridic Publishing House

Edited by Universul Juridic Publishing House

Copyright © 2020, 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:	Ciprian Radu
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. MIHÁLY TÓTH
Dr. IOANA CELINA PAȘCA
Dr. LÁSZLÓ KŐHALMI
Dr. ZOLTÁN ANDRÁS NAGY
Dr. CSABA FENYVESI
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, centered, 14)

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

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

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 July 2020. The main topic of the future issue is: **New Technologies and the Criminal Justice System.**

THE BOARD OF EDITORS

Contents

THE IMPACT OF NEW TECHNOLOGIES ON THE CRIMINAL JUSTICE SYSTEM

Shenkuo Wu*
Cybersecurity Obligations of ICT Companies in P. R. China 9

Bogdan Bodea
Argument Regarding the Need to Incriminate Computer Data Input Forgery Committed by an Official 22

Füszter Erzsébet
New Technical Devices and Methods in Crime Scene Investigation 29

Andrea Kraut, László Kőhalmi, Dávid Tóth PhD
Digital Dangers of Smartphones 36

Aleksandar R. Ivanović
Hate Speech in Electronic Media and Challenges for the Criminal Justice System of the Republic Of Serbia 50

Zoran S. Pavlovic, Nikola Paunovic
The Impact of Misuse of Cryptocurrencies in Combating Money Laundering and Terrorist Financing 66

Silvia Signorato
Streamlining the Fight Against Child Sex Offenders Trough EU Regulation of IP address 77

Matei-Ciprian Graur
Videoconference in Criminal Proceedings – Between Ideal and Current Social Reality 87

VARIA

Dragan Jovašević
Juvenile Institutional Criminal Sanctions in The Law System of Republic of Serbia 95

Nenad Avramović, Marijana Mladenov
Some Controversies on Modern Terrorism 112

Dragana Ćorić
The Importance of Thought Experiments 127

Ervin Belovics
Requirements for Criminal Law 136

Flaviu Ciopec
Far and Beyond Territory. Lessons for the EU from the US Legal Practice.....147

Dr. László István Gál
The Possible Impact of the COVID-19 On Crime Rates in Hungary 165

Ioana Celina Paşca
Is Terrorism an International Crime? 177

Cybersecurity Obligations of ICT Companies in P. R. China

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, ICT technologies, P.R. 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

---

* 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, n. 1, p. 37.

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.

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

[2] On the practical perspective of "Internet Plus" Action Plan, see Li Congyuan, Future of "Internet Plus" Action Plan, in Information Research, 2018, n. 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, n. 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, n. 31, p. 37.

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 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

---

[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, n. 2, p. 115.

[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, n. 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, n. 5, p. 21.

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.

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 IX 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

[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, n. 5, p. 1.

[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, n. 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, n. 4, p. 156.

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.

(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:

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).

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.

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.

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 considered 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 analysis).

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 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 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.

---

[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, n. 1, p. 10.

[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, n. 5, p. 25.

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.

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 Counterterrorism Law of 2015.

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.

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.

---

[13] On the principle of no obligation conflict in China, see Liu Sheng, Studies on the Obligation Conflict, in Law and Economy, 2011, n. 4, p. 9.

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 provisions of this Law and cause other people to suffer damage, they shall bear civil liability according to law.

Also 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.

---

[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, n. 1, p. 15.

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. Liao Jingwei-Yu Juan, *Research on the Big Data Industry*, in Modern Business Trade Industry, 2018, n. 6, p. 7.

4. Li Haiying, *Digital Economy and International Cooperation on Cyberspace*, in Civil-Military Integration on Cyberspace, 2018, n. 6, p. 24.

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.

Zhang Boqin-Sun Shuyang, *2019 Development Trend Prospects of Network Security in China*, in Cyberspace Security, 2019, n. 1, p. 37.

Argument Regarding the Need to Incriminate Computer Data Input Forgery Committed by an Official

Dr. Bogdan Bodea[1]

Abstract

As digital format becomes a necessity, public authorities need to adapt to this concept and the law must follow. Up until now, authorities kept different records in a written form and they conducted their activity exclusively in writing, as the written form provided both certainty of the existence of the act and of its content.

The incrimination under art 325 falls short in offering adequate protection of public confidence in the authenticity of digital documents and the veracity of stipulations recorded in them, as it does not sanction the act of inputting false data committed by a public official acting within his right to input data.

Keywords: *Computer data, forgery, acting without right, fraudulent, public official*

I. General Considerations Regarding the Need to Protect New Social Values

The Global pandemic of 2020 has taken its toll on society through digitalization. More and more we see that working online or in a digital format becomes a necessity, and public authorities need to adapt to this concept.

Nevertheless, in some areas, the law falls short as traditionally all the work of public authorities was done in writing. Up until now such authorities kept different records in a written form and they conducted their activity exclusively in writing, as the written form provided both certainty of the existence of the act and of its content.

Times are changing fast and we believe that they would have changed regardless of the current crisis, as more and more authorities embrace the need of digitalization and as more and more people are accustomed to use modern means of communication on a daily basis.

The technology enters our lives and therefore changes our behaviour thus creating the need to protect new social values, as they arise. In this context, considering the transition from non-digital to digital it proves necessary to incriminate new offences such as data forgery[2]. As society fights cybercrime, such incriminations must be uniform, given the transboundary nature of the offences[3].

Nevertheless, we argue that the Romanian Criminal Code falls short in offering adequate protection, in light of recent cases. We are going to take into consideration

---

[1] Lecturer, *University of Oradea, Faculty of law.* Contact: avocatbodea@yahoo.com.

[2] S. Bogdan, D.A. Șerban, G. Zlati, *Noul Cod penal. Partea specială. Analiză, explicații, comentarii. Perspectiva Clujeană (New Criminal Code. Special Part. Analysis, explanations, comments. Cluj Perspective),* Ed. Universul Juridic, Bucharest, 2014, p. 557.

[3] C. Miheș, *Infracțiuni informatice: reglementare și investigare (Cybercrime: regulations and investigation)*, Ed. Universității din Oradea, Oradea, 2007, p. 9.

the necessity of incriminating computer data input forgery committed by a public official, a necessity that arose from a case we argued in front of the Romanian Courts.

II. The Point of Origin

On the 28th of April 2020 the prosecutors accused two border policemen of falsely inputting in the border police computer system data they knew not to be real.

The circumstances of the case regarded the situation of Romanian citizens entering the national territory and declaring that they were lorry or truck drivers, which they weren't, a fact easily verifiable by checking the driver's license.

New regulations adopted in the context of the pandemic crisis stipulated that a person, when entering Romania, needs to give a written statement in front of the border policeman in which they have to declare whether or not they have specific symptoms of COVID 19, the place of departure and several other data[4]. They are placed in quarantine, in certain designated places, under police and military supervision.

Under the provisions of art. 4 of Military Order no. 1[5] as supplemented by art. 9 of Military Order no. 2[6], truck and lorry drivers are exempt from the measure of quarantine if they are entering the Romanian territory. They are placed in self-isolation in their homes or in arranged spaces provided by their company or by local authorities. Therefore, some of the people entering Romania thought it better to declare themselves to be lorry drivers in order to avoid the measure of quarantine, mandatory for all other persons that crossed the Romanian border.

In this context 4 individuals who later became denouncers stated in front of border police that they were lorry drivers working in a member state of the EU, and therefore asked to be placed in self-isolation in their own homes.

Leaving aside the debate whether or not the idea came from the border police officer or form the four persons, given the fact that such a debate has to take place in front of the courts and needs to be supported by evidence, we are interested more in the theoretical aspect of the false computer data inputting, working under the presumption that the public official knows that the data he is going to enter into a digital record is false.

The prosecutor office argued that such an input of false data represents the offence of computer forgery stipulated by the Romanian Criminal Code under article 325 NCC[7]. This article incriminates the act of entering, modifying or deleting, without right, computer data or restricting, without right, the access to such data, resulting in data that is untrue, if the crime is committed for using such data to produce legal consequence.

---

[4] Art. 1 par. (2) of the Order no. 414/11 March 2020 of the Health Minister published in Official Gazette, Part I, no. 201 of 12 march 2020 stipulated that: The institutionalized quarantine measure will be imposed on asymptomatic persons entering the territory of Romania coming from the areas with extended community transmission affected by COVID-19 (red zone), for a period of 14 days, in specially arranged spaces provided by local authorities. This order was subsequently amended by Order no. 622/2020 for amending and supplementing the Order of the Minister of Health no. 414/2020 published in the Official Gazette, Part I, no. 315 of April 15, 2020.

[5] Published in Official Gazette, Part I, no. 219 of 18 March 2020.

[6] Published in Official Gazette, Part I, no. 232 of 21 March 2020.

[7] The Romanian New Criminal Code (NCC) was adopted was published and enter into effect on 01.02.2014.

III. The Interpretation of the Provisions of art. 325 NCC

The prosecutor argued that by inputting false data the public official acted "without right" in the sense of the incrimination, given the fact that he has the right to input only data he knows to be true.

Although the case is not yet judged in the arrest proposal that followed the charges, we have fought the charges on the grounds that the incrimination relates to a deed committed without right and in this case the border policeman had not only the right but the obligation to input that data, whether or not he knows it to be true or false.

The Court embraced our opinion and rejected the arrest proposal relating to this accusation on the grounds that the border policemen acted within their right entering the data.

In the Romanian doctrine the offence incriminated under art 325 NCC is presented to be a correlative incrimination to document forgery incriminated under articles 320 and 321 NCC committed in regard to computer data[8] a fact deduced even in relation to the placement of the text in the criminal code among forgery offenses[9].

In fact, under previous legislation[10] the incrimination was identical and derived from the obligation assumed by Romania in accordance with the European Convention on Cybercrime adopted in Budapest on 23 November 2001[11] to incriminate entering, altering, deleting or restricting access to computer data without right.

The legislator opted for a separate incrimination in respect to document forgery, although in France such an action that translates into a data forgery falls within the offence of forgery regulated by article 441.1 French Criminal Code. The French Supreme Court stipulated that modifying computer data in a manner similar to a document is incriminated under this article[12].

The legislator felt compelled to incriminate this offence in order to protect a new social value that is to protect public confidence in the authenticity of digital documents and the veracity of stipulations recorded in them[13] as the crime of illegal

---

[8] S. Bogdan, D.A. Șerban, G. Zlati, *cited above,* p. 559; C. Rotaru, A.-R. Trandafir, V. Cioclei, *Drept penal. Partea Specială II* (*Criminal Law. Special Part.*) Ed. C.H. Beck, Bucharest, 2020, p. 410, G. Antoniu, T. Toader, V. Brutaru, S. Daneș, C. Duvac, I. Griga, I. Ifrim, G. Ivan, G. Paraschiv, I. Pascu, I. Rusu, M. Safta, I. Tănăsescu, T. Toader, I. Vasiu, *Explicațiile Noul Cod penal Comentat. Vol. IV –art. 257-366 (Explinations of the New Criminal Code. Vol. IV –art. 257-366),* Ed. Universul Juridic, Bucharest, 2016, p. 547.

[9] V. Dobrinoiu, I. Pascu, M.A. Hotca, I. Chiș, M. Gorunescu, C. Păun, M. Dobrinoiu, N. Neagu *Noul Cod penal Comentat. Vol. II – Partea specială. (New Criminal Code Commented. Vol II. Special Part),* Ed. Universul Juridic, Bucharest, 2012, p. 722.

[10] Article 48 of Law 161/2003 regarding measures to ensure transparency in the exercise of public dignity, public office and in the business environment, prevention and sanctioning of corruption stated: *The act of entering, modifying or deleting, without right, computer data or of restricting, without right, the access to these data, resulting in data untrue, in order to be used in order to produce a legal consequence, constitutes a crime and is punished with imprisonment from 2 to 7 years*.

[11] Ratified through Law no. 64/2004 published in Official Gazette, Part I, no. 343 of 20 April 2004.

[12] see the Decision from 21st of January 2001 in *Bulletin criminal,* apud. G. Zlati, *Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare precum și a noului cod penal* în Revista Dreptul, nr. 10/2012 (*Some aspects related to computer crimes from the perspective of the legislation in force as well as the new criminal code* in Law Magazine, no. 10/2012) p. 212. The situation is the same in the Dutch criminal system.

[13] S. Bogdan, D.A. Șerban, G. Zlati, *cited above,* p. 558.

accessing of computer data incriminated under art. 362 NCC[14] did not offer sufficient protection.

In conclusion the majority of the doctrine[15] considered this incrimination to be a translation in respect to digital data of both criminal conducts relating to documents, and although stipulating that the action must be done without right, did not stop to analyse this condition in detail with the exception of a reference to the art. 35, paragraph (2) of Law no. 161/2003[16].

IV. Our Perspective and Arguments for the Need of Incriminating a New Offence

We argue that the current incrimination does not cover the input of false data by an official that has the right to access or input such data.

Article 35 paragraph (2) of law no. 161/2003 defines, the person who acts without right as the person who:

a) is not authorized under the law or a contract;

b) exceeds the authorization limits;

c) does not have the permission, from the competent natural or legal person, according to the law, to grant it, to use, manage or control a computer system or to carry out scientific research or to perform any other operation in a computer system.

A person *not authorized* by law or contract is a person who acts without any authorization, a subject that could not, in a legal manner, enter, modify or delete data stored on a computer. This is the case of a particular lacking any authorization, for instance in our example the 4 men trying to cross the Romanian border.

A person who *exceeds the authorization limits* is a person that has an authorization but acts above its clearance. For instance, if there are different levels of security, entering, modifying or deleting data by the person who has a lower access level falls within this incrimination. A person acting within the limits of authorization or clearance (for instance the one that has the right to input such data) cannot commit this offence. Of course, we will not argue that false data are authorized to be inputted, but in general terms, in this case the authorization refers to levels of clearance given, in respect to the nature of the data. Following the reasoning of the legislator, we argue that under letter a) the subject has no authorization and under letter b) the authorization is insufficient.

A person that *does not have the permission* under letter c) is a person that acts without a consent given by the entitled entity, the distinction to the letter a) being that such a right can be given in an informal manner not through an authorization, for instance in the case of a system not protected by password.

---

[14] A similar incrimination in the French Criminal Code is article 323 paragraph 3 that stipulates that fraudulent introduction, deleting or modifying data stored in a computer system constitutes an offence. A distinction is however obvious in the case of the Romanian law as the text still refers to an act done "without right" whereas the French law incriminates fraudulent actions against computer data G. Zlati, *cited above,* page 215.

[15] Including ourselves, see R. Bodea, B. Bodea, *Drept Penal. Partea Specială* (*Criminal Law. Special Part*) Ed. Hamangiu, Bucharest, 2018, p. 513.

[16] C.Rotaru, A.-R. Trandafir, V.Cioclei, *cited above,* p. 411; A. Maxim, *Falsul și frauda informatică* în Caiete de Drept penal nr. 3/2011 (*Forgery and Computer fraud* in Criminal Law Writings, no. 3/2011), p. 62.

In respect to article 325 NCC we think that through the way the text describes the offence, first of all there needs to be an act of accessing or restricting data *without right* that causes an alteration of the data and renders them untrue[17]. Thus, the incrimination does not cover the situation in which the policeman or any public official for that matter acts intentionally and within his own right inputting false data.

The same opinion was embraced by the Court. Although judge of rights and liberties retained from postulating opinions regarding the typical character of the deed (as it is the attribute of the trial judge to decide whether or not this type of act can be treated as the offence of computer forgery) the proposal was rejected, the judge emphasizing of the lack of the sufficient accuracy regarding the legal framework applicable, insisting upon the existing authorization, as the border policeman had the obligation to input data.

As we have shown, some authors argue that by incriminating this offence the legislator wanted to sanction the corresponding action of the perpetrator in relation to the forgery offence of a written document, either by counterfeiting it or by alteration. In exemplifying the content of the norm, the authors argue that introduction of data resulting in creating the forge electronic document is sanctioned by article 325 criminal code and modifying an existing document falls under the alteration of such an electronic document of electronic data[18].

Even if we agree that this was the intention of the legislator, we cannot stumble upon the end result. Respecting the idea that the public official cannot by himself enter in good faith data he knows to be false and such a conduct must be prohibited we think that such prohibition is not imposed through article 325 NCC.

First of all, the law does not define the active subject of this incrimination. Indeed, it does not require a special capacity, therefore allowing any person that commits such an act to be punished according to the law, including, in our case the four people that tried to cross the border. The way the text is stipulated tends to incriminate the act of a *foreigner in respect to that system* (a person who has no or insufficient access to such data and that without right enters data to modify the content of the electronic document), whether or not he is a public official.

On one hand, it is true that a public official can commit the offence, *if he has no right*. But we think it would be better if there was a distinction between a stranger and a specialized subject acting without right, in correspondence with forging documents done by a private individual or a public official. This distinction is needed because in most cases persons having a special capacity (for instance a public official) can have an easier physical access to the system (even though they are not authorized or are exceeding the level of authorization). Furthermore, given the nature of their occupation, that involves exercising public authority they should restrain themselves further.

On the other hand, the law needs to cover the situation in which the person *has the right* but opts for inputting forged data. In such a case, despite of any of the legislator's intention, the person who has access to such data cannot be sanctioned, as

---

[17] In the Italian criminal system, the usage of the term "without right" is limited to computer fraud sanctioned under art. 640 (ter.) of the Italian Criminal code; it is placed in correlation with the expression "in any way" and relates to any form of intervention different from the act of alteration of the functioning of computer systems. See F. Mantovani, *Dirrito Penale. Parte Speciale II Seconda edizione (Criminal Law. Special Part II Second edition)*, Ed. Wolters Kluwer – Cedam, Milano, 2018, p. 233.

[18] see S. Bogdan, D.A. Șerban, G. Zlati, *cited above,* p. 559.

his action does not fall within 360 NCC (illegal access to a computer system)[19], art 362 NCC (alteration of computer data integrity)[20] or any other offense against the security and integrity of computer systems and data.

Another interpretation is possible: that such act should fall under art 321 NCC. But that would represent an analogy against the defendant, prohibited as a concept by the constant jurisprudence of the European Court of Human Rights regarding art. 7 of the Convention[21] as the text in question explicitly refers to written official documents.

Therefore recognizing the need to protect computer data or the content of such data even from the persons that have the right to access them, but do so with in ill-faith, the need of incriminating a special crime designated to sanction the deed done by the person who has the right to alter, input or delete such data arises.

Although we could argue the need to re-formulate the text of art 325, we think it is best to set up a new incrimination under paragraph 2 that sanctions the act of inputting false data or fraudulent modifying or deleting data in a manner that alters the content of the electronic data and renders them to be false by the person who has proper authorization. This way paragraph 1 will protect the value against offenders acting without authorization and paragraph 2 against offenders acting with authorization. The Italian legislator had an even wider approach, incriminating under art. 491 (bis) any type of forgery sanctioned by Title VII, Chapter III of the Italian Criminal Code committed in respect to an official digital document. This approach rendered all debates useless as the doctrine insists only upon differences between different types of forgery[22].

If we were to argue that entering data without right means entering false data, like the prosecutor did, we think that there will be an issue regarding the unforeseeable content of the incrimination, due to the way in which the misconduct is described: it refers to an active subject that does not have the *right* of acting in the manner prescribed by law. Therefore, by exclusion if he has such right, the general interpretation of the incrimination is that he cannot commit such a crime.

The prosecutor`s thesis is dangerous seen through another example: if the agent is acting *within his right* inputting *true data* but in a manner that alters the end result, thus creating a legal consequence. Continuing the prosecutor`s reasoning this action would be sanctioned too, as acting without right would mean any improper usage of his right to input data, and would suppress any misconduct of the agent in fulfilling his attributions weather or not they are prescribed by law, an interior order, a work instruction or a recommendation. We cannot accept this thesis as it is simpler and clearer to incriminate the fraudulent inputting false data. In relation to this concept we emphasize that in the UK criminal system it is considered that an instrument is false if it purports to be something it is not or if it 'tells a lie' about its own authorship, origins or history[23].

---

[19] Art. 360 NCC incriminates the unauthorized access to a computer system, but as we have seen the offender is authorized to access the system.

[20] Art. 362 NCC incriminates the act of modifying, deleting or damaging computer data or restricting access to this data, without right. A similar incrimination that also refers to an unrightful act.

[21] See F. Streteanu, *Tratat de drept penal. Partea Generală* (*Criminal law treatise. General Part*), Ed. C. H. Beck, Bucharest, 2008 p. 48.

[22] S. Preziosi in A. Fiorela (a cura di) *Questioni fondamentali della parte speciale del diritto penale. Terza edizione* (*Fundamental issues regarding the special part of criminal law. Third edition*), Ed. G. Giappichelli, Torino, 2019, p. 607-650.

[23] See H.r.l.j. H.D. Ormerod (General editor) *Blackstone`s Criminal Practice*, Oxford University press, 2012, p. 476.

V. Conclusions and *de Lege Ferenda* Proposals

As a conclusion the need to protect public confidence in the authenticity of digital documents and the veracity of stipulations recorded in them is undisputed. Article 325 NCC responds to this need in relation to subjects acting without right. We think that the text should be left untouched and a new incrimination should follow in the same article under paragraph (2) sanctioning the act of inputting false data or fraudulent modifying or deleting data in a manner that alters the content of the electronic data and renders them to be false, by the person who has the proper authorization.

Furthermore we would argue for a separate new aggravated incrimination under a proposed paragraph (3), that sanctions the act stipulated in paragraph (1), committed a public official that acts *without right*, a distinction that should be made in a similar manner to the one made in relation to forgery of written documents.

References

1. Antoniu, G. *et.all., Explicațiile Noul Cod penal Comentat. Vol. IV – art. 257-366 (Explanations of the New Criminal Code. Vol. IV – art. 257-366),* Ed. Universul Juridic, Bucharest, 2016.

2. Bodea, R., Bodea, B., *Drept Penal. Partea Specială* (*Criminal Law. Special Part*) Ed. Hamangiu, Bucharest, 2018.

3. Bogdan, S., Şerban, D.A., Zlati, G., *Noul Cod penal. Partea specială. Analiză, explicații, comentarii. Perspectiva Clujeană (New Criminal Code. Special Part. Analysis, explanations, comments. Cluj Perspective),* Ed. Universul Juridic, Bucharest, 2014.

4. Dobrinoiu, V. *et.all., Noul Cod penal Comentat. Vol. II – Partea specială. (New Criminal Code Commented. Vol II. Special Part),* Ed. Universul Juridic, Bucharest, 2012.

5. Mantovani, F., *Dirrito Penale. Parte Speciale II Seconda edizione (Criminal Law. Special Part II Second edition)*, ed. Wolters Kluwer – Cedam, Milano, 2018.

6. Maxim, A., *Falsul și frauda informatică* în Caiete de Drept penal nr. 3/2011 (*Forgery and Computer fraud* in Criminal Law Writings, no. 3/2011).

7. Miheş, C., *Infracțiuni informatice: reglementare și investigare (Cybercrime: regulations and investigation)* ed. Universității din Oradea, Oradea, 2007.

8. H.r.l.j. H.D. Ormerod (General editor) *Blackstone`s Criminal Practice*, Oxford University press, 2012.

9. Preziosi, S. in Fiorela, A. (a cura di) *Questioni fondamentali della parte speciale del diritto penale*. *Terza edizione* (*Fundamental issues regarding the special part of criminal law. Third edition*), Ed. G. Giappichelli, Torino, 2019.

10. Rotaru, C., Trandafir, A.-R., Cioclei, V., *Drept penal. Partea Specială II* (*Criminal Law. Special Part*), Ed. C. H. Beck, Bucharest, 2020.

11. Streteanu, F., *Tratat de drept penal. Partea Generală* (*Criminal law treatise. General Part*), Ed. C. H. Beck, Bucharest, 2008.

12. Zlati, G., *Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare precum și a noului cod penal* in Revista Dreptul, nr. 10/2012 (*Some aspects related to computer crimes from the perspective of the legislation in force as well as the new criminal code* in Law Magazine, no. 10/2012).

New Technical Devices and Methods in Crime Scene Investigation

***Dr. Füszter Erzsébet*[1]**

Abstract

The aim of this article is to draw attention to the importance of crime scene investigation, because the thorough detection of traces, physical evidence, crime related facts and other phenomena indicating the circumstances of the crime are of decisive significance. Recording the state of the scene of crime can provide the investigator with data, points of reference and evidence. Recently developed professional scene processing equipment and imaging tools greatly help the work of the authorities.

Keywords: *special imaging tools and techniques, infrared photography, thermography, 3-dimensional laser scanning, optical crime scene processing equipment, ALS/FLS-light sources*

I. Introduction

Examining the domestic and international professional literature, it can be concluded that the investigation of the crime scene and the detection of traces, physical evidence, crime-related facts and other phenomena indicating the circumstances of the crime are of decisive importance. Recording the state of the scene can provide the investigator with data, points of reference and evidence. The use of data originated from the crime scene can be very widespread during investigations, as evaluating the photos taken at the crime scene and examining other crime scene related data can help the profiling work, even during specific profiling[2].

During the crime scene investigation, we should, without question, search for and collect all the material evidence and we have to ensure that they will be properly preserved. As there is rarely more than one opportunity to obtain evidence from a crime scene, the investigation by the CSI team must be methodical and complete.

The success of the crime scene investigation depends not only on the necessary professionalism and essential legality, but also on the effectiveness of the tools and methods used. Today, we are experiencing a revolution in the field of crime scene processig devices. In addition to the decades-old trace-search techniques, photography, and what are now referred to as traditional trace-recording techniques, we are witnessing the emergence and rapid expansion of new tools and procedures that may change our outlook on crime scene investigation.

---

[1] Prof. dr., National University of Public Service, Faculty of Law Enforcement.

[2] Nyitrai Endre: Bűnelemzés a nyomozásban (Crime analysis in investigation), In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) Modernkori veszélyek rendészeti aspektusai, Pécs, Magyarország: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2015. p. 145.

Recently developed professional scene processing equipment and imaging tools greatly help the work of the authorities.

II. New Imaging Features and Techniques

During the last decade, modern imaging techniques have become more and more important in crime scene investigation. Digital technology replacing traditional analog photography provided powerful new tools for capturing, analyzing and storing records of the crime scene and its physical evidence.

On many occasions, the CSI team has to work under conditions that are far from optimal. In poor lighting conditions, however, like at night, where the illumination of the area or object being photographed cannot be achieved properly in the conventional way, the infrared range of the light spectrum is also capable of recording. Two fundamentally different methods are known today for this purpose.

Beyond the visible light range, the so-called Near InfraRed (NIR) (760-1600 nm) image capture is called infrared photography as the camera's optical system captures infrared light reflected from objects. Special infrared projectors are used to "illuminate" the area to be photographed with infrared radiation, with either infra LEDs integrated into the digital camera itself with special optics or with independent lasers or LED light sources, so called infrared reflectors. The illumination distance of infrared radiators can vary from a few meters to hundreds of meters, depending on the light source.

The infrared camera captures what you see in black and white, but imaging is different than usual. Subjects that are bright in visible light are generally dark in the IR image, while those that should be dark are bright in the IR image. Whether a part of the image is white, black, or gray is basically determined by the infrared absorption or reflection property of the object or part of the object. The unusual appearance of photos taken with infrared filters is due to the natural light absorption phenomenon. A feature of an image taken with an infrared camera is that the green vegetation looks white, as if covered by thick snow. The explanation of the white foliage is that the plant chlorophyll absorbs the waves at the beginning and at end of the light spectrum, i.e. the blue and red rays, while reflecting the green and yellow color ranges. That is why plants look green in normal light. However, chlorophyll does not absorb infrared radiation at all, but completely reflects it, and since landmarks usually reflect less infrared light than chlorophyll, plants appear to be the brightest, that is, blinding white. However, e.g. water and sky absorb infrared rays, making them look dark in IR photos.

Infrared, or "IR" photography, offers photographers of all abilities and all budgets the opportunity to explore a new world – the world of the unseen. Why "unseen"? Because our eyes literally cannot see IR light, as it lies just beyond what is classified as the "visible" spectrum – which human eyesight can detect[3].

Infrared photography plays an increasingly important role in many disciplines as well as in forensics. In fact, infrared photos can reveal details that are hidden from the naked eye. Forensic writing and document examination are impossible to imagine without the use of infrared imaging technology. Among the security features of security documents is the so-called security system of IR absorbent and IR

[3] Bob Vishenski: Introduction to Infrared Photography, Photographylife, Available at: https://photographylife.com/introduction-to-infrared-photography, Accessed: 02.09.2020.

transparent inks. Printed elements printed with an IR absorbent ink are not visible under normal lighting conditions. These elements are optically imaged in the infrared light range. Shapes printed with IR transparent inks are visible under natural light, but not observed when viewed through an infra-converter.

In addition to infrared photography, another method that can be used in low vision conditions is thermal imaging or thermography.

Thermal imaging is simply the process of converting infrared (IR) radiation (heat) into visible images that depict the spatial distribution of temperature differences in a scene viewed by a thermal camera. Thermal imaging technology developed by the military has recently found its way not only into the commercial market but into forensic use as well because it is a very powerful sensing technique.

Infrared photography and thermal imaging both operate in the range of infrared light. However, infrared illuminators are not required for thermal imaging, because thermal cameras detect the thermal radiation emitted by objects. Thus, a thermal camera detects a thermal image, that is, it is capable of detecting the heat emitted by the area it is observing, the temperature of people and objects outside it, and displaying it in an image transformed into visible light. Therefore, thermal cameras do not detect the radiation reflected from the bodies, but the heat emitted by them.

The operation of thermal cameras is based on the principle that all objects with a temperature above the absolute zero degree generate heat, due to the constant vibration of the atoms and molecules that they are consisted of, thus all things in the infrared range emit infrared rays i.e. heat. Even cold objects like an ice block emit infrared rays. The intensity of radiation depends on the temperature of the object. The warmer an object, the more heat it discharges. The thermal contrast detection method provides the basis for the functioning of thermal cameras.

During thermal imaging, the optical system (usually made of germanium) of a thermal imaging camera collects electromagnetic waves in the range of its sensitivity and converts them into electrical signals using its infrared detector, which is used by specialized imaging software to produce images that are valuable to us. Most thermal cameras create black-and-white images, with the warmer parts appearing white, and the cooler parts appearing black. There are camera types that artificially color the image for easy recognition. Some mark red for warm areas, others mark yellow for warm areas and blue for cold areas. Because objects have constant heat radiation, thermal imaging cameras are capable of imaging even under the most extreme environmental conditions (night, day, mist, fog, rain, snow, smoke etc.).

In general, all forms of photography and video recording are characterized by the fact that analog and digital cameras, but also thermal and video cameras, direct light/electromagnetic rays reflected from or emitted by the object through various lenses (lens systems) into the photosensitive part of the device, which then creates the visual form of the object. In contrast, 3D scanning is a professional imaging technique that is completely different.

3D laser scanning is a state-of-the-art data acquisition method that began to be utilized in the second half of the 1990s and was initially used for surveying. Today, three-dimensional technologies, such as 3D imaging and printing, can be considered as revolutionary innovations of the 21th century.

3D scanning is considered as one of the most efficient and state-of-the-art methods of spatial data acquisition. 3D scanners are devices that "digitalize" objects and spatial objects, capturing their geometry in a 3D data file without being physically in contact with them.

The laser scanner emits millions of laser beams within seconds to measure the distance between the instrument and the spatial object. The data set/spatial point cloud created this way can be used to extract geometric data of the surveyed objects with a software.

Thanks to 3D point cloud technology, the result of scanning is a three-dimensional snapshot of objects and spaces, the detailedness of which depends on the resolution of the instrument used. The resulting point cloud can be used to retrieve the geometry of scanned objects. These can be viewed in three dimensions, and the data for each point can be compared to each other.

The 3D scanners consist of a high-power laser diode, high-speed rotating mirrors, a high-sensitivity laser detector and a control computer.

Several types are known for their efficiency, performance and mode of operation, depending on the size of their surface, the accuracy of their measurements, their resolution and the distance from which they can scan.

Handheld scanners are used primarily to record the morphological and geometric features of small objects and spatial details.

Depending on the complexity of the site, "tripod" space scanners are capable of perfectly reproducing the spaces and objects being examined as a result of multiple measurement scans. With the help of scanned point clouds and spherical panorama photos, all objects of the virtual space can later be observed and accurately measured. The duration and quality of the 3D laser scanner survey depends on the parameters of the 3D laser scanner.

Using a space scanner, you can create a 3D model that is dimensionally accurate and, depending on the resolution you set, is characterized by the accuracy of a fraction of a millimeter. As 3D data acquisition technology is also capable of providing a true virtual representation of the subject being scanned, and since 3D scanning produces high-resolution, detailed virtual replica, it may be ideally suited for capturing a variety of traces, including volume traces in the future. Using appropriate software and 3D printing technology, you can make an exact copy of any object that is relevant to your case.

The use of the 3D technique has many advantages over manual photography, because the images of the 3D laser scanner are always scalable, undistorted, and due to their positioning, every single detail is captured, even in a situation when the crime technician or the CSI team may not consider something to be relevant information, so it would probably not be recorded in the first place[4].

III. Optical Crime Scene Processing Equipment

A new development on the market has been the discovery of optical tracking devices that help detect traces and material remains of less prominent appearance by emitting light at different frequencies. The light emitted by conventional bulbs has different intensities but produces light at all wavelengths. Such lamps are called continuous spectrum light sources.

[4] Rucska András: A helyszín képi rögzítése hagyományos és háromdimenziós eljárással a kriminalisztikai szabályok szerint (Visualization of the scene by conventional and three-dimensional procedures according to forensic rules), Ügyészek lapja, 24(5), 2017.

The visible light ranges from violet to red, complemented by infrared and ultraviolet regions that are no longer visible to the naked eye[5].

Optical trace detection, that is, exposure to traces and physical evidence by using different optical scene processing equipment, is based on four basic photometric phenomena: light absorption, light reflectance, light scattering and fluorescence.

The color we see in an object depends on the wavelength range and the rate at which it is absorbed and reflected by incident light. Unabsorbed rays determine the color of the body.

The color of opaque objects is represented by a mixture of reflected colors. While black "colored" objects absorb all the light falling on them, white "colored" objects reflect all light. Different shades of gray are created by surfaces that absorb and reflect every color range of white light.

The color of a "colored" object can be resulted from two different mechanisms: first, by reflecting only one color range from the white light on its surface and absorbing the rest, and secondly, by absorbing only the complementary color of the specified color from the entire spectrum of incident light and reflecting all the rest[6].

The color of transparent materials is also determined by the range of light transmitted through them. If an object is not completely transparent, it transmits a certain part of the light and reflects the other.

Since the color of an object is the result of a mixture of reflected (or transmitted) colors, it always depends on the composition of the illuminating light[7].

The phenomenon of light scattering can be truly observed when the light rays are projected at a low angle, not perpendicularly on an object. By illuminating the surface of the object with “oblique light”, small surface protrusions and depressions as well as small objects, which are otherwise barely perceivable due to the scattering phenomenon, become visible with contrast.

Fluorescence is a physical process in which a substance absorbs electromagnetic radiation of a given wavelength, in this case light, and as a result, the molecules of the substance enter a higher energy state. When the illumination ceases, they return to their original resting position while giving off some of the energy they have absorbed in the form of light. The light emitted will always be of less energy, that is, of a longer wavelength than the excitation light. If, for example, fluorescence was caused by blue light, the fluorescent object will emit a light in the yellow wavelength range. In such cases, the crime scene technicians should wear orange goggles. In order to detect a faint light phenomenon, it is important that the strong blue light used for illumination

---

[5] The so-called “white light” is a mixture of different wavelengths in the range of visible light in the same proportion as the light of the sun. White light is thus a complex (polychromatic) light, which is a mixture of several lights of different wavelengths and colors (violet, blue, green, yellow, orange and red). The color of the light is determined by the wavelength of the electromagnetic radiation.

[6] For example, an object looks yellow when it reflects only the yellow wavelength of white light and absorbs the rest, so only the yellow light reaches our eyes. But even if it only absorbs violet, the complementary color of yellow, the object is yellow, as all the rest is reflected. By the same logic, an object is green when it reflects only green, and when the complementary color of green, red, is absorbed by the object and all other wavelengths are reflected.

[7] A white object looks green when illuminated by green light, and red when illuminated by red light. A green object is green in both white and green light because it absorbs red (green is the complementary color of red), but when illuminated by red light, it becomes black because it completely absorbs the red.

does not obscure the emitted light, which is always much dimmer than the illuminating light. The orange glasses filter out all the blue light and let only the rays in the yellow range through.

After illumination by the correctly chosen wavelength (color), most organic material demonstrates fluorescence, which can be seen with suitable goggles or a color filter. For example, bone and tooth residues, when illuminated with blue light at 455 nm, exhibit a faint fluorescence phenomenon, which is perceptible through orange goggles and can be captured by photographs using an orange filter.

Forensic tracing was the first field to use illumination with ultraviolet rays in every single ranges of light in the 1970s. The use of various UV light tracing lamps has become widespread both in the field and in laboratory work, as the biological residues of semen, saliva, vaginal secretions, sweat and urine spots are clearly visible to the naked eye when exposed to UV light. However, UV-illumination can also help detect untreated blood spots, because they are completely absorbed by UV, so they look completely black when exposed to UV light.

In forensic practice, UV lamps operating in the 254 nm (UV-C) and the 365 nm (UV-A) ranges are the most commonly used.

A special form of optical crime scene processing in the ultraviolet region is the so-called RUVIS (Reflected Ultra-Violet Imaging System), which is suitable for the optical detection of latent or otherwise untreated fingerprints and certain residues of material on both porous, greasy, sticky surfaces where conventional fingerprinting is very difficult and not very efficient.

RUVIS consists of an ultraviolet illumination unit operating in the 254 nm range and a digital camera with appropriate color filters for photographic documentation based on the detection of reflected beams.

The RUVIS test is based on the principle that some substances absorb light when exposed to ultraviolet light, while others reflect light beams projected onto them. As most materials, and thus the vast majority of trace surfaces, are characterized by UV absorption, the method is capable of detecting/visualizing any trace and material residue that does not absorb, but reflect, ultraviolet rays.

In the international literature and police jargon, special lamps that are specifically designed for crime scene processing are called ALS (Alternate Light Source) or FLS (Forensic Light Force) illuminators. In each case, these lamps consist of a strong light source and a system of special color filters associated, which produce monochromatic light rays of the required wavelength, from UV to IR, for the particular test.

IV. Conclusion

Optical crime scene processing is of outstanding forensic importance. Simple, fast, repeatable, without damaging the evidence. The digital recording of the test result is also suitable for documentation and expert examination.

References

1. Fish J. T., Miller L. S., Braswell M. C., Crime scene investigation, Elsevier, 2011.
2. Gárdonyi Gergely: Kógencia a bűnügyi helyszínelésben (Cogency in criminal investigation), Magyar Bűnüldöző, 2011.
3. Lloyd J. M., Thermal Imaging Systems, Springer Science-Business Media, 1975.

4. Lovas Tamás, Berényi Attila, Barsi Árpád: Lézerszkennelés (Laser Scanning), TERC Kft., Budapest, 2012.

5. Nyitrai Endre, Bűnelemzés a nyomozásban (Crime analysis in investigation), In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) Modernkori veszélyek rendészeti aspektusai, Pécs, Magyarország: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2015.

6. Petraco N., Sherman H., Illustrated guide to crime scene investigation, Taylor and Francis Group, 2006.

7. Rahne Eric, TERMOGRÁFIA – elmélet és gyakorlati méréstechnika (TERMOGRAPHY – theory and practical measurement technology), Budapest, Invest-Marketing Bt., 2018.

8. Rucska András, A helyszín képi rögzítése hagyományos és háromdimenziós eljárással a kriminalisztikai szabályok szerint (Visualization of the scene by conventional and three-dimensional procedures according to forensic rules), Ügyészek lapja, 24(5), 2017.

9. Tomcsányi Péter, Demeter Lászlo, Fizika Optika Hőtan (Physics Optics Thermology), Műszaki Könyvkiadó, Budapest, 2000.

10. Vishenski B., Introduction to Infrared Photography, Photographylife, Available at: https://photographylife.com/introduction-to-infrared-photography, Accessed: 02.09.2020.

11. Vollmer M., Möllmann, K.-P., Infrared Thermal Imaging, John Wiley & Sons, 2011.

Digital Dangers of Smartphones[1]

Dr. Andrea Kraut*
Prof. Dr.László Kőhalmi LLM**
Dr. Dávid Tóth PhD****

Abstract

The appearance of the digital space is a Janus face phenomenon because on one hand it helps in making life easier but on the other hand it creates opportunities to commit criminal actions as well.
The smartphones become part of our everyday life, and even they also replace in many aspects the role of personal computers.
In the online world one of the most difficult task is to find the adequate balance of the double clamping of the users convenience and the digital security.

Keywords: *smartphone, digital, cyber-crime, Android, zero-day exploit, security*

I. The Importance of Smartphone

Smartphones become miniature computers. Such portable multimedia devices that users use for a myriad of other functions besides telephone conversation. With the Internet becoming available on mobile devices as well, the original functions of telephones (calling, text messaging) have been marginalised along with countless other functions.

The owners use smartphones for emails, chats, video conversations, and for web browsing.

The phone can also be used as a camera, music player, notebook, appointment book, navigation system etc. function. The latest devices can give you access in many areas which can ease our everyday live.

According to the Hootsuite's statistics in 2020[2] out 7.75 billion people of the world 3.8 billion inhabitant uses the social media and 4.54 billion users have access to the internet and 5.19 billion people (67% of the population) have a mobile communication device[3]. The report also deals with the Hungarian statistics as well.

---

[1] This publications was supported by the Ministry of Justice lawyer excellence scholarship.

* PhD Candidate, *University of Pécs, Faculty of Law Department of Criminology and Penal Execution Law.*

**Professor, Head of Department of Criminology and Penal Execution Law, Faculty of Law, University of Pécs. Email: *kohalmi.laszlo@ajk.pte.hu.*

*** Senior Lecturer, *University of Pécs, Faculty of Law Department of Criminology and Penal Execution Law*. Email: *toth.david@ajk.pte.hu.*

[2] The report of the Hootsuite Digital in 2020. See further: https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media.

[3] In addition to the data set referred to above, of course, numerous other statistical surveys are known. See further: Kemp, Simon: Digital in 2018: World's internet users pass the 4 billion mark. Special

This highlights that 79% of the adult Hungarian populations can be considered as an internet user, and within this 65% is a mobile internet user. Under these data we can firmly state that the smartphones are an *integral part of our daily lives* and even take over the role of computers in many areas of life.

As the users often use their phone as a work tool, as a main administrative device, in addition to keeping in touch and having fun, the devices are in the immediate vicinity of the users 24 hours a day.

In order to have a faster, more efficient and simpler administration, the convenience factors came to the fore, and smartphones appeared in this area. Due to this in many occasions many confidential data were saved such as the user's personal, bank, local data and the business. In addition to these, company data and confidential information at work became easier to access[4].

During the coronavirus *pandemic*, the value of mobile communication devices increased in value, but the global spread of the home office also brought some dangers[5] because *without adequate IT* protection critical infrastructures can become *vulnerable*.

The potential of smartphones has also been noticed by *criminal groups*, and thus these devices – as a perpetration object – became a target for organized crime groups. The danger to society of these criminal conducts are highly significant[6].

New attack surfaces have emerged on mobile devices, new forms of computer fraud appeared with new perpetration conducts especially in order to obtain personal and sensitive data.

The protection options developed for desktop PCs in connection with mobile devices are in many cases unsatisfactory, and users are not aware of the dangers or may not deal with them with enough knowledge[7]. As a result, smartphones have become the focus of criminals, causing serious material and moral damage to a multitude of users[8].

In our study, we would like to point out the dangers of using smartphones (primarily Android-powered phones), presenting the crimes that are typically associated with the proliferation of mobile devices. We also want to highlight the vulnerabilities of various systems and present developer and user opportunities to reduce criminal acts resulting from weaknesses in mobile operating systems.

II. The Android Operating System

The term for these new devices first appeared in English language as *"smart phone"*, and as a translation into Hungarian ("okostelefon"), it gained civil rights in the common language.

Report. https://wearesocial.com/blog/2018/01/global-digital-report-2018 [Downloaded: 2018.12.05].

[4] Kempin, von Stephan, *Android Smartphones im Fokus krimineller Aktuere* [*Android smartphones in the focus of criminal actors]*. Kriminalistik 10/2014. pp. 615-616.

[5] See:Elek, Balázs, *From poaching to financing terrorism*. Journal of Eastern-European Criminal Law 2016.1. pp. 191-193.

[6] Gál, László István, *Economic policy, criminal policy and economic crimes*. Journal of Eastern-European Criminal Law 2019.1. pp. 100-103.

[7] Gál, László István – Serbakov, Márton Tibor, *How acts of terrorism are financed and orchestrated in secrecy today: criminal offences, donations, legal business and smartphone applications*. Journal of Eastern-European Criminal Law 2019.1. pp. 67-69.

[8] Kempin, S., *op. cit.,* p. 615.

Citing the typology of Péter Bányász, the development of smart mobile phones can be divided into three major stages:[9]

– The emergence of so-called first-generation devices spans the period from 1994 to 2002, which was characterized by a preparation for technological foundations of smartphones, and perhaps more precisely the pre-smart mobile era. (At this stage the high category of phones has been produced by Nokia and Ericson)[10].

– The period from 2002 to 2008, which brought the mass proliferation of smartphones[11].

– The third period, from 2009 to the present, can be described by the worldwide proliferation of user-friendly devices. The launch of this era emerged with the entry of *iPhone***s** into the market, as it prompted competitors to innovate in the market[12].

Smartphones can be divided into two groups in terms of their operating system. Some of them run closed source software (IOS, Windows Phone, Blackberry), but most of them today are running open source operating systems. (Android, Samsung, LG, HTC, Sony, Motorola)[13].

Open source software (FLOSS) is a computer program that can be freely used, copied, distributed, studied and modified[14]. In addition to allowing anyone free access, anyone can develop the software in a personalized way (with good programming skills). Closed source systems only allow you to run programs without changing it the core of the system[15].

In a virtually two-player market, Android leads with a huge advantage, although Android's open philosophy also has its downsides: users don't get the same experience on different hardware. The user experience can be compromised on simpler devices, and the applications can't run as well like on a more powerful flagship model.

Another key to success is for open source phones is the Google Toolbar, which has a Google Account at its core. After logging in to your account, all your data is sent to a central server, and your mail system, contacts, calendar, conversations, photos etc. are stored and synchronized in the cloud and the phone[16].

a) Vulnerabilites of Android Systems

Programs that threaten mobile operating systems do not mean viruses known from desktop computers in the classical sense. Mobile devices running Android and iOS are not at risk of automatically installing *malicious software* – which transmits

---

[9] Bányász, Péter, *Az okos mobil eszközök biztonsága* [The smart mobile devices]. Hadmérnök 2018, June. p. 361.

[10] E.g. Nokia 9000 Communicator, Nokia 9210, Ericson R380.

[11] The hallmarks of the era were as follows: Nokia 6600, Blackberry 5810.

[12] See: Bányász, P., *op. cit.*, pp. 363-364. The tablets as they were expensive were not competitive. The breakthrough, as with smart mobile devices, was brought here by Apple as well with the launch of the Ipad in 2010.

[13] See: Bányász, P., *op. cit.,* pp. 363-364.

[14] Szabó, András, *A felhasználók digitális lábnyomának, anonimitásának vizsgálata technikai szempontból. II.* rész Mobil eszközök [*Demonstrating user anonimity and digital footprint with technical tools part II. – Mobile devices*]. Hadmérnök 2018/1. p. 220.

[15] Rátai, Balázs, *Nyílt forrású /open source/ szellemi közjavakkal kapcsolatos gazdasági-üzleti kérdések elemzésének alapjai* [*Fundamentals of analysis of economic-business issues related to open source intellectual public goods*]. Infokommunikáció és Jog 2011/43. p. 39.

[16] Szabó, A., *op. cit.*, p. 229.

itself to your "friends" devices or even deletes your phone data – when you open an email or navigate to an untrusted website. This is because they are mostly used to steal personal information, such as passwords or credit card information, and can practically only be placed on mobile devices if the user negligently installs it himself[17].

According to Kempin, the vulnerability of the system is provided by the already mentioned open platform. By allowing anyone to make changes to the software, it is also easier for malicious programmers to gain ground. Although it should be noted that the huge development community is fortunately plentiful with well-meaning professionals who report discovered bugs, vulnerabilities, or fix them after they are noticed[18].

In addition, manufacturers' *development policies* do not always take users into account. Manufacturers are constantly working to update programs, using new versions to fix bugs, vulnerabilities, and try to filter out previously released malware. For iOS, newly released updates reach iPhone owners immediately. On Android phones, however, usually there is no automatic security update for previously manufactured devices.

Manufacturers dedicate a *short product life cycle to devices*[19]. Thus, viruses that are removed by newer versions of programs can still gain ground on older devices.

According to Kempin, the risk of attacks is increasing in connection with ***legal concept*** of applications. Users have the option to download and run an application if an entire block of permissions is approved in advance, meaning that the application is given wide access to a wealth of information displayed on their phone[20].

Privileges are granted *on an all-or-none-policy* basis, meaning that users do not have the option to choose from the privileges offered. They either accept some or cannot run that program on their device[21].

This set of conditions, to quote Kempin, results in certain applications being granted more privileges than they would require. Most users do not read the legal disclaimers when they download an application. The majority of programs asks for permission to network, to keep your phone awake, frequently query your phone's status, and access social databases, all of which can pose another threat to your phone's security[22].

Some *functions* can be considered as risk even though at first glance their aim is to protect the user's personal data security. A good example for this is the google account in which all the personal user data is saved on the cloud servers.

Kempin points out that Google stores our emails, contacts, photos, and monitors location data on all Android mobile phones by default. The primary purpose of this feature is to ensure that in the event of damage to or loss of your phone, the dreaded data will not be lost and will remain available. However, this can also be a huge *vulnerability* if an attacker gains access to your Google Account. The offender can steal all the personal information of the owner of the account in a matter of seconds.

---

[17] Nagy, Zoltán András, *Az informatikai bűncselekmények* [*The information technology crimes*]. Magyar Tudomány 2001/8. p. 948.

[18] Kempin, S., *op. cit.,* p. 616.

[19] Forgács, Imre, *Senki földje a jogban: a globális vállalat* [*No one's land in law: the global company*]. Jogtudományi Közlöny 2017/2. pp. 61-62.

[20] Kempin, S., *op. cit.,* p. 616.

[21] Kempin, S., *op. cit.,* p. 616.

[22] Kempin, S., *op. cit.,* p. 616.

The problem is that apps are created and placed in the Google Play Store without the necessary care and control. Approximately 2.2 million applications are available in the application store, as mentioned above with Kempin's research findings. The huge development community can easily put on new applications on the store without any control. Although there has been a pre-screening of programs to be uploaded since 2015, this is not necessarily a satisfactory solution against malware software[23].

Most of the applications are free or advertisement funded. According to some experts estimate 62% of all applications examined were capable of smuggling *malware* software[24].

b) Zero-day Exploit

In connection with the updating of operating systems, which is in the basic interest of users, it is important to draw attention to the so-called *zero-day vulnerabilities*. By this we mean a security threat in which attackers exploit a vulnerability in a software or hardware that is unknown to developers[25].

With a zero-day vulnerability, it is virtually impossible to patch it within a short time. This means a great threat for users, because IT hackers can exploit them. Systems that are also connected to the Internet are particularly exposed.

The "zero day" bug is not known to anyone, so no security patch has been added yet. *Zero-day exploit* is the actual code that attackers use to exploit the vulnerability[26] before its developer knew about it[27].

c) The Data Transfer Risk, Especially with WiFi

By data transfer we mean the transfer of any information from one place to another. We distinguish between wired and wireless types of data transmission[28]. A typical form of wired data transfer – and a security risk unknown to many – is when you charge your phone using a data cable through an USB port. If your phone comes in contact with an infected machine, the offender has the opportunity to *exploit the vulnerabilities*[29].

Wireless data transmission for a smart mobile device can take place in several ways, e.g. using infrared light, Bluetooth, mobile internet or WiFi.

Regarding the vulnerability of Bluetooth, Péter Bányász draws attention to a case

---

[23] Kempin, S., *op. cit.,* p. 617.

[24] Bányász, P., *op. cit.,* pp. 363-364.

[25] Marsi, Tamás, *A célzott támadások és megelőzésük sérülékenységvizsgálattal* [*Targeted attacks and their prevention through vulnerability testing.]*. In: Bodó, Attila Pál – Marsi, Tamás – Sebők, Viktória – Zámbó, Nóra, *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára* [*Targeted cyber attacks – Annual training for the manager responsible for the protection of electronic information systems*]. Nemzeti Közszolgálati Egyetem, Budapest, 2018. p. 42.

[26] Erdősi, Péter Máté – Horváth, Attila – Kiss, Ferenc, *Információrendszerek biztonsági kockázatainak vizsgálata a szoftverek nyíltsága szerint* [*Examining the security risks of information systems according to the openness of the software*]. In: IT és hálózati sérülékenységének társadalmi hatásai. [*Social impacts of IT and network vulnerabilities.*] Információs Társadalomért Alapítvány, Budapest. 2016. pp. 5-7.

[27] Bányász, P., *op. cit.,* p. 368.

[28] Bányász, P., *op. cit.,* p. 368.

[29] Bányász, P., *op. cit.,* p. 368.; Kemp, Simon, *Digital in 2017- Global overview, We are social*, 2017. 01. 24., https://wearesocial.com/special-reports/digital-in-2017-global-overview.

in 2017, when a security company called Armis Labs identified eight vulnerabilities and their technological exploitability[30].

Wi-Fi (wireless fidelity) is a wireless connection, a network technology that allows you to connect to a wired network via radio waves[31].

The average user is now increasingly aware of the vulnerability of WiFi networks, but in the case of open networks, a *false sense of security* develops in lay people for a variety of reasons (e.g., carelessness, carelessness, financial reasons etc.). The network operator can *monitor* the network traffic and thus essentially "eavesdrop" on the WiFi users. We would probably be in for an unpleasant surprise if, after an open network banking transaction at a breakfast buffet, we could only wait for a statement of our bank account has lost money. Different routers also allow for serious abuse[32].

Koska Melinda Henriett also highlights two flaws in WiFi technology: *the flaw in the WPA2 encryption protocol*[33], which affects billions of devices and vendors, and *Rogue Access Points*, commonly known as rogue aps, which are vulnerabilities for unauthorized access. In both cases, the data streams can be intercepted and manipulated, so special attention must be paid to these two areas[34].

d) The Malwares

The economic and cybercrime in recent years become a professional crime form[35] and Android based systems are a primary target for criminals. Basically it ***is the criminal innovation*** of the so called underground economy, which is also characterized by a kind of horizontal diversification.

According to the unanimous opinion of security experts, the most popular goal of attackers is *to make money*. It is common for Malware to focus on premium SMS and calls, as well as "discount" subscriptions.

Criminals have a criminal interest in attacking *online banking applications*[36], such as Trojan horses, and try to read secret online banking and credit card information with various "discounted" offers. In addition, the current criminal trend includes sending infected spam, DDOS attacks, and misuse of crypto currencies[37].

It is interesting and also a sign of criminal threat that largest Internet search portal, google has removed several applications from the Google Play Store that searched for data without the user's knowledge.

Regarding cryptocurrencies,[38] it is worth noting that in addition to its criminal dangers, its economic rationality is also Janus-faced.

---

[30] Bányász, P., *op. cit.,* p. 369.

[31] Koska, Melinda Henriett, Wi-Fi hálozatok két kijátszhatósági pontja: WPA2 és ROGUE AP [The two vulnerabilites of Wi-Fi networsk: WPA2 and ROGUE AP]. Hadmérnök 2018/3. P. 501.

[32] Bányász, P., *op. cit.,* pp. 370-371.

[33] Koska, M., *op. cit.,* pp. 505-506.

[34] Koska, M., *op. cit.,* p. 507.

[35] Szász, Antónia, *A kiberbűnözés társadalmi kontextusa* [*The social context of cybercrime*]. In: Kovács, Janka – Kökényessy, Zsófia – Lászlófi, Viola (eds.): A normán innen és túl [*From here and above of the norm*]. ELTE BTK Történeti Kollégium. Budapest, 2017. pp. 95-97.

[36] See also: Kollár, Csaba, *A magyarországi online csalások fontosabb tulajdonságai* [*The characteristics of online frauds in Hungary*]. Belügyi Szemle 2018/10. pp. 58-61.

[37] See also: Gábor, Tamás – Kiss, Gábor Dávid, *Bevezetés a kriptovaluták világába*, [*Introduction to the world of crypo currencies]*. Gazdaság és Pénzügy 2018/1, pp. 31-65.

[38] Simon, Béla, *Kriptovaluták – rendészeti válaszok*, [*Cryptocurrencies – law enforcement responses*]. Belügyi Szemle 2018/10. pp. 74-77.

The so-called *Ransom programs*,[39] *software*[40] represent a new trend that allow access to a smartphone for a ransom. Given the importance of smartphones to a large portion of the population, this is the area where the prospects for results are most promising[41]. Unfortunately, malwares have previously posed a threat to mobiles as well as personal computers[42].

e) The Cloud Services

The growing amount of data that has to be stored and accessed rapidly, and the growth of the internet and on the other the declining size of hardware, gave birth to the idea and the need for businesses that users should not store their data on their own computers, but at a so-called *cloud service provider*[43].

Cloud service providers store the data on multiple servers and other devices, in the same or a in a different country, and it can be accessed by the user anytime and anywhere where there is an internet connection.

According to András Zoltán Nagy[44], in addition to its practical and convenience possibilities, cloud service causes a lot of problems for criminal justice[45]. Logged information stored at the cloud provider as digital evidence is typically dynamic digital content; it certifies the user activities, processes, data changes.

According to Nóra Georgina Tóth, very serious *data security issues* also arise in connection with cloud computing, as data storage is not tied to a location, and thus differences in the security standards of the data protection regulations of different countries and regions are unresolved[46]. While it may be cheaper for a company to use cloud technologies, the *risk of information security is* much higher, not to mention cases where the cloud service company goes bankrupt, and with it, irreplaceable data seems to go to "nirvana" for the company hiring the service.

Difficulties of legal aids in criminal matters[47] in connection with cloud services:

– the condition of double incrimination in general (in the case of content communication – doubtful due to different interpretations of freedom of expression);

---

[39] Budai, Balázs – Gerencsér, Balázs Szabolcs – Veszprémi, Bernadett (eds.), *A digitális kor hazai közigazgatási specifikumai. A magyar közigazgatás és közigazgatási jog általános tanai X. kötet*. [*The specifics of the domestic administration in the digital age. General Doctrines of Hungarian Public Administration and Administrative Law Volume X.]*. Dialóg Campus Kiadó. Budapest, 2018. p. 381.

[40] About the beginnings of cybercrime see further in: Parti, Katalin – Kiss, Anna, *A számítástechnikai bűnözésről akkor és most* [*About cybercrime then and now]*. In: Bárd, Petra – Hack, Péter – Holé, Katalin (eds.): Pusztai László emlékére. Országos Kriminológiai Intézet – ELTE Állam-és Jogtudományi Kar. Budapest, 2014. pp. 298-301.

[41] Bányász, P., *op. cit.,* p. 373.

[42] Kempin, S., *op. cit.,* p. 617.

[43] Nagy, Zoltán András, *A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén* [*The future has been going on since yesterday. Challenges of modern technical-technological processes in the field of law*]. Belügyi Szemle 2018/10. p. 46.

[44] Nagy, Z., *op. cit.,* p. 47.

[45] See further: Kovács, Zoltán, *Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.* [*Examination of legal control methods for cloud-based systems I.*]. Hadmérnök, 2013/3. pp. 184-189.

[46] Tóth, Georgina Nóra, *Számítástechnikai felhők és veszélyei* [*The computer technology cloud and its dangers*]. Óbuda University e-Bulletin 2011/1. pp. 449-451.

[47] The Act XXXVIII. of 1996 (From Section 62) and the Act CLXXX of 2012 (From Section 66/A).

– it is not possible to localize in which country the servers are located;

– it is not possible to localize on which server of which country the incriminated content is located at the time of the offense and adjudication[48].

A circumstance that makes the success of criminal proceedings related to cloud services difficult is the specific legal regulatory background of the given country[49].

An add-on, the GDPR[50] prohibits the so-called *profiling ads* that are generated by service providers according to the users profiles and interests (e.g., previous browsing, social post, other Internet activity, "collecting" spyware for marketing purposes). The prohibition rule reads as follows:

„The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [GDPR Article 22. (1)].

According to András Zoltán Nagy, this is a clear and unambiguous rule but if the user has entered a program of the given service provider (email, browser, cloud etc.), there may be a legal interpretation that the advertisement can showed in accordance with the user profiles. It is also a problem if large service providers store European users' data on overseas or Asian servers rather than in Europe.

f) The Question of Jurisdiction

Crimes committed in connection with smartphone are often have *international* nature, but law enforcement is confined to national frameworks. András Zoltán Nagy in connection with this correctly formulates the need that a unified criminal law action programme is required, whether regional or global[51].

In the case of crimes committed on android phones, it is very difficult to determine[52] where the perpetrator is geographically located and which country should be considered the place of the commission, ergo which country's criminal code should be applied in the certain case. This would require IT experts.

This causes problems in the legal practice due to there is a greater or lesser tendency in all authorities to declare a lack of jurisdiction, because these cases are *problematic*. They are difficult-to-detect criminal cases and the law enforcement is reluctant to start a high probability unsuccessful investigation, so everyone spreads their hands and points to the other authority of that country[53].

---

[48] Nagy, Z., *op. cit.,* p. 48.

[49] Stănilă, Laura, *Legal ccculturation and criminal law. Between uniformity and preservation of identity*. Law Series Annals of the West University of Timisoara Vol. 2019, Issue 1, pp. 119-131.

[50] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Further referred as GDPR.

[51] Nagy, Zoltán András, *A joghatóság problémája a kiberbűncselekmények nyomozásában* [*The problems of jurisdiction in the investigation of cybercrimes*]. In: Homoki-Nagy, Mária (ed. in chief), Karsai, Krisztina – Fantoly, Zsanett – Juhász, Zsuzsanna – Szomora, Zsolt – Gál, Andor (eds.): Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Acta Universitatis Szegediensis Acta Juridica et Politica Tomus LXXXI. Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Szeged, 2018. pp. 755–759.

[52]Fenyvesi, Csaba: *A kriminalisztika tendenciái. A bűnügyi nyomozás múltja, jelene, jövője [The tendencies of criminalistics. The past the present and the future of criminal investigation]*. Dialóg Campus Kiadó. Budapest-Pécs, 2014. pp. 218-219.

[53] See: Stănilă, Laura, *Principiul legalității: de la lex scripta la lex certa*. Law Series Annals of the West University of Timisoara Vol. 2018, Issue 2, pp. 61-63.

III. The Legal Regulation Background in Hungary

The information technology crimes appeared in the Hungarian substantive criminal law in the middle of the 1990's as the computer devices started to spread.

The first statutory provisions were related to intellectual properties. The amending Act XVII. of 1993 of the Act IV of 1978 on the Criminal Code codified the statutory provision of Infringement of Copyright and Certain Rights Related to Copyright (Section 329/A) which guaranteed criminal law protection against software counterfeiting as well.

The modifying Act IX. of 1994 introduced the *information technology crimes* to the Criminal Code. Alongside Computer Fraud (Section 300/C.) Counterfeiting of Credit Card (Section 313/B.), Credit Card Fraud (Section 312/A.) became punishable under the law in Hungary.

Two and four years later another two amending acts of the Criminal Code (The Act of 1996 and the Act LXXXVII of 1998) expanded the statutory provisions of computer fraud and credit card counterfeiting[54].

The Act LXXIII of 1997 established the legal basis of criminal law means against the creators and distributors of child pornography (Section 195/A. of the Criminal Code).

The Act CXX of 1999 brought conceptual changes because – alongside the changes of Special Part – new regulations appeared in the General Part of the Criminal Code in connection with the evolution of computer technology and of the environment. The interpretation section of the General Part (Section 137. 12.) extended the concept of broad publicity with electronic communications network as well.

In the Special Part alongside the previously mention Infringement of Copyright and Certain Rights Related to Copyright appeared new crimes like the Compromising or Defrauding the Integrity of Technological Measures for the Protection of Copyright and Certain Rights Related to Copyright (Section 329/B.) Falsifying Data Related to Copyright Management (Section 329/C.), and Violation of Industrial Design Rights (Section 329/D.).

The Act CXXI. of 2001 which amended the substantive criminal law by implementing the Convention on Cybercrime from the Council of Europe in first of April 2002.

The crime of Illicit Access to Data (Section 422. of the CC), Breach of Information System or Data (Section 423. of the CC) and the Compromising or Defrauding the Integrity of the Computer Protection System or Device (Section 424 of the CC) are based on the above mentioned Cybercrime Convention and on the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[55].

IV. The Criminological Aspects of the Android Related Crimes

The main criminological characteristics of crimes committed against android systems, – like other information technology delicts, – is *anonymity*[56]. The World Wide

---

[54] Nagy, Zoltán András, *A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda* [*About the codification of the crimes committed in computer environment de lega lata – de lege ferenda*]. Belügyi Szemle 1999/11. pp. 16-23.

[55] The justification of the Criminal Code (Act C of 2012.)

[56] Gyaraki, Réka, *A számítógépes környezetben elkövetett gazdasági bűncselekmények*. [*Economic*

Web provides anonymity, as on the one hand, legal provisions do not always criminalize those who log in with a false name, and if all this is revealed, it is easy to remain hidden behind a new false profile.

Speed is also good for offenders and unfavorable for law enforcement with a slow response time. By the time the perpetrators come to the attention of the authorities, hundreds, thousands or tens of thousands of victims have already been harmed by fraudsters.

Réka Gyaraki rightly draws attention to the *latency* of adroid delicts, as a significant number of cases – for various reasons e.g. shame, small amount of damage caused, distrust of the authorities etc. – victims do not report to law enforcement[57].

The fact that crimes remain hidden is sometimes explained[58], by the relatively low financial damage caused by the crime, as it is simply not worthwhile for victims to "*waste*" time, energy (and money) to make a police report, as there are no solid chances of finding out who the perpetrators are[59].

Crimes android systems gives a favorable opportunity[60] for organized crime that have expert skills in information technology[61].

It is difficult to predict what new criminal conducts will be induced by mobile phones as a they become a part of the payment system like an *electronic wallet* (e.g. with the technology Near field communication, abbreviated as NFC) as well[62].

A real threat can be the IT-related screening of "discarded", lost or discarded mobile phones if they fall into the hands of criminals[63].

V. The Possible Means of Protection Against Phones Running on Android Based Systems

Before analyzing the methodology for protection against criminal conducts, it is necessary to note that *proving* these crimes in accordance with the principles criminal

---

crimes committed in computer environment] In: Gaál Gyula – Hautzinger Zoltán (eds.), Pécsi Határőr Tudományos Közlemények XIII. Tanulmányok „A Biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja. Pécs, 2012. p. 236.

[57] Gyaraki, R., *op. cit.,* p. 236.

[58] Parti, Katalin – Kiss, Tibor, *Informatikai bűnözés* [*Information technology crimes*]. In: Borbíró, Andrea – Gönczöl, Katalin – Kerezsi, Klára – Lévay, Miklós (eds.): Kriminológia. Wolters Kluwer Kiadó. Budapest, 2016. p. 503.

[59] See: Gál, István László, *25 Years of fight against money loundering in Hunagry*. Journal of Eastern-European Criminal Law 2019.2. pp. 63-65.

[60] See also: Nagy, Zoltán András, *New technologies – new challenges to copyriht law*. Journal of Eastern-European Criminal Law 2015./2. pp. 165-175.

[61] See also Tóth Dávid, *Credit card fraud in Hungary*. In: Tuboly-Vincze, Gabriella (eds.): XIV. Országos Grastyán Interdiszciplináris Konferencia előadásai. PTE Grastyán Endre Szakkollégium. Pécs, 2015. pp. 87-89.

[62] Tóth, Dávid, *A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények büntetőjogi szabályozása*, [*The regulation of crimes related to cash substitute payments instruments*] In: Kecskés, Gábor (eds.): Doktori Műhelytanulmányok 2015. Széchenyi István Egyetem Állam-és Jogtudományi Doktori Iskola. Győr, 2015. pp. 231-233.; Gál, István László – Tóth, Dávid, *Risk analísis of counterfeitin: money in Hungary and in the EU*. Journal of Criminology and Criminal Law 56 (3). 2018. pp. 7-22.

[63] Deák, Veronika: *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során* [*The role of open source intelligence ont he implementation of cyber attacks*], Hadmérnök 2018/3. p. 400.

procedure[64] can be *difficult*, as so many new viruses are "born" (according to some opinions every 8 days) that it is almost impossible to trace them[65]. What also makes these cases difficult is the constant relocation of mobile devices, the place and time of potential evidence is constantly changing, and the jurisdictional questions (e.g. different rules of evidence in different countries etc.).

The creation of various alternative virtual means of payment (e.g. bitcoin) has also become a practical "consequence" of the criminal conducts staying in *the folding screen of anonymity*.

Every participant has to take part in prevention: the developers, the producers, the users, the law enforcements, and the authorities. Modern up to date preventive means are also essential in combatting cybercrime.

According to Simon KEMP, who considers the theoretical model of *situational crime prevention* as a starting point, three main strands can be identified to reduce crime: a) making it harder to commit an act, b) reducing the profit of crime, and c) concretizing the rules (focusing on prevention).

– The *realization of the crime is hindered* by conscious and careful user behavior e.g. installing an antivirus program; password storage methods should not be implemented on the device used; regular program updates, downloading applications from legal (official) sources.

– The *profit* of criminal behavior can be reduced[66] by various prior protection measures, e.g. preferably do not do online banking on android mobile phones; do not save credit card details, if you do online banking, set limits; in the case of online banking, the SMS-Tan process must be performed on a different device; purchases in App Stores should be made with pre-loaded cards; making unsolicited advertisements by third parties subject to authorization; consistently encrypt confidential data or store it on mobile devices at all.

– In terms of emphasizing the rules: developing and disseminating prevention offers to users, as the majority of users do not place enough emphasis on mobile security, do not adequately assess its risks.

VI. Conclusion

Android-powered devices have clearly become the focus of criminal associations. Crime trends related to mobile use are, on the one hand, influences a professional, purposeful criminal environment; on the other hand, it is affected by security vulnerabilities in users and manufacturers.

It can be clearly demonstrated that the user himself can protect himself from significant damage by simple manual measures (e.g. avoiding the storage of sensitive data on a mobile device), although these measures are against the convenience of the user. We need to find the "aurea mediocritas" (*golden mean*) between user convenience and the double squeeze of IT security.

---

[64] Stănilă, Laura: *Specific aspects ont he right to a fair trial in the recent caselaw against Romania*, Journal of Eastern European Criminal Law 2019.1. pp. 166-169.

[65] See furhter analyses in: Fantoly, Zsanett – Lichtenstein, András, *Számítógépes kockázatelemzés és büntetőeljárás*, [Computer risk analyses and criminal procedure], Belügyi Szemle 2018/10. pp. 7-11.

[66] Stan, Adrian, *The challenges of extended confiscation. Directive 2014/42/EU and tranposing difficulties in Romania*. EU and Comparative Law Issues and Challenges Series Issue 3.2019. pp. 637-658.

References

1. Bányász, P., *Az okos mobil eszközök biztonsága* [*The smart mobile devices*]. Hadmérnök 2018, June.

2. Budai, B., Gerencsér, B.S., Veszprémi, B. (eds.): *A digitális kor hazai közigazgatási specifikumai. A magyar közigazgatás és közigazgatási jog általános tanai X. kötet.* [*The specifics of the domestic administration in the digital age. General Doctrines of Hungarian Public Administration and Administrative Law Volume X.*]. Dialóg Campus Kiadó. Budapest, 2018.

3. Deák, V., *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során* [*The role of open source intelligence ont he implementation of cyber attacks*]. Hadmérnök 2018/3.

4. Elek., B., *From poaching to financing terrorism.* Journal of Eastern-European Criminal Law 2016.1. pp. 190-200.

5. Erdősi, P.M., Horváth, A., Kiss, F*., Információrendszerek biztonsági kockázatainak vizsgálata a szoftverek nyíltsága szerint.* [*Examining the security risks of information systems according to the openness of the software*]. In: IT és hálózati sérülékenységének társadalmi hatásai [*Social impacts of IT and network vulnerabilities.*], Információs Társadalomért Alapítvány, Budapest. 2016.

6. Fantoly, Z., Lichtenstein, A., *Számítógépes kockázatelemzés és büntetőeljárás* [*Computer risk analyses and criminal procedure*]. Belügyi Szemle 2018/10. pp. 5-22.

7. Fenyvesi, Csaba: *A kriminalisztika tendenciái. A bűnügyi nyomozás múltja, jelene, jövője.* [*The tendencies of criminalistics. The past the present and the future of criminal investigation*]. Dialóg Campus Kiadó, Budapest-Pécs, 2014.

8. Forgács, I., *Senki földje a jogban: a globális vállalat* [*No one's land in law: the global company*]. Jogtudományi Közlöny 2017/2.

9. Gábor, T., Kiss, G.D., *Bevezetés a kriptovaluták világába*, [*Introduction to the world of crypo currencies*] Gazdaság és Pénzügy 2018/1.

10. Gál, L.I., *Economic policy, criminal policy and economic crimes,* Journal of Eastern-European Criminal Law 2019.1.

11. Gál, L.I., Serbakov, M.T., *How acts of terrorism are financed and orchestrated in secrecy today: criminal offences, donations, legal business and smartphone applications*. Journal of Eastern-European Criminal Law 2019.1.

12. Gál, L.I., *25 Years of fight against money loundering in Hunagry*. Journal of Eastern-European Criminal Law 2019.2.

13. Gál, L.I., Tóth, D., *Risk analísis of counterfeitin: money in Hungary and in the EU*. Journal of Criminology and Criminal Law 56 (3). 2018.

14. Gyaraki, R., *A számítógépes környezetben elkövetett gazdasági bűncselekmények.* [*Economic crimes committed in computer environment*]. In: Gaál Gyula – Hautzinger Zoltán (eds.), Pécsi Határőr Tudományos Közlemények XIII. Tanulmányok „A Biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja. Pécs, 2012.

15. Kempin, von S., *Android Smartphones im Fokus krimineller Aktuere* [*Android smartphones in the focus of criminal actors*]. Kriminalistik 10/2014.

16. Kollár, C., *A magyarországi online csalások fontosabb tulajdonságai,* [*The characteristics of online frauds in Hungary*] Belügyi Szemle 2018/10.

17. Koska, M.H., *Wi-Fi hálozatok két kijátszhatósági pontja: WPA2 és ROGUE AP* [*The two vulnerabilites of Wi-Fi networsk: WPA2 and ROGUE AP*]. Hadmérnök 2018/3.

18. Kovács, Z., *Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.* [*Examination of legal control methods for cloud-based systems I*]. Hadmérnök, 2013/3.

19. Marsi, T., *A célzott támadások és megelőzésük sérülékenységvizsgálattal* [*Targeted attacks and their prevention through vulnerability testing*]. In Bodó, A.P., Marsi, T., Sebők, V., Zámbó, N., *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára* [*Targeted cyber attacks – Annual training for the manager responsible for the protection of electronic information systems*], Nemzeti Közszolgálati Egyetem, Budapest, 2018.

20. Nagy, Z.A., *A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda* [*About the codification of the crimes committed in computer environment de lega lata – de lege ferenda*]. Belügyi Szemle 1999/11.

21. Nagy, Z.A., *Az informatikai bűncselekmények* [*The information technology crimes*]. Magyar Tudomány 2001/8.

22. Nagy, Z.A., *New technologies – new challenges to copyriht law*. Journal of Eastern-European Criminal Law 2015./2.

23. Nagy, Z.A., *A joghatóság problémája a kiberbűncselekmények nyomozásában*. [*The problems of jurisdiction in the investigation of cybercrimes]*. In Homoki-Nagy, M. (ed. in chief), Karsai, K., Fantoly, Z., Juhász, Z., Szomora, Z., Gál, A. (eds.), Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Acta Universitatis Szegediensis Acta Juridica et Politica Tomus LXXXI. Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Szeged, 2018.

24. Nagy, Z.A., *A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén* [*The future has been going on since yesterday. Challenges of modern technical-technological processes in the field of law*]. Belügyi Szemle 2018/10.

25. Parti, K., Kiss, A., *A számítástechnikai bűnözésről akkor és most* [*About cybercrime then and now*]. In Bárd, P., Hack, P., Holé, K., (eds.), Pusztai László emlékére. Országos Kriminológiai Intézet – ELTE Állam-és Jogtudományi Kar, Budapest, 2014.

26. Parti, K., Kiss, T., *Informatikai bűnözés [Information technology crimes]*. In Borbíró, A., Gönczöl, K., Kerezsi, K., Lévay, M., (eds.): Kriminológia. Wolters Kluwer Kiadó, Budapest, 2016.

27. Rátai, B., *Nyílt forrású /open source/ szellemi közjavakkal kapcsolatos gazdasági-üzleti kérdések elemzésének alapjai [Fundamentals of analysis of economic-business issues related to open source intellectual public goods].* Infokommunikáció és Jog 2011/43.

28. Simon, B., *Kriptovaluták – rendészeti válaszok, [Cryptocurrencies – law enforcement responses*], Belügyi Szemle 2018/10.

29. Stan, A., *The challenges of extended confiscation. Directive 2014/42/EU and tranposing difficulties in Romania*. EU and Comparative Law Issues and Challenges Series Issue 3.2019.

30. Stănilă, L.M., *Principiul legalității: de la lex scripta la lex certa*. Law Series Annals of the West University of Timisoara Vol. 2018, Issue 2.

31. Stănilă, L.M., *Legal ccculturation and criminal law. Between uniformity and preservation of identity*. Law Series Annals of the West University of Timisoara Vol. 2019, Issue 1.

32. Stănilă, L.M., *Specific aspects ont he right to a fair trial in the recent caselaw against Romania*, Journal of Eastern European Criminal Law 2019.1.

33. Szabó, A., *A felhasználók digitális lábnyomának, anonimitásának vizsgálata technikai szempontból. II. rész Mobil eszközök [Demonstrating user anonimity and digital footprint with technical tools part II. – Mobile devices],* Hadmérnök 2018/1.

34. Szász, A., *A kiberbűnözés társadalmi kontextusa [The social context of cybercrime]*. In: Kovács, Janka – Kökényessy, Zsófia – Lászlófi, Viola (eds.): *A normán innen és túl. [From here and above of the norm]*. ELTE BTK Történeti Kollégium, Budapest, 2017.

35. Tóth D., *Credit card fraud in Hungary*. In: Tuboly-Vincze, Gabriella (eds.): XIV. Országos Grastyán Interdiszciplináris Konferencia előadásai. PTE Grastyán Endre Szakkollégium, Pécs, 2015.

36. Tóth, D., *A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények büntetőjogi szabályozás, [The regulation of crimes related to cash substitute payments instruments]*. In Kecskés, G. (ed.): Doktori Műhelytanulmányok 2015. Széchenyi István Egyetem Állam-és Jogtudományi Doktori Iskola. Győr, 2015.

37 .Tóth, G.N., *Számítástechnikai felhők és veszélyei [The computer technology cloud and its dangers]*. Óbuda University e-Bulletin 2011/1.

Hate Speech in Electronic Media and Challenges for the Criminal Justice System of the Republic Of Serbia

***Prof. dr. Aleksandar R. Ivanović*[1]**

Abstract

The author deals with the analysis of hate speech in electronic media in the Republic of Serbia, with a special focus on criminally legal repression. In this regard, the author seeks to analyze the current state of hate speech in electronic media and the provisions of criminal substantive law governing this matter, with the aim to point out the challenges that this form of criminal manifestations imposes to the criminal justice system of Republic of Serbia, and to offer certain recommendations for improving the situation on the field of combating online hate speech with measures of criminal law.

Keywords: *online hate speech, criminal offences, detection, prosecution, criminal justice system*

I. Introduction

Digital technologies provide opportunities for learning and education, provide access to information, can provide economic opportunities by offering young people training opportunities and access to job search services, or by creating new types of jobs. However, there is also the dark side of the Internet and digital technologies, from sexual or other types of abuse, child trafficking and other illegal activities that harm children, hate speech, violent radicalization and extremization, and so on.

The basic idea of the creators of the Internet is that the Internet should be a free highway, a public space where everyone can say what they have in mind. This wonderful innovation of the unrestrained platform is unfortunately abused. The Internet is open to use and abuse. Internet abuse threatens public space and poses many challenges at all levels: to the individual, the community, the state and the international community. Public authorities are in the early stages of learning how to deal with and how to combat Internet abuse, and this is especially true in the fight against hate speech on the Internet[2].

The Internet is the safest and most powerful means of spreading hate speech. A virtual space that can mobilize a large number of like-minded people at high speed and poses a real threat to society if it moves to the real world, which often happens. The Internet enables the creation of global groups whose members are physically

---

[1] Associate professor of Criminal law, Department for law sciences, International University of Novi Pazar, Republic of Serbia, Contact: a.ivanovic@uninp.edu.rs.

[2] Ivanović, R.A. (2018) *Hate speech on internet through illegality to punishment.* Yearbook, no.1 – Human rights protection „From unlawfulness to legality", Novi Sad: Provincial Protector of Citizens – Ombudsman and Institute of Criminological and Sociological Researcsh Belgrade, p. 416.

distant but between whom there is a sense of closeness due to the interactivity of social networks. It is in the explanation of the behavior of the individual in the crowd that the explanation of the dangers of hate speech over the Internet lies. In a group, the individual loses his individuality. She enjoys the protection of the majority and the comfortable comfort of anonymity. Due to the difficulty of identifying the individual in the mass, the sense of responsibility for one's actions is lost, which becomes much more extreme and destructive. There is a mass spread of certain behaviors like viruses, because individuals in the crowd tend to accept and follow the ideas, opinions and emotions of the majority without question[3].

Hate speech is certainly not a stranger on the Internet, or even in conventional media, but it has certainly found its full negative affirmation on social media. This enables him, first of all, the anonymity of the subject as well as the focus on as large a population as possible, but also the distance from the passive subject, i.e. the subject to whom the hate speech itself is addressed[4].

The benefits of the Internet for disseminating views and opinions are used by those who promote democratic values and the rule of law, as well as by racist or similar hate groups. The Internet is filled with a multitude of diverse commercial and private users. Among the attitudes available in interactions on the Internet are those that humiliate people on the basis of their race, ethnicity, national origin, gender and sexual orientation, and the like. Hate groups exploit this relatively cheap medium for ideological distribution. In this way, they can distribute pamphlets, letters and pictures to groups of users who can anonymously participate in strategic racist meetings and planning committees. One of the ugly sides of the internet is that it provides a global forum for advocates of intolerance and inequality[5].

Hate speech often appears online, especially on social networks. Hate speech is defined as an expression that insults, threatens or encourages attacks on individuals or social groups based on race, religion, national origin, sexual orientation, disability or other characteristics. As in the real world, so in the virtual world, when we talk about the problem of hate speech, it is impossible not to touch on the issue of the relationship between freedom of speech on the Internet and hate speech on the Internet. In this regard, one of the most complicated questions regarding the relationship between freedom of speech and hate speech is the question of where does free speech end and where "offensive words" begin? If we start looking for an answer to this dilemma among theorists from the United States, we can conclude that in that sense, the gray zone has never transformed into black or white in this regard. Namely, libertarians who claim that freedom of speech implies hate speech believe that placing restrictions on freedom of speech weakens all rights. They also firmly believe that the state government should not restrict hate speech, unless it directly threatens peace. Communitarists share the opposite view. They believe that freedom of speech takes the last position in terms of the security of the community and all its citizens. Their view is that hate speech should not be allowed when propagated by those who should prevent individuals or groups from being treated with dignity and

---

[3]

[4] Miladinović, A., (2013) *Facebook and crime* [*Fejsbuk i kriminalitet]*, Banja Luka: International Association of Criminalists, p. 180.

[5] Tsesis, A., (2001) *Hate in Cyberspace: Regulating Hate Speech On the Internet*, San Diego Law Review 817/01, p. 832.

respect. Libertarians, on the other hand, argue that such restrictions would severely restrict freedom of speech and would be subject to an interpretation of intent that would be impossible to determine[6].

It is often very difficult to define precisely when speech actually hurts someone, that is, where the dividing line is between freedom of speech and hate speech. Freedom of speech is a concept according to which no one can be legally prosecuted for the things he said or stated. According to this concept, no one can stop someone from saying something that contains hatred or prejudice. It is his right to freedom of expression.

However, hate speech is only someone's opinion or attitude, but the possibility that he could actually harm someone with that speech. And that is forbidden under international law. It is very ungrateful to try to point out the boundary between freedom of speech and hate speech. In this regard, in the next part, we will try to point out through examples where the limit of freedom of speech ends, and hate speech begins.

For example, someone may tell a particular person that they do not love him/her because of their ethnicity or cultural heritage. That is somewhat wrong, but it is his right and he cannot be arrested, prosecuted or punished by law for that. However, if someone threatens to kill someone or publicly calls on others to attack someone because of ethnicity or cultural heritage etc., it crosses the line of freedom of speech. This has gone from freedom of speech to a real threat that must be taken seriously. Therefore, hate speech has all the characteristics of freedom of speech plus some additional characteristics that distinguish it from it. What are the characteristics that distinguish freedom of speech from hate speech, are seen differently in the eyes of observers of that speech, from individual to individual, from one social group to another, and therefore we have a problem to say clearly in some situations this is hate speech and not freedom of speech, and vice versa.

When we considering hate speech on the Internet, we must take into account the existence of two types of media, the classic ones, which with the advent of the Internet got their digital, i.e. online version and the so-called social media. So we can divide the media into those that serve us ready-made information (newspapers, radio, and television) and those that allow us to participate in the creation, assessment, exchange and distribution of the same. The former are usually call as classic medias and the latter social media[7].

While these first long exists at social life, and with the appearance of the Internet are just get their digital or online version, the latter appeared only with the development of modern information and communication technologies, especially the Internet, which now for the first time enables interactivity between the sender – recipient of message. Interactivity allows the establishment of a feedback of the participants in the communication process[8].

Social media is most often defined as a set of new sources of online information that is created, initiated, circulated and used by consumers with the intention of

---

[6] Gitlin, M. (2018) *When Is Free Speech Hate Speech?* New York: Greenhaven Publishing, 2018, p. 8.

[7] Miladinović, S., (2015) *The growing importance of social media in a dynamic society* [*Rastući značaj socijalni medija u dinamičnom društvu]*, Conference proceedings: Statehood, democratization and a culture of peace, Faculty of Philosophy, University of Nis, Nis, p. 342.

[8] *Ibid.*

exchanging information about products, brands, services, features and specifics. They include numerous and diverse media, such as blogs by company sponsors for discussion, chat rooms, websites and consumer forums for ranking products and services, online discussion forums, blogs (sites containing digital, audio, images, movies or photos), social networking websites etc. The most common form of social medias are social networks. In this regard, in the next part of the paper we will present the forms of expression of hate speech through classical media, which have received their digital or online form through the Internet, such as the so-called electronic newspapers and through social media, among which from the aspect of hate speech the most current are social networks. However, before embarking on the analysis of the forms of expression of hate speech on the Internet, it is necessary to point out the current state regarding the issue of online hate speech and criminal repression in the Republic of Serbia. With regard to legal norms and sanctions prescribed for them, we can divide all hate speech into those that are allowed by law, those that are prohibited by law and represent a criminal offense and those that are sanctioned by some other norms that most often belong to self-regulation (codes of ethics, professional standards and conditions of use of communication platforms on the Internet etc.). It should be noted here that although precise data covering all content in internet communication is not yet available, according to existing research, hate speech that is considered a crime, extreme speech that calls for violence and other crimes, is very rare. In the analysis of hate speech, which is not illegal in Serbia, it was noticed that this type of speech makes up about 20% of the entire internet content reported for violating the rules of the Code of Journalists on various grounds[9].

In the Final Report on Serbia of the European Commission against Racism and Intolerance (ECRI), which was adopted on March 22, 2017, ECRI expressed great concern over the increasing hate speech in public discourse in Serbia, which is further encouraged by media coverage. Politicians and the media use incendiary, pejorative and nationalist language and there has been a significant increase in regional tensions in the former Yugoslavia. The current public discourse is reminiscent of hate speech used before the recent wars in the region, and polls indicate the existence of great social distance between different segments of the population. Hate speech is spreading more and more online[10]. ECRI also states that it is necessary to improve the recording, investigation and punishment of hate speech and hate crimes and to ban racist, homophobic and transphobic hooligan groups (ECRI report 2017:5). According to the statistics of the prosecutor's offices, between January 1, 2011 and May 30, 2016, criminal charges were filed for hate speech against 216 people. Of these, 211 were filed under Article 317 of the CC (Instigating of national, racial and religious hatred and intolerance), three under Article 387 of the CC (Racial and other discrimination) and two under Article 174 of the CC (Infringement of reputation due to racial, religious, national or other affiliation) racial, religious, national or other affiliations). In 207 cases, hate speech referred to the victim's national or ethnic origin, in five cases to her religion, in one case to citizenship and in one to sexual orientation. Most crimes are committed against Roma and lesbians, gays, bisexuals or transgender (LGBT) people. 106 people were indicted and 41 people were convicted. 138 reports were

[9] Nikolić, P., (2018), *Internet hate speech in Serbia [Govor mržnje u internet komunikaciji u Srbiji]*, Doctoral Dissertation, Faculty of political sciences, Belgrade, p. 4.

[10] ECRI report on Serbia (fifth monitoring cycle) (2017), p. 4.

filed due to racial (20) and homophobic, i.e. transphobic (118) cybercrime. The outcome of these cases is convictions against 20 persons under Article 138 of the CC (Endangering Security), against three persons under Article 317 of the CC (Instigating of national, racial and religious hatred and intolerance) and against one person under Article 387. CC (Racial and other discrimination)[11].

Despite a number of positive developments, ECRI notes with regret that the criminal justice system still fails to effectively deal with hate speech. First, ECRI was informed that non-reporting is very common: many victims do not report hate speech to the police and other authorities. To address this issue, there need to be police officers and prosecutors specialized in investigating hate speech and hate crimes. As hate speech spreads more and more online, these officers must have the specialist knowledge and technical means to conduct investigations effectively; they must also work closely with the MUP's High-Tech Crime Department. Additional training on dealing with hate speech and hate crimes should be concentrated on these individuals[12].

Second, civil society groups state that the police are not always open to receiving complaints about hate speech cases, especially in relation to Roma and LGBT people. In addition, members of vulnerable groups often do not know where and how to complain about these incidents. More than 2 years have passed from the adoption of this report to the moment of writing this paper, and the Republic of Serbia has taken numerous measures to improve the situation in terms of criminally legal repression of online hate speech. Also, when the WHO declared a pandemic of the COVID-19 virus, at Republic of Serbia was introduced emergency state during which hate speech towards members of minority groups has been increased. The state of emergency and the restriction of freedom of movement as well as bigger use of social networks and Internet platforms', together with fear of infection lead to increasing of online hate speech against migrants and foreigners. Also, when it comes to online hate speech during the crisis with the virus, it should be emphasized that in the Republic of Serbia, in the electronic media and on social networks, there has been an expansion of sexist and misogynistic statements and attacks mainly on women performing public functions (teachers, doctors, members of various crisis groups etc.).

For the above reasons, in this paper we want to address the following issues: whether the Republic of Serbia has an adequate criminal framework for combating hate speech in electronic media, especially in conditions imposed by the crisis with the COVID-19 virus, as well as, what are challenges on combating hate speech on the Internet before the criminal justice system of the Republic of Serbia.

II. Hate Speech in Online Versions of Classic Media

The increasing use of the Internet has led to the classic media developing their online versions. So today we have the sites of many television channels and radio channels, where we can relatively quickly and easily find an archive of video and audio content that is broadcast on a given television or radio. Also, many television and radio channels have on their sites, the option of watching their program live over the Internet (so-called live streaming). Also, when it comes to print media, i.e.

[11] *Ibid*, p. 11.
[12] *Ibid*, p. 17.

newspapers, they also have their own websites, where journalistic articles and news, together with archives of printed content can be found very easily and quickly. What is a common feature of the online versions of the aforementioned media is that not only did they increase the potential audience in this way, that is, they accelerated the process of publishing information and provided the so-called "Digital eternity"[13] of the same, they have already created the possibility to receive information from their audience, i.e. to have two-way communication with the audience. Namely, almost all of these media have the option of commenting, i.e. leaving comments below the published video, audio or textual content. Which, as in the case of social networks, which will be discussed later, gives users of these media the opportunity to influence the creation of content, or information that is disseminated through online versions of these media.

So, online versions of these media have two-way communication, the first that goes through the published video, audio or textual content by the editor of that media, and the second that appears in the form of comments from the audience, on the published content on that media.

The expansion of online media in this format represents a significant step in the democratization of reporting and the rise of the so-called. "Citizens journalism", which was further encouraged by social networks, primarily Facebook, Twitter and YouTube. Video broadcasts of protests, speeches by state officials, reporting on communal and similar problems, and analysis of social phenomena – all this and much more information is available at any time, on any device that can connect to the Internet. The emergence of online media is particularly characteristic of the local level. Namely, the expansion of online media and journalistic reporting through them at the level of local communities occurs primarily because the national media generally do not pay enough attention to local problems and opportunities in smaller communities.

When it comes to hate speech, it can appear on these media in classic forms, texts, videos, audio recordings that contain a message of hatred and a call for discriminatory or offensive activities. This is especially a problem with online media of this type that are of the local type. Namely, it is very common at the level of local communities at the position of journalists or editors in those medias are appointed persons who do not have a formal education in the field of journalism. Also, it is not so rare that these media are funded, i.e. they are owned by persons who are associated with certain political parties or interest groups operating in the area of that local community. In such situations, it often happens that these media are used as a means of a certain interest group to place content with which they want to discredit their political opponents, i.e. to propagate hatred and intolerance towards certain social groups, political options and their members or supporters. As a consequence, we have tendentious texts at this type of media, i.e. other types of content that directly or indirectly disparage individuals or social groups due to some personal characteristics and call for their exclusion from society, their persecution, and even open physical attack. Given that these are online media of the local type, such content generally does

[13] Ivanović, R. A., Dečković, S., (2016) *The right to be forgotten as a fundamental principle of personal data protection in the digital age* [*Pravo da budeš zaboravljen (Right to be forgoten) kao temeljni princip zaštite ličnih podataka u digitalnoj eri]*, Conference proceedings – Volume 2 / Scientific conference with international participation: European integration: justice, freedom and security, Tara, 24-26. May 2016, Criminalistic-Police Academy, Hanns Seidel *Foundation*, Belgrade, p. 478.

not attract public attention at the national level, but at the local level can have very negative consequences, because the creation and transmission of such content can be an initial trigger for discriminatory or offensive activities against social groups targeted by published hate speech.

In addition to the previously described form of hate speech in these media, it also occurs in the form of comments, i.e. two-way communication between the editors / journalists of these media and the audience. Namely, the publication of some content on these media, which has to do with interethnic, interfaith, inter-party and other issues, generally accompanies the possibility of commenting on the given content by the audience (users). This is where the space for propagating hate speech appears. People who comment on such content do so under a pseudonym, i.e. a nickname that they assign to themselves. In this way, they provide anonymity and in their comments they utter insulting, disparaging and other similar words with which they propagate hatred towards members of certain social groups. Of course, the members of such media should take care of such comments and remove them if they represent hate speech. However, many editorial boards of such medias do not have administrators in charge of supervising such comments, or they have them but not in sufficient numbers to be able to follow all the comments published on their portals. In addition, a good part of these types of media lack an efficient comment pre-moderation procedure. Namely, the rule on what is allowed in the comments and what does not have to be clearly stated in order for users to be familiar with it. That is, to know on what basis their comment was not published or was removed. When it comes to online versions of classic media at the local level, it often happens that the pre-moderation of comments is not performed, i.e. that comments that represent hate speech appear on such media. Since the possibility of commenting creates space for public discussion, then a comment that contains hate speech through other comments that appear as a comment on the original comment is only multiplied. This phenomenon can be explained by the so-called spiral of conflict. Namely, the conflict in these comments arises when two or more people or parties express disagreement on a topic. Conflict can be over different things or sides (commentators) may simply have different opinions or views on a given issue. In the second phase of the conflict, the parties begin to discuss and present arguments defending their views. Each side is convinced that it opinion is right, and cares to explain its views to others. There is no real dialogue, because neither one side does not listen to the other. Both sides experience a situation that leads nowhere, and that makes them frustrated. In a situation where the other side is not listening and there is no real dialogue, each side will repeat their arguments, but with heightened emotions. At this stage, the participants in the conflict usually start to get angry and feel that their interests are not taken into account, and that they are being treated unfairly. At this stage, things start to be mentioned that, in essence, have nothing to do with the conflict. For example, instead of dealing with the current subject of discussion, that is, discussion, they begin a discussion about the characteristics of the other. Generalizations and presentation of negative characteristics of another person, i.e. the group to which that person belongs, are typical in these situations. The inclusion of such irrelevant elements is in fact a suitable ground for the appearance of hate speech in these comments. Usually it starts with insulting words at the expense of some social group and continues with the same or similar response from the other side. This is followed by the involvement of a larger number of people in mutual insults, which usually leads to the classic form of hate

speech in which it publicly invokes discriminatory and offensive activities against members of another social group. Here we should mention the so-called. mass influence. Namely, in such situations, individuals in the mass of similar comments identify with the opinion of the group, that is, the masses are encouraged by support, which often leads to the extremization of their attitudes and the intensification of hate speech. At this stage, comments are already beginning to be made, which in terms of content have no essential connection with the news, that is, the information around which the discussion started. In the worst case, such commenting on online media can result in the transfer of conflict from the virtual environment to the real one, that is, scheduling the place and time of physical reckoning in the real world. So, the point is that the bigger the spiral of conflict, that is, the mutual conflict in the comments, the harder it is to put it under control. Therefore, it is very important to punish those persons who publishing in the form of comments all provoke further commenting. Namely, it is completely natural for people to feel uncomfortable due to reading comments in which offensive words are uttered at the expense of the social group to which they belong, whether they are national, religious, political or some other social groups. Which is especially dangerous when it comes to young people, who still do not have a firmly formed awareness and attitudes on many issues, where such comments can cause prejudice, stereotypes and intolerance towards members of other social groups[14].

III. Hate Speech on Social Media

Social networks on the Internet today represent content that is very popular among Internet users, and especially among young people. In addition to representing a kind of trend, which contributes to their popularity, they also bring new opportunities in communication, as well as easier contact making, as well as the use and exchange of various content, which makes them attractive to use. Social networking platforms differ from other websites because they are based on individual activism. Another name for this type of connection is “web 2.0. applications”, where these platforms are considered "hosts", while third parties are allowed to post content on them[15].

There are three key actors in online speech on social media, and they are:

a) the sender, i.e. the one who sends the information;

b) the recipient, i.e. the one who receives the information;

c) an intermediary or service provider acting as an intermediary between the speaker and the listener.

Social networking platforms act as intermediaries and ensure communication between the sender and the recipient of information. Social Networks are services or, better said, a functionally interconnected set (synergy) of services on the Internet that combines both technology (observed through services) and social interactivity in order to communicate between members of a particular social network. In addition to enabling communication between users, these networks are also a form of online socializing ("new sociability"), but they also allow (which is also important) a form of self-promotion for

[14] Ivanović, R. A., Ranđelović, D., Totić, M., (2019) *Hate speech in electronic media and on social networks [Govor mržnje u elektronskim medijima in a društvenim mrežama]*, Novi Pazar: Monitor, p. 85.

[15] Citron, D. K., & Norton, H. (2011) *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*. Boston University Law Review, (4), p. 1437.

various purposes, then the ability to post videos, photos, blogs, playing various games and other useful (or less useful) activities through these networks[16].

Formal and one of the most well-known academic definitions of social networking sites, which contributes to further thinking and research of social online networking, defines online social networks as web-based services that allow individuals to create public or semi-public profiles within a closed centralized system, which have common connections (connections) and a selective list of connections which they call – friends (confidential circle of friends). These are usually a list of friends, as well as an overview of communication connections and practices that take place on the walls, notebooks, and personal pages of users[17].

Use, i.e. communication via social networks takes place in such a way that it is first necessary for the user to register online, i.e. create his profile. Creating a profile involves entering basic information about yourself and possibly uploading a profile photo, followed by verification of identity by clicking on the link received from the social networking platform by email, which the user specified when creating his personal profile. After confirming the identity, i.e. valorization of the user, he starts using the given social network. The first steps are usually reflected in the search for friends or acquaintances that already have profiles on that network, or in sending invitations to friends and acquaintances in order to establish communication with them on a given network, or to establish a connection. After establishing connections with acquaintances, i.e. friends, communication follows, which takes place in the form of textual, video, audio or graphic expression and is mainly manifested in the form of dialogue or monologue. In addition to creating and posting their own content on social networks, they also offer other communication options, such as the so-called likes, i.e. visual marking that a given user likes some published content, or so-called hate, i.e. visual indication that a given user does not like some published content. Then, there is the possibility of commenting on the same, as well as the possibility of sharing, i.e. further forwarding of a given content through its connections on social networks.

When it comes to hate speech on social networks, we single out the following forms as the most common. The first is to create and publish various content (text, video, audio or graphics) on your own profile. However, the profile is real, not fake, i.e. the profile really belongs to the person listed as the profile owner. Such phenomena of hate speech are mostly found in persons who try to propagate the rhetoric of hate by abusing their freedom of speech, on the one hand, and on the other hand, to give importance to the declared hate speech with their authority. So, in such manifestations of hate speech on the Internet, we have when a person does not want to hide his identity, that is he does not want to be anonymous, but that those to whom the content was sent (the public, the audience, or the Internet community within a given social network), as well as those to whom hate speech was addressed, know that she stated it. This form of hate speech is mostly resorted to, the so-called public figures, such as politicians, representatives of religious communities, media workers, journalists, representatives of various associations or organizations, leaders of fan groups etc. These are people who enjoy respect in certain social communities, which is why in this way they want to impose their views on those who respect their character and work, or at least get their support. Here, however, it should be emphasized that

[16] Miladinović, A., (2013), *op. cit.*, p. 36.
[17] *Ibid*, p. 37.

this type of manifestation of hate speech on social networks is not only characteristic of public figures. Namely, it is often used by persons who are unknown to the general public, and who in this way want to draw attention to themselves, i.e. to be accepted by some groups because of their "courage" to publicly express the rhetoric of hatred.

The second model is the anonymous publication of content that contains hate speech. This model is usually resorted to by people who do not want the public, as well as members of the social group to whom hate speech is addressed, to know its true identity. The reason for the anonymous, i.e. more specific pseudonymous statement of hate rhetoric is reflected primarily in the intention to avoid responsibility and bear the legal consequences for the words spoken. This is usually done by creating a fake profile, with fake personal information, and then using it to propagate hate speech.

The third model is sharing of content that contains hate speech, and which someone else posted on social networks. This is actually a concept of promoting hate speech, which is characteristic primarily for social networks, because they provide that opportunity. Unlike previous models, where the person who posts content that contains hate speech is also the author of that content, in this model the person who shares or shares that material is not the author of the same, but primarily an intermediary or transmitter between the real creator of content and further audience.

The fourth model of hate speech on social networks is commenting, i.e. giving comments on published or shared content. In this regard, everything that is stated when commenting on content published on online versions of classic media applies.

Finally, it should be noted that sharing and commenting can be done both from real profiles and from fake ones, i.e. under a pseudonym.

IV. Characteristics of the Internet that Favor the Spread of Hate Speech

Various forms of angry, threatening, racist, misogynistic epithets are viral on the internet. The reasons why this happens lie in the factors related to the internet. Namely, the number of Internet users is increasing every year. People prefer to communicate through social networks than in classic, direct or direct communication. Also, another possibility offered by the internet is anonymity and virality. This means that many things can be said or posted online anonymously and that overnight content can be viral online. Because of all this, it is necessary to point out the specific characteristics of the Internet that affect the spread of hate speech. So the features of the Internet that favor the spread of hate speech in the online world are as follows:

Global availability. Information can reach a billion people in an instant. This is a positive characteristic of the Internet, however, it can also be negative at the same time because it enables the mobilization of like-minded people, the spread of hate speech, especially in situations when it appears as a companion to criminal attacks. The Internet is available to almost everyone today. It is no longer necessary to have expensive computers to have internet access. You can also access it via "smart" phones that are available to everyone. Through them, global accessibility gained a wider, temporal dimension. Content on the Internet can be accessed at any time and in any place. You don't even have to be constantly active on networks. They signal to you when the desired content arrives.

Anonymity. The term anonymity comes from a Greek word “anonymia” (άνωνυμία), which means anonymous, unidentified or unknown name, and usually refers to the appearance of a person in public. Consequently, anonymity occurs if a

person's identity is involved in a non-transparent / unpublished process in an indefinable sense, because the actor remains unknown to other actors acting or does not appear to other participants in the interaction without recognizing his true identity[18]. However, anonymity does not necessarily require complete ignorance of a person's identity or lack of knowledge of his or her name. In order to distinguish anonymity from the impossibility of identifying a person, it is necessary for one party to vaguely know about the existence of the other party without knowing his or her complete identity. It is also necessary to point out the difference between anonymity and pseudonym, which is characterized by the use of a false name, although this practice can also lead to anonymity. In fact, we can freely say that pseudonymity can be described as a common variant of anonymity in which a different name from the real author of a content is shown[19]. Which is especially pronounced when it comes to anonymity on the internet. You can be completely anonymous online. You do not need to sign with your personal name when leaving comments on content that is published on the Internet. It is not necessary to leave personal data. You can open fake accounts on social networks, post fake pictures, present yourself as a fake name. You can have multiple e-mail addresses and if a portal requires registration, you do not have to leave your private or business email. Because of this characteristic of the Internet, the sense of personal responsibility for actions that become much more extreme and destructive than they would be if they were done in the real world is lost. Terminological distinction and division into real and virtual worlds can lead to the dangerous misconception that the virtual world is not real, that what happens in it does not create consequences.

Interactivity. The Internet allows interaction between its users. Interaction that is not limited by geographical boundaries. This characteristic enables like-minded people to mobilize and self-organize. It also allows users to create their own content that is placed on the Internet with their comments. Users themselves become distributors of content on the Internet by transmitting it.

Instantness. The Internet allows you to transfer information in an instant, with one click. Event information becomes available to billions of Internet users almost instantly when it occurs.

The decentralized structure prevents uniform application of regulations because the placement of content on servers located in other countries prevents the application of national regulations on them.

V. Criminal Law Sanctioning of Hate Speech on the Internet in the Republic of Serbia

Criminal Code of the Republic of Serbia[20] Article 317 prescribes the criminal offense of Instigating National, Racial and Religious Hatred and Intolerance. The

[18] Weber, R., Heinrich, U., (2012) *Anonymization*, Springer: London, p. 1.

[19] Ivanović, R. A., (2017) *The right to privacy and anonymity within the scope of freedom and security*, Conference proceedings: International Scientific Conference „Freedom, security: the right to privacy (ed. Zoran Pavlović), Provincial Protector of Citizens – Ombudsman and Institute for Criminological and Sociological Research, Novi Sad, p. 157.

[20] Criminal Code of Republic of Serbia *("OG", no. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019).*

protective object of this crime is the national, religious and racial equality of the citizens of the Republic of Serbia. Equality and unity of citizens in the Republic of Serbia is built on mutual respect and trust of all who live in it. This unity is preserved by constant nurturing, respect for all the characteristics of national, religious, racial, cultural and other values that characterize certain peoples and ethnic communities in the Republic of Serbia[21]. The Code prescribes the basic, qualified and special form of this criminal offense. Intent is the only form of guilt for this criminal offence.

The act of committing the basic form of this crime is set alternatively as instigating or exacerbating national, racial or religious hatred, or intolerance (paragraph 1). This further means that the act will exist both in a situation when there is no national, racial, religious hatred or intolerance between peoples or ethnic communities, so it is provoked in different ways (i.e. it creates, causes), and when it exists as latent, a state or as a state of lesser intensity, and then further inflamed[22]. Instigating implies the creation of hatred or intolerance on the mentioned grounds, in a situation where such phenomena did not exist, while exacerbating is an increase (deepening, i.e. expansion) of already existing hatred, intolerance and bigotry. Thus, Instigating or exacerbating national, racial or religious hatred or intolerance can be done in different ways and by different means: speech, inscription and other actions, which influences the creation or strengthening of certain feelings or attitudes towards a nation or ethnic community. In terms of the nature of this crime, hatred is understood as a negative feeling of high intensity which represents a very fertile ground for undertaking various excessive behaviors towards members of a certain people or ethnic community. When it comes to intolerance, it is understood in relation to hatred as a negative feeling of "milder" intensity (the so-called vestibule of feelings of hatred), which can also cause certain negative behaviors that may ultimately contribute to the commission of this crime. It should be noted here that in criminal law theory, the question arises, and there are conflicting opinions, as to whether contempt for a nation or ethnic community can be included in the notion of intolerance. Namely, unlike hatred and intolerance, contempt for a nation or ethnic community, is a negative attitude that is most often expressed in the form of ignoring and as such does not contain the potential to perform certain activities and actions against a nation or ethnic community, so that provoking and inciting contempt would still not be sufficient for the existence of this crime[23]. The passive subject in this criminal offense is represented by peoples, national minorities and ethnic communities living in the Republic of Serbia, and in connection with this, committing actions under this criminal offense against national or ethnic groups not living in the Republic of Serbia cannot constitute this criminal offense.

The criminal offence has been done by undertaking an activity with the aim of instigating or exacerbating hatred or intolerance, i.e. it is not necessary that these activities have led to the provocation or incitement of hatred or intolerance, or that a consequence has occurred. Therefore, the very consequence of this act is endangering the equality of citizens regardless of national, racial or religious affiliation. This form of criminal offence is punishable by imprisonment from six months to five years.

---

[21] Jović, M. (2011). *Criminal law – special part – script I* [*Krivično pravo – posebni deo – skripta I]*, Novi Pazar: International university of Novi Pazar, p. 240.

[22] Stojanović, Z. (2017). *Commentary on the Criminal Code: Sixth Amended Edition* [*Komentar Krivičnog zakonika: šesto izmenjeno i dopunjeno izdanje]*, Belgrade: Službeni glasnik, p. 936.

[23] *Ibid*.

The qualified form of this criminal offense exists when some of the legally established qualifying circumstances (paragraph 2) have been met, which indicate the commission of the basic form of the criminal offense: a) coercion, b) abuse, c) endangering security, d) exposing national, ethnic or religious symbols, e) damage to other people's property, f) desecration of monuments, memorials or graves[24]. For this form of criminal offence is punishable by one to eight years in prison.

The second qualified form will exist when the basic form or the first serious form of this criminal offense is committed by abuse of position or authority or if as a result of these acts there were riots, violence or other serious consequences for the common life of peoples, national minorities or ethnic groups living in Serbia (paragraph 3). For this form of offense, in the event that under the qualifying circumstances the offense referred to in paragraph 1 was committed, a sentence of imprisonment of one to eight years is prescribed, and if the offense referred to in paragraph 2 is committed, imprisonment of two to ten years.

In addition to the aforementioned criminal offense, Article 387 prescribes the criminal offense of Racial and Other Discrimination, paragraph 3 of which prescribes the conduct of this criminal offense, which is reflected in: a) spreading the idea of superiority of one race over another, b) propagating racial hatred or inciting racial discrimination. These are actually three forms of racist propaganda[25]. For this form of crime, a prison sentence of three months to three years was listed. Also, paragraph 4 of this criminal offense prescribes the act of committing this offense, the form of which is reflected in the dissemination or otherwise making publicly available texts, images or any other presentation of ideas or theories that advocate or incite hatred, discrimination or violence against any persons or groups of persons based on race, color, religion, nationality, ethnic origin or any other personal characteristic. This form of crime is punishable by imprisonment from three months to three years.

Article 174 prescribes the criminal offense of Infringement of Reputation Due to Racial, Religious, National or Other Affiliation, which stipulates that whoever publicly exposes a person or group for belonging to a certain race, skin color, religion, nationality, ethnic origin or any other personal characteristic shall be punished with a fine or imprisonment for up to one year.

Article 138 prescribes the criminal offense of Endangering Security, Article 1 of which stipulates that whoever endangers the security of a person by threatening to attack the life or body of that person or a person close to him, shall be punished by a fine or imprisonment for a term not exceeding one year. The act of committing the basic form of a criminal offense (paragraph 1) is the use of the threat to attack the life or body of a person or a person close to him. So, it is not ordinary, but the so-called a qualified threat, given that it is necessary to threaten a specific evil – an attack on the life or body of a passive subject or a person close to him. It can be threatened either only by an attack on life, or only by an attack on bodily integrity (therefore, the threat of inflicting light bodily injuries is sufficient), or cumulatively by an attack on life and

---

[24] Simonović, D. (2010) *Criminal offenses in Serbian legislation* [*Krivična dela u srpskoj legislativi]*, Belgrade: Službeni glasnik, p. 624.

[25] Ivanović. R. A., Ranđelović, D., (2019) *Sanctioning hate speech on the internet, according to the national regulations of the Republic of Serbia [Sankcionisanje govora mržnje nainternetu prema nacionalnoj regulative Republike Srbije],* Arhiv za pravne i društvene nauke vol. 1, no. 1, Law faculty Lukavica, p. 55.

an attack on the body. Under the notion of a close person in the sense of this incrimination should be considered blood relatives in the direct line, brother and sister, spouse and a person living in a permanent extramarital union, adoptive parent and adoptee, custodier and custodian. As the criminal offense of endangering security in Serbian criminal law is set as a consequential criminal offense, it is understood that the passive subject knows about the threat. Also, for the existence of the criminal offense is not affected by whether passive subject find out for threat directly from the perpetrator or from another person (so-called "indirect threat"). Paragraph 2 stipulates that whoever commits the act referred to in paragraph 1 of this Article against several persons, or if the act caused disturbance of citizens or other severe consequences, shall be punished by imprisonment for a term between three months and three years.

VI. Conclusion

Based on all the above-mentioned, we can conclude that in Serbia there is a relatively good criminal law framework for the suppression of hate speech that spreads through the electronic media. So-called online hate speech is covered by several acts prescribed in the Criminal Code. However, it can be said that the prescribed criminal offences are not fully in line with ECRI's General Policy Recommendation no. 7 on national legislation to combat racism and racial discrimination. This is because certain elements of these recommendations have still not been introduced into the criminal justice system of the Republic of Serbia. Namely, in the criminal offense of Instigating National, Racial and Religious Hatred and Intolerance from Article 317, paragraph 1 of the Criminal Code of Republic of Serbia, incitement to national, racial or religious hatred or intolerance among peoples or ethnic communities living in Serbia is prescribed as an act of committing the criminal offense. This legal wording does not meet the requirements contained in the ECRI Recommendations in several respects: no incitement to violence is mentioned, and skin color, language, citizenship, national origin, sexual orientation and gender identity are omitted as grounds for hatred or intolerance. In addition, despite the fact that incitement to hatred against individuals and groups living outside Serbia should be punishable, as it is pointed out in the paper, this provision only protects against incitement to hatred among “peoples or ethnic communities living in Serbia. Encouraging discrimination is punishable under the provisions of the criminal offense of Instigating National, Racial and Religious Hatred and Intolerance 387, paragraph 3 of the Criminal Code of Republic of Serbia, which also does not state all the prohibited reasons listed in ECRI Recommendations no. 7. Article 387, paragraph 3 of the Criminal Code of Republic of Serbia prohibits the spread of ideas about the superiority of one race over another. This is not fully in line with the ECRI Recommendation, which should also prescribe as a criminal offense and the expression of an ideology that belittles or defames a group of persons on the grounds listed. Also, in this crime, the presentation of ideas or theories that advocate or incite hatred, discrimination or violence against any person or group of persons based on race, color, religion, nationality, ethnic origin or any other personal characteristic. This is not fully in line with the ECRI Recommendation, as it does not cover the preparatory actions for the production or storage of such material, and because it only mentions incitement to hatred, but not other acts listed in the Recommendation.

In addition to the problem of insufficient compliance of domestic criminal legislation with ECRI Recommendations on General Policy no. 7 on national legislation to combat racism and racial discrimination, there is also a problem that is reflected in the fact that the general public, but also many staff in state bodies, as well as in the judicial system, are not sufficiently familiar or versed in dealing with such criminal offences. Namely, despite the relatively good legal framework that can regulate hate speech, judging by the very small number of processed and even initiated cases dealing with hate speech in Serbia, it is obvious that there are certain obstacles to its effective suppression.

Of course, it is ungrateful to talk about the efficiency of the police and criminal justice bodies, without the existence of official statistics on the number of reported, initiated and completed proceedings for such acts committed online, but based on reports from many NGOs we can conclude that the situation has not changed much from ECRI report from 2017. In this regard, there is still a need to raise staff capacity whose dealing with combating online hate speech, especially at the level of local police stations and prosecutors offices.

Based on all the above, we can conclude that there are two biggest challenges in terms of criminal repression in relation to hate speech in the electronic media in the Republic of Serbia. The first is reflected in the harmonization of the provisions of substantive criminal law with the ECRI Recommendations on General Policy no. 7 on national legislation to combat racism and racial discrimination and second, which is reflected in the need for constant education of police and prosecutors from the field of methodology of detecting and investigating such crimes, with special focus on local context of appearance of this negative phenomena.

References

1. Citron, D.K., Norton, H. (2011) *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*. Boston University Law Review, (4), p. 1435-1484;

2. Criminal Code of Republic of Serbia *("OG", no. 85/2005, 88/2005, 107/2005,72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019);*

3. ECRI report on Serbia (fifth monitoring cycle) (2017);

4. Gitlin, M. (2018) *When Is Free Speech Hate Speech?* New York: Greenhaven Publishing, 2018;

5. Ivanović, R.A. (2018) *Hate speech on internet through illegality to punishment.* Yearbook, no.1 – Human rights protection „From unlawfulness to legality“, Novi Sad: Provincial Protector of Citizens – Ombudsman and Institute of Criminological and Sociological Researcsh Belgrade, p. 405-417;

6. Ivanović, R. A., (2017) *The right to privacy and anonymity within the scope of freedom and security*, Conference proceedings: International Scientific Conference „Freedom, security: the right to privacy (ed. Zoran Pavlović), Provincial Protector of Citizens – Ombudsman and Institute for Criminological and Sociological Research, Novi Sad, p. 152-165;

7. Ivanović, R.A., Dečković, S., (2016) „The right to be forgotten as a fundamental principle of personal data protection in the digital age“ [*Pravo da budeš zaboravljen „(Right to be forgoten) kao temeljni princip zaštite ličnih podataka u digitalnoj eri]*, Conference proceedings – Volume 2 / Scientific conference with international participation: European integration: justice, freedom and security, Tara, 24-26. May 2016., Criminalistic-Police Academy, Hanns Seidel *Foundation*, Belgrade, p. 477-490;

8. Ivanović, R.A., Ranđelović, D., (2019) *Sanctioning hate speech on the internet, according to the national regulations of the Republic of Serbia [Sankcionisanje govora mržnje nainternetu prema nacionalnoj regulative Republike Srbije],* Arhiv za pravne i društvene nauke vol. 1, no. 1, Law faculty Lukavica, p. 49-61;

9. Ivanović, R.A., Ranđelović, D., Totić, M., (2019) *Hate speech in electronic media and on social networks [Govor mržnje u elektronskim medijima in a društvenim mrežama]*, Novi Pazar: Monitor;

10. Jović, M. (2011) Criminal *law – special part – script I [Krivično pravo – posebni deo – skripta I]*, Novi Pazar: International university of Novi Pazar;

11. Miladinović, A., (2013) *Facebook and crime [Fejsbuk i kriminalitet]*, Banja Luka: International Association of Criminalists;

12. Miladinović, S., (2015) *The growing importance of social media in a dynamic society [Rastući značaj socijalni medija u dinamičnom društvu]*, Conference proceedings: Statehood, democratization and a culture of peace, Faculty of Philosophy, University of Nis, Nis, p. 341-355;

13. Nikolić, P., (2018) *Internet hate speech in Serbia [Govor mržnje u internet komunikaciji u Srbiji]*, Doctoral Dissertation, Faculty of political sciences, Belgrade;

14. Simonović, D. (2010) *Criminal offenses in Serbian legislation [Krivična dela u srpskoj legislativi]*, Belgrade: Službeni glasnik;

15. Stojanović, Z. (2017) *Commentary on the Criminal Code: Sixth Amended Edition [Komentar Krivičnog zakonika: šesto izmenjeno i dopunjeno izdanje]*, Belgrade: Službeni glasnik, p. 936;

16. Tsesis, A., (2001) *Hate in Cyberspace: Regulating Hate Speech On the Internet*, San Diego Law Review 817/01, p. 817-874;

17. Weber, R., Heinrich, U., (2012) *Anonymization*, Springer: London.

The Impact of Misuse of Cryptocurrencies in Combating Money Laundering and Terrorist Financing

Dr. Zoran S. Pavlovic*
Nikola Paunovic*

Abstract

Cryptocurrencies are designed as a secure form of financial transaction via the Internet. However, the development of information and communication technology has created new space for their misuse in criminal purposes, especially in the area of money laundering and terrorist financing. Bearing in mind the complexity in conducting financial transactions via the Internet, the paper in the first part deals with most important legal challenges regarding the misuse of cryptocurrencies through money laundering and terrorist financing. Furthermore, in the second part of the paper, the most relevant crime detection methods are considered. Finally, the practical challenges at the level of the protection of financial transactions against their misuse in criminal purposes, have created a need for normative regulation of cryptocurrencies, which is why last part of this paper includes the analysis of the relevant legal framework in this area at international, European or national level. In the concluding remarks, the key recommendations for better legal protection of the cryptocurrency transactions are provided, since it is noticed that although the cryptocurrency financial transaction system has created opportunities for relatively secure financial operations in a digital environment, there is still space for improvement.

Keywords: *cryptocurrencies, money laundering, terrorist financing, detection, phenomenological forms, legal framework*

I. Introduction

Cryptocurrency is the latest topic of discussion in the financial world[1]. The term cryptocurrency refers to currencies, which rely upon cryptogenic algorithms to ensure network and transactional validity, and are distributed over the Internet, but are not issued by any centralized source. The first decentralized cryptocurrency created in 2009 was Bitcoin. Since then, numerous other cryptocurrencies have been created. All

* Professor of Criminal law, Chairman of the Department for Criminal Law, Faculty of Law University Business Academy Novi Sad, Ombudsman of the Autonomous Province of Vojvodina, Republic of Serbia. Contact: zoran.pav@hotmail.com.

* Research Assistant, Attaché at Ministry of Foreign Affairs, Republic of Serbia, Ph.D. Student, The University of Belgrade, Faculty of Law. Contact: dzoni925@gmail.com.

[1] K., Sontakke, A., Ghaisas, „Cryptocurrencies: A Developing Asset Class“, *International Journal of Business Insights & Transformation*, No. 2, 2017, 10.

of these currencies are distinguished from other virtual currencies such as e-Gold, Amazon, Tokens that are exchanged solely through the Internet, but are also issued and controlled from a centralized source[2]. Foremost type of decentralized cryptocurrencies is Bitcoin. The issuance of this currency is computer-programmed and limited, based on peer-to-peer technology and data encryption technology, which practically eliminates the possibility of double-spending, counterfeiting and similar abuses. At the same time, this is one of the main reasons why this currency is considered safe, even though there is no central issuing institution[3].

On the other side, cryptocurrencies such as bitcoin allows criminals to generate, transfer, launder, and steal illicit funds with anonymity. Accordingly, the first fact that disables as well as makes it difficult to detect the misuse of cryptocurrencies is variety of obliged entities included in the cryptocurrencies transactions. Thus, there is a *cryptocurrency user* which means a natural person or legal entity who obtains coins either to use them to purchase real or virtual goods or services, as well as to make peer-to-peer payments, or to hold them for investment purposes i.e. in a speculative manner. Second player is the so-called *cryptocurrency exchanger* which means the person or entity who offer exchange services to cryptocurrency users, usually under payment of a certain fee (i.e. a commission), allowing them to sell their coins for fiat currency or buy new coins with fiat currency. In this regard, it should be mentioned coin inventors and offerors. *Coin inventors* are individuals or organizations who have developed the technical foundations of a cryptocurrency and set the initial rules for its use. Moreover, there are *coin offerors* meaning individuals or organizations that offer coins to cryptocurrency users. Another player is *wallet provider* who provides cryptocurrency users digital wallets or e-wallets which are used for holding, storing and transferring coins. In this sense, there are two types of wallet providers. On the one hand, there is *hardware wallet provider* which provides cryptocurrency users with specific hardware solutions to privately store their cryptographic keys (e.g. Ledger Wallet). On the other side, exists *software wallet provider* which provides cryptocurrency users with software applications allowing them to access the network, send and receive coins and locally save their cryptographic keys. Furthermore, there is *custodian wallet providers* who takes online custody of a cryptocurrency user's cryptographic keys. Finally, there is *miner* who participates in validating transactions on the blockchain technology by solving a cryptographic puzzle[4].

Furthermore, the second thing that disables as well as makes it difficult the detection is reflected in fact that there are a lot of phenomenological forms in which perpetrators can misuse the cryptocurrency transactions. In other words, the misuse of cryptocurrency transactions may involve various forms of fraud, corruption crimes, as well as organized crimes[5]. However, taking into account the fact that all mentioned forms could not be analyzed in this article, the focus should be put on the most

---

[2] T. Bierer, „Hashing It Out: Problems And Solutions Concerning Cryptocurrency Used As Article 9 Collateral", *Journal Of Law, Technology & The Internet*, Vol. 7, 2016, 81.

[3] V. Dinić, „Bitcoin as a decentralized currency", *Bankarstvo* No. 2 2014, 135.

[4] R. Houben, A. Snyers, *Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion*, European Parliament, Brussels, 2018, 25-28.

[5] Z., Pavlović, „Institutional Capacities of the Republic of Serbia for Opposing Organized Criminal, Terrorism and Corruption", *Proceedings from scientific conference Financial Crime (Ed. J. Kostić, A. Stefanović)* Institute of Comparative Law and Institute of Criminological & Sociological Research, Zrenjanin, 2018, 58.

prevalent examples of criminal offenses by which it is manifested the misuse of the cryptocurrencies transactions. In that context, in the following lines it will be analyzed two criminal offences: money laundering and terrorist financing focusing the legal challenges regarding the qualification of alleged criminal activities.

Finally, the last thing that disables as well as makes it difficult the investigation of the cases concerning the misuse of cryptocurrencies is a lack of comprehensive normative regulation at international, European as well as national level. However, bearing in mind some achievements in this field in recent period in this article it will be considered the legal framework concerning the misuse of cryptocurrencies through money laundering and terrorist financing.

II. Legal Challenges Regarding the Misuse of Cryptocurrencies Through Money Laundering and Terrorist Financing

One of the major goals of every criminal investigation is to provide a proper qualification of alleged criminal activities to corresponding provisions of substantive criminal law, i.e. to define the elements of crime. Some new forms of criminal activity such as misuse of virtual currencies may call for the need to re-think and re-adjust currently available substantive criminal law options to real-life cases. Cybercrime aspects of the misuse of virtual currencies can manifest themselves in a multitude of ways. Standalone offences of cybercrime that are connected with virtual currencies, may not be, at a first glance, particularly relevant for the investigations focusing on laundering of crime proceeds. On the other side, reality shows that such offences which involve money-laundering by use of virtual currencies may be connected to criminal proceeds derived from forms of cybercrime such as computer-related identity offences, or computer-related fraud or forgery. Therefore, cybercrime offences may be deemed as predicate offences to money-laundering. In this case, investigations will be relying on cybercrime elements of crime to construct the offence of money-laundering. In this regard, it is important to understand the nature of specific cybercrime offences, including illegal access, system interference, data interference and misuse of devices[6]. Cybercrime offences concerning the misuse of cryptocurrencies dominantly represent the predicate offenses of money laundering and terrorist financing.

Money laundering is a process of concealing the illicit origin of money or assets acquired through crime[7]. Precisely, it means the process of conversion or transfer of illegally derived property, by concealing or disguising the illicit origin of that property, as well as eliminating traces of its acquisition, possession or use in order to integrate laundered proceeds into legal financial flows[8]. This crime has three essential stages. During the first stage, so-called *the investment* phase, the perpetrator breakdowns the

---

[6] United Nations Office on Drugs and Crime, Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, United Nations Office on Drugs and Crime, 2014, 78-81.

[7] N. Važić, *„Pranje Novca- Materijalni I Procesni Aspektu Međunarodnom I Domaćem Zakonodavstvu", Bilten sudske prakse Vrhovnog suda Srbije, No. 2, 2008, 121-122.* See also, L., Cvitanović. et.al., *Kazneno pravo-posebni dio*, Pravni fakultet Sveučilišta u Zagrebu, 2018, 381-389.

[8] Z. Pavlović, „Fighting money laundering and control of real estate transactions", *Proceedings from scientific conference Financial Crime and corruption (Ed. J. Kostić, A. Stefanović) Institute of Comparative Law and Institute of Criminological & Sociological Research*, Vršac, 2019, 79-81.

direct link between money and the illegal activity through it has acquired, introducing the illegally acquired money into the financial system most often in the form of some legal activity in which payment is made in cash. After the money had entered the legal financial system in the second *concealment* stage it is transferred from the account to which it is placed on other accounts in order to hide the link between money and criminal activity from which it originates. Finally, in the context of the last *integration* stage, laundered money appears as money from some legal activity[9].

Furthermore, terrorist financing means providing or collecting funds, by any means, directly or indirectly, with the intention that they be used, or in the knowledge that they are to be used, in full or in part, to commit, or to contribute to the commission of, either terrorist offences or offences related to terrorist activities. The link between money laundering and terrorist financing is reflected in the fact that the second one crime could be the associated predicate offence of the first one. Precisely, financing terrorism is a preparatory action to secure or collect funds or assets, intending to be used or knowing that they can be used, in whole or in part, for the commission of a terrorist act by a terrorist or by terrorist organizations[10].

Like money laundering, terrorist financing also has several stages. The first phase includes the acts of the *collection of funds* derived either from the clandestine legitimate business of the entity that is connected or even guided by terrorist organizations or individuals or from criminal activities. A significant source of these funds is donations by individuals who support the goals of terrorist organizations, as well as charities funds that raise funds and channel them to terrorist organizations. In the second phase, the collected funds are *stored* in various ways, including banks accounts opened by intermediaries, individuals or companies. The third phase is the *transfer of these funds* to terrorist organizations or individuals for operational use, through the use of fund transfer mechanisms, such as international electronic transfers between banks or money remittances, the use of charity organizations, alternative systems or money transfer networks, through couriers or smuggling over state borders[11].

The use of virtual currencies such as bitcoin for money-laundering or terrorist financing purposes is going to highlight distinction between objective elements of crime (an act in itself, as well as objects and tools of crime) and subjective (intent, purpose, complicity etc.). The use of virtual currency as objective elements of these criminal offences can be brought down to the following aspects. In terms of placement, when criminally obtained funds are introduced in the financial circulation, the procurement of the virtual currency through an exchanger may be used as a relevant element of crime. In terms of layering (the process in which criminally derived funds are legalized and their ownership and source is disguised), the essential features of virtual currency can be brought forward as an element of money-laundering offence where the prosecution will be willing to prove the case that the virtual currency was selected precisely for these features, in order to conceal the criminal origin of funds. In terms of integration (the process by which the property legalized through layering is re-introduced into the economy), the use of virtual currency may be one of the

---

[9] B., Sinanović, „Pranje novca", *Bilten sudske prakse Vrhovnog suda Srbije*, No. 2, 2011, 63-64.

[10] D., Bolta „Sprječavanje financiranja terorizma", *Policija i sigurnost*, No. 4, 2010, 420. D., Derenčinović, The Review Of The Harmonisation Of The Croatian Criminal Law With International Legal Documents On Combating Terrorism, *Hrvatski ljetopis za kazneno pravo i praksu*, No. 2, 2003, 959; D., Derenčinović, et. al., *Posebni dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, 2013, 32.

[11] N., Stanković *Terorizam i finansiranje terorizma*, Evropski Univerzitet Brčko, Brčko, 2014, 63-64.

elements, for instance if the laundered proceeds are re-invested into the virtual currency market, this may be an additional element of offence that can be used. On the other hand, in terms of proof of intent, as a subjective element of crime, which is an essential feature of money-laundering offences, focus should be on the following aspects of bitcoin. Firstly, anonymity and general lack of face-to-face interaction may be a valid proof of intent to commit offence related to illegal use of virtual currencies. Secondly, difficult traceability, including lack of paper/document trail can be specifically noted as element of intent. Finally, reliance on cryptography overall lack of regulation can be proven as a deliberate choice[12].

III. Crime Detection Methods of Money Laundering and Terrorist Financing Concerning the Misuse of Cryptocurrencies

In the context of the issue regarding virtual currencies, it should be noted that the development and widespread use of the Internet, personal computers, mobile devices, and related platforms and services, has had a vast impact on financial transactions[13]. The ability of new financial innovations to enable rapid cross-border payments presents elevated money laundering as well as terrorist financing risks. For that reason, financial institutions should identify the money laundering as well as terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products[14].

The anonymity of virtual currencies is considered the main risk in connection with the misuse of cryptocurrencies through money laundering or terrorist financing. In addition, international investigations, especially those involving advanced technology, can create challenges for law enforcement with respect to gathering evidence and information. The uncertain or non-existing legal instruments to trace, freeze and seize illicit virtual currencies that are related to illicit funds, can create an obstacle for law enforcement. Even though most virtual currencies leave a digital footprint, it might, in some cases, be challenging if not impossible to link the digital footprint to a physical person, especially if a person has extensive knowledge regarding covering key evidences[15]. While this means that law enforcement can utilize transaction monitoring technology, it again means many people using Bitcoin and cryptocurrencies already know that, and have driven the development of more anonymous currencies known as altcoins in response, or use techniques to further enhance their anonymity. This includes technology that masks identifying information on transaction ledgers, as well as the use of software like The Onion Router (Tor), known for its association with the Dark Web and online marketplaces like Silk Road, to anonymize a person's IP address[16].

---

[12] United Nations Office on Drugs and Crime, *op. cit.,* 85-86.

[13] T., Keatinge, D., Carlisle, F., Keen, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Parliament, Brussels, 2018, 21.

[14] Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation- The FATF Recommendations*, Paris, 2016, 17.

[15] Office for Prevention of Laundering of Proceeds Derived from Criminal Activity, *Virtual currencies – Risks of Money Laundering and Financing of Terrorism*, Riga, 2019, 8-9.

[16] How Law Enforcement Catches Cryptocurrency Crimes, https://www.iannfriedman.com/blog/2019/february/how-law-enforcement-catches-cryptocurrency-crime/, Accessed 09.05.2020.

However, the truth is that cryptocurrencies like Bitcoin are not entirely anonymous. Bitcoin transactions are visible to all who use the network. Through the use of monitoring technologies that track transaction ledgers, there can be significant visibility of activity. The fact that Bitcoin transactions leave a trace is not enough to deter criminals since law enforcers are not able to immediately identify the parties involved in a Bitcoin transaction, but they can spot and study patterns in the movement of cryptocurrency to profile and de-anonymize suspects[17]. For example, no matter what cryptocurrency or concealment technology is used, a suspected criminal will need to eventually exchange their digital currency for real money. This can allow law enforcement to implement two main things: to **de-anonymize suspects** by stripping down of anonymity as well as to **detect unusual patters** by identifying unusual or suspicious behavior[18]. Therefore, the abovementioned has shown that, although difficult, the investigation of the ownership of digital currencies is not impossible.

Moreover, concerning the detection of the misuse of cryptocurrencies, it should be noted that digital currency networks usually record transactions in a distributed public ledger, which can be subjected to analytical monitoring tools capable of highlighting suspect transactions[19]. In this regard, the application of blockchain technology is required since it allows to make a link between bitcoin transactions and individual users taking into account the fact that these ledgers are public or open sourced, meaning that anybody can access or maintain these ledgers[20]. However, in some cases even where bitcoin, keeps an open, transparent ledger of all transactions available as open-source information, linking a specific transaction to individual users may require additional indicators from other sources such as i.e. virtual currency administrator or virtual currency exchange company located in one country but holding accounts in other countries where it does not have a significant customer base or the volume and frequency of cash transactions conducted by the owner of a virtual currency administrator or virtual currency exchange company do not make economic sense[21].

IV. Legal Framework Concerning the Protection Against Misuse of Cryptocurrencies Through Money Laundering and Terrorist Financing

1. Money laundering and counter-terrorism financing risks concerning criptocurrencies at the international level

In that regard, in 2014, the FATF took up the specific topic of virtual currencies linking cryptocurrencies with the anonymity risks because customer identification features such as name and address are not attached to a user's Bitcoin address, and because the system has no central service provider that has oversight of transactions and can be held accountable. According to the FATF's assessment, suspicious activity

[17] How Law Enforcement Catches Cryptocurrency Criminals, https://thenextweb.com/hardfork/2019/12/26/bitcoin-cryptocurrency-criminals-law-enforcement/, Accessed 09.05.2020.

[18] How Law Enforcement Catches Cryptocurrency Crimes, https://www.iannfriedman.com/blog/2019/february/how-law-enforcement-catches-cryptocurrency-crime/, Accessed 09.05.2020.

[19] International Centre For Asset Recovery, *Tracing Illegal Assets – A Practitioner's Guide*, Basel 2015, 115.

[20] K., Sontakke, A., Ghaisas, *op. cit.,* 11.

[21] United Nations Office on Drugs and Crime, *op. cit.,* 148-149.

may therefore not only be more difficult to detect, but the source of payments may be blurred in contrast to traditional credit or debit cards, or payment systems such as PayPal and Western Union. Since the existence of the anonymity risks in relation to cryptocurrencies, there are increasing concerns about the use of virtual currencies by terrorist organizations, especially with evidence of websites connected to terrorist organizations seeking Bitcoin donations or providing instructions of how to purchase weapons using Bitcoin[22]. For that reason, financial institutions should identify the money laundering as well as terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products[23].

2. Money laundering and counter-terrorism financing risks concerning criptocurrencies at the EU level

Directive (EU) 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing constitutes the main EU legal instrument in the context of the detection and investigation misuse of virtual currencies through money laundering and terrorist financing[24]. This Directive introduces the definition of the following terms: 1) virtual currencies, 2) fiat currencies and 3) custodian wallet provider. The adoption of this Directive represents a significant step forward in the area of the protection of EU financial interests against misuse of cryptocurrencies for criminal purposes, bearing in mind the fact that providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers were under no Union obligation to identify suspicious activity, enabling terrorist groups to transfer money into the Union financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms. It was therefore essential to extend the scope of Directive (EU) 2015/849 so as to include providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers[25]. Namely, according to article 2 paragraph 1 of the amended Directive (EU) 2018/843 anti-money laundering and counter-terrorism financing framework has been extended so as to include providers of virtual as well as fiat currencies, and custodian wallet providers as the

---

[22] N., Paunović, Terrorist Financing As The Associated Predicate Offence Of Money Laundering In The Context Of The New Eu Criminal Law Framework For The Protection Of The Financial System, EU and Member States – Legal and Economic Issues, ed. (Duić, D, Petrašević, T., Novokmet, A.), Faculty of Law, Josip Juraj Strossmayer University of Osijek, Osijek, 2019, 670-671.

[23] Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation- The FATF Recommendations*, Paris, 2019, 15.

[24] 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, Official Journal of the European Union, L 141/73 of 5 June 2015, (hereinafter: Directive (EU) 2015/849).

[25] 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, Official Journal of the European Union, L 156/43 of 19 June 2018, (hereinafter: Directive (EU) 2018/843).

new obliged entities[26]. Precisely, amended Directive (EU) 2018/843 shall apply to the following obliged entities: a) providers engaged in exchange services between virtual currencies and fiat currencies; b) custodian wallet providers. For the purposes of this Directive, *virtual currencies* means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically. On the other side, *fiat currencies* mean coins and banknotes that are designated as legal tender and electronic money, of a country, accepted as a medium of exchange in the issuing country. Finally, *custodian wallet provider* means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies[27].

3. Money laundering and counter-terrorism financing risks concerning criptocurrencies at the national level

In the context of accession and negotiations process to EU, the Republic of Serbia has recently adopted the new framework concerning money laundering and terrorist financing, introducing new obliged entities of the importance against misuse of virtual currencies through money laundering and terrorist financing[28]. Thus, amended Serbian Law on money laundering and terrorist financing *in Article 4 point 17* recognizes as obliged entities *providers of virtual currencies* defining as persons providing the services of purchasing, selling or transferring virtual currencies or exchanging of such currencies for money or other property through internet platform, devices in physical form or otherwise, or which intermediate in the provision of these services[29]. However, it should be mentioned that Serbian law does not contain any further provision which defines virtual currencies. In that regard, the Serbian law should be amended, according to the meaning of virtual currencies referred to in Directive (EU) 2018/843, since it is incomprehensible that it recognized as obliged entities persons providing the services of purchasing, selling or transferring virtual currencies, but that did not include the definition of virtual currencies in the list of terms used in this Law. Moreover, comparing to the amended provisions of the Directive (EU) 2018/843 concerning virtual currencies, Serbian Law does not recognize the term of custodian wallet provider as an obliged entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies. To conclude, it should be noted that Serbian law is incompletely harmonized with EU *acquis* in this area and in the context of *de lege ferenda* amendments it would be necessary to include these solutions[30].

---

[26] L., Haffke, M., Fromberger, P., Zimmermann *Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and how to Address them*, 9-12. Available at SSRN: https://ssrn.com/abstract=3328064 or http://dx.doi.org/10.2139/ssrn.3328064 Accessed 09.05.2020.

[27] T., Keatinge, D., Carlisle, F., Keen, *op. cit.,* 50-53.

[28] Law on the prevention of money laundering and the financing of terrorism, Official Gazette of the Republic of Serbia, No. 113/17 and 91/2019.

[29] T., Lukić, „Borba Protiv Pranja Novca I Finansiranja Terorizma U Republici Srbiji", *Zbornik radova Pravnog fakulteta u Novom Sadu*, No. 2, 2010, 202.

[30] N., Paunović, *op. cit.,* 676.

V. Conclusion

The analysis of the impact of misuse of cryptocurrencies in combating money laundering and terrorist financing has shown that although use of virtual currencies has created opportunities for relatively secure financial operations in a digital environment, there is still space for improvement. Variety of obliged entities included in the cryptocurrencies transactions, a lot of phenomenological forms in which perpetrators can misuse virtual currencies, as well as a lack of comprehensive normative regulation at international, European and national level, had influence on some achievements in this field in recent period. Thus, EU framework is enriched with the Directive (EU) 2018/843 which introduced three new types of obliged entities of significance for the effective fight against misuse of virtual currencies through money laundering and terrorist financing. The main contribution of the Directive (EU) 2018/843 in the respect of the amended provisions is related to the fact that providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers are under Union obligation to identify suspicious activity concerning money laundering and terrorist financing.

Moreover, following the adopted framework at the EU level, the Republic of Serbia has recently adopted the new framework concerning money laundering and terrorist financing, introducing new obliged entities of the importance against misuse of virtual currencies through money laundering and terrorist financing. However, since incompletely harmonized with EU *acquis* in this area, national framework should be amended by introducing the definition of virtual and fiat currencies as well as custodian wallet provider.

To conclude, bearing in mind, emerging new trends, in particular regarding the way organized criminal groups conduct their operations regarding the misuse of virtual currencies through money laundering and terrorist financing it is extremely important to apply training programs, through appropriate channels of international cooperation and exchange of relevant information in the process of development of the skills and capabilities of persons and entities involved in the suppression of this type of crimes to enable them to be prepared for all methods and techniques used by criminals.

References

1. Bierer, T. „Hashing It Out: Problems And Solutions Concerning Cryptocurrency Used As Article 9 Collateral“, *Journal Of Law, Technology & The Internet*, Vol. 7, 2016.
2. Bolta D., „Sprječavanje financiranja terorizma“, *Policija i sigurnost*, No. 4, 2010.
3. Cvitanović. L., et.al., *Kazneno pravo- posebni dio*, Pravni fakultet Sveučilišta u Zagrebu, 2018.
4. Derenčinović, D., The Review Of The Harmonisation Of The Croatian Criminal Law With International Legal Documents On Combating Terrorism, *Hrvatski ljetopis za kazneno pravo i praksu*, No. 2, 2003.
5. Derenčinović, D., et. al., *Posebni dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, 2013.
6. Dinić, V. „Bitcoin as a decentralized currency“, *Bankarstvo* No. 2, 2014.
7. 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, Official Journal of the European Union, L 141/73 of 5 June 2015, (hereinafter: Directive (EU) 2015/849).

8. 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, Official Journal of the European Union, L 156/43 of 19 June 2018, (hereinafter: Directive (EU) 2018/843).

9. Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation- The FATF Recommendations*, Paris, 2016.

10. Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation- The FATF Recommendations*, Paris, 2019.

11. Haffke, L., Fromberger, M., Zimmermann P., *Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and how to Address them*, 9-12. Available at SSRN: https://ssrn.com/abstract=3328064, Accessed 09.05.2020.

12. Houben, R., Snyers, A. *Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion*, European Parliament, Brussels, 2018.

13. How Law Enforcement Catches Cryptocurrency Criminals,

14. https://thenextweb.com/hardfork/2019/12/26/bitcoin-cryptocurrency-criminals-law-enforcement/,Accessed 09.05.2020.

15. How Law Enforcement Catches Cryptocurrency Crimes,

16. https://www.iannfriedman.com/blog/2019/february/how-law-enforcement-catches-cryptocurrency-crime/, Accessed 09.05.2020.

17. International Centre For Asset Recovery, *Tracing Illegal Assets – A Practitioner's Guide*, Basel 2015.

18. Keatinge, T. Carlisle, D. Keen, F., *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Parliament, Brussels, 2018.

19. Law on the prevention of money laundering and the financing of terrorism, Official Gazette of the Republic of Serbia, No. 113/17 and 91/2019.

20. Lukić, T., „Borba Protiv Pranja Novca I Finansiranja Terorizma U Republici Srbiji", *Zbornik radova Pravnog fakulteta u Novom Sadu*, No. 2, 2010.

21. Office for Prevention of Laundering of Proceeds Derived from Criminal Activity, *Virtual currencies – Risks of Money Laundering and Financing of Terrorism*, Riga, 2019.

22. Paunović, N., Terrorist Financing As The Associated Predicate Offence Of Money Laundering In The Context Of The New Eu Criminal Law Framework For The Protection Of The Financial System, EU and Member States – Legal and Economic Issues, ed. (Duić, D, Petrašević, T., Novokmet, A.), Faculty of Law, Josip Juraj Strossmayer University of Osijek, Osijek, 2019.

23. Pavlović, Z. „ Institutional Capacities of the Republic of Serbia for Opposing Organized Criminal, Terrorism and Corruption ", *Proceedings from scientific conference Financial Crime (Ed. J. Kostić, A. Stefanović)* Institute of Comparative Law and Institute of Criminological & Sociological Research, Zrenjanin, 2018.

24. Pavlović, Z. „Fighting money laundering and control of real estate transactions*", Proceedings from scientific conference Financial Crime and corruption (Ed. J.Kostić, A.Stefanović)* Institute of Comparative Law and Institute of Criminological & Sociological Research, Vršac, 2019.

25. Sinanović, B., „Pranje novca*", Bilten sudske prakse Vrhovnog suda Srbije,* No. 2, 2011.

26. Sontakke, K., Ghaisas, A. „Cryptocurrencies: A Developing Asset Class“, *International Journal of Business Insights & Transformation*, No. 2, 2017.

27. Stanković N., *Terorizam i finansiranje terorizma*, Evropski Univerzitet Brčko, Brčko, 2014.

28. United Nations Office on Drugs and Crime, *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, United Nations Office on Drugs and Crime, 2014.

29. Važić, N. „Pranje Novca- Materijalni I Procesni Aspektu Međunarodnom I Domaćem Zakonodavstvu“*, Bilten sudske prakse Vrhovnog suda Srbije*, No. 2, 2008.

Streamlining the Fight Against Child Sex Offenders Trough EU Regulation of IP address

Dr. Silvia Signorato*

Abstract

The sexual abuse and the sexual exploitation of children, which includes child pornography, are very serious crimes which must be combated to the highest degree. At present, however, there are still too many legal obstacles in the prevention and the prosecution of these crimes. One of the main obstacles is the difficulty encountered in the collection of IP addresses, which often constitute very important evidence. Each Member State has its own legislation, and there are no clear EU indications regarding the retention period of IP addresses. In this article, a four-year retention period of the IP address is proposed in order to balance the needs of the protection of fundamental rights as well as those of investigative activity. This suggested retention period derives from the analysis of the regulations regarding data retention and the data on the investigative practices of all the Member States, taking into account the need to protect fundamental rights.

Keywords: *IP address, data retention, sexual abuse and sexual exploitation of children, child pornography, cyber investigations*

I. Introduction

This article is aimed at evaluating the significance of IP addresses in the fight against child sex offenders in the European Union. This topic is analysed with regard to data retention laws[1].

In Europe, the proportion of children sexually assaulted during their childhood is between 10% and 20%[2]. The sexual abuse and the sexual exploitation of children, including child pornography, constitute serious violations of fundamental rights. In

* PhD, Assistant Professor in Criminal Procedure – University of Padua (Italy), Lecturer in Criminal Procedure – University of Innsbruck (Austria). E-mail: silvia.signorato@unipd.it.

[1] Data retention is the storage activity of 'traffic data' for a given period (which is called 'retention time') for the purposes of the prevention, investigation, detection or prosecution of criminal offences. Traffic data "means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service" (see article 1, letter d of the Convention on Cybercrime – Council of Europe, 2001). Whenever personal data is stored, there is a violation of the Right to protection of personal data. This also occurs in cases where the processing of personal data takes place by European Agencies or a prosecution office, e.g. the European Public Prosecutor's Office (EPPO). See in this respect P. De Hert, V. Papakonstantinou (2019). Data Protection and the EPPO. *New Journal of European Criminal Law*, v. 10, p. 34-43.

[2] See https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/child-sexual-abuse_en.

particular, they are violations of the rights of children to the protection and the care necessary for their well-being, as provided for by United Nations Convention on the Rights of the Child[3]. Moreover, Article 34 of that Convention provides that "States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse".

These crimes are particularly cruel and cause huge suffering to the victims. Unfortunately, this phenomenon continues to grow, mainly due to four factors: the Internet (in particular, the Darknet)[4]; the ease of international travel aimed at child sex tourism; business related to this kind of crime; and the lack of an adequate legal framework. These factors are described in detail.

1. The Internet facilitates the commission of serious crimes such as the sexual abuse and the sexual exploitation of children, including child pornography[5]. This is because the Internet makes these actions easier: grooming[6]; solicitation of children for sexual purposes; production, distribution and use of child pornography; arranging and booking trips aimed at child sex tourism (CST); incitement and aiding such crimes. Furthermore, the use of anonymisation programs or of the Darknet[7], which makes investigations more difficult, helps to guarantee the anonymity of those who commit crimes.

2. The existence of organised international travel aimed at child sex tourism is extremely worrying. This phenomenon started in the second half of the 20th century[8] and shows no sign of abating. On the contrary, it is increasingly organized and difficult to combat.

---

[3] See Preamble of such a Convention. See also Article 24 Charter of Fundamental Rights of the European Union. In addition, see Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography of 2000, the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Abuse of 2007 (a.k.a., the Lanzarote Convention), and the Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography.

[4] According to Meter (2018). Annual Report. Pedophilia and child pornography, p. 17, these different types of paedophiles which use the Internet can be identified: Closet collector; Isolated collector; Cottage collector; Commercial collector; Pedo-crime (organized).

[5] See P. Torretta, C. Bonucchi. M. Cotroneo, E. D'Amato (2016). White paper on child sex offenders. Treatment and diagnostic profile of online sex offenders to the detriment of minors for the prevention of and fight against this phenomenon (CSE Project HOME/2012/ISEC/AG/4000004373, Co-funded by Prevention of and Fight against Crime Programme of the European Union), p. 10-25. A system for automatic recognition of child grooming in online chat conversations is proposed by P. Anderson, Z. Zuo, L. Yang, Y. Qu, 2019. Intelligent Online Grooming Detection System Using AI Technologies. 2019. Paper presented at 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, United States.

[6] Grooming is the enticement of children or the solicitation of children for sexual purposes. Grooming is the process by which an adult befriends a child in order to commit sexual abuse. See A.-M. McAlinden, (2012). 'Grooming' and the Sexual Abuse of Children: Institutional, Internet and Familial Dimensions, 1st ed. Oxford: Oxford University Press.; S. Ost, (2009). Child pornography and sexual grooming: legal and societal responses. Cambridge: Cambridge University press, p. XIII-273.

[7] The Darknet is an application and protocol layer riding on the Internet where the user navigates in a completely anonymous way. See e.g. J. Pace (2017). Exchange Relations on the Dark Web. *Critical Studies in Media Communication*, 34(1), p. 1-13.

[8] See Commission of the European Communities, 1996: 2, which states that "The sexual exploitation of children in tourism is perpetrated not only by paedophiles, who constitute the hard core of child sex abusers, but also by preferential abusers and occasional abusers. (…) However, the distinction should in no way disguise the unacceptable nature of any such practices".

3. The increase related to sexual abuse and the sexual exploitation of children is enormous and constitutes a real business activity on an international scale. For this reason, such cruel crimes have become attractive even for organized crime networks which have an increasing role in their commission.

4. Finally, the legal framework does not seem entirely adequate and its improvement appears to be urgently needed. The sexual abuse and the sexual exploitation of children are increasingly transnational crimes. They can only be prosecuted on the basis of fast and effective investigative cooperation between states[9]. At the European level, some acts aimed at improving investigative cooperation were issued. Among these acts, there is the one that established the European Investigation Order (EIO)[10]. However, investigators still tend to use this tool too little[11]. Furthermore, although the EIO speeds up the evidence collection time, the collection of e-evidence is still generally too slow. Since an e-evidence is characterised by potential instability and can therefore quickly undergo alteration, degradation, or loss[12], its collection must be timely[13].

The sexual abuse and the sexual exploitation of children, including child pornography, are very serious crimes, which must be combated to the highest degree. Therefore, it is necessary and urgent to remove the legal obstacles to the prosecution of these crimes. In particular, the diversity of the regulations of the various Member States regarding IP Address retention is a significant legal obstacle. This problem is examined in this article, where a possible solution is also suggested.

II. The IP Address: Basic Technical Knowledge

The term IP address means Internet Protocol address. An IP address is a numerical label connected to a computer network that uses the Internet Protocol for

---

[9] For example, in Operation Tantalio, Interpol, Europol, and Law Enforcement Agencies from fifteen countries in Central America, South America, and Europe, cooperated in the investigation of child sexual abuse material distributed via WhatsApp.

[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. A discussion on EIO can be found in L. Bachmaier Winter (2015). Towards the Transposition of Directive 2014/41 regarding the European Investigation Order in Criminal Matters. *Eucrim*, p. 47-60; M. Daniele (2015). Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles. *New Journal of European Criminal Law*, p. 179-194; and A. Mangiaracina (2014). A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order. *Utrecht Law Review*, p. 113-133.

[11] There are cases where the Judiciary prefers not to request evidence by means of EIO. This is due to several reasons. For example, some judiciaries do not know how to request an EIO; in some cases the judiciary finds the procedure to obtain the EIO too difficult or the preliminary authorization by his/her head is required and this becomes an obstacle.

[12] See S. Signorato, S. (2017). Types and features of cyber investigations in a globalized world. Paşca, V., Ciopec, F. (Eds), *Probleme actuale în dreptul penal european*: Universul Juridic, p. 60.

[13] At present, there are two proposals for a Community act aimed at improving the speed and effectiveness of e-evidence collection. The first one is the 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 – 2018/0108 (COD). The second one is the 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 – 2018/0107 (COD).

communication. It serves two main functions: host or network interface identification and location addressing. Therefore, on the one hand it enables devices to communicate with each other, and on the other, it is a sort of fingerprint of the device. Each device connected to the network has a specific IP address, different from the one used by all other devices[14].

There are currently two versions of the IP address: IPv4 and IPv6. An IPv4 is a string of four dot-separated numbers between 0 and 255, therefore encoded with 8 bits, for a total of 32 bits[15]. A typical IPv4 address is 192.0.2.53. Version 4 allows the definition of just over four billion unique IP addresses, which are now largely assigned, leading to the risk of their exhaustion[16]. To overcome this problem, version 6, i.e. IPv6, was introduced. An IPv6 is a string of eight colon-separated groups of 4-bit hexadecimal digits, for a total of 128 bits. An example of IPv6 is 2001:0db8::53[17].

Every time a user sends an email, visits a site, participates in a video conference, or performs any online operation, its IP address can be stored by the server[18]. This happens, of course, also in the case of automatic access to the Internet by a device.

The IP address retention is very important for investigation purposes. For example, in the case of a child pornography website, the identification and prosecution of its users is critically based on the knowledge of the IP addresses of those who have connected to it[19]. This is because the IP address allows the unique identification of the device from which the connection to the network occurred.

---

[14] It should be noted that the development of the Internet of Things leads to a significant increase in the number of devices that are connected to the network. See G. Fortino, P. Trunfio (2014). Internet of Things Based on Smart Objects. Berlino: Springer 2014.

[15] ICANN (2011). Beginner's Guide to Internet Protocol (IP) Addresses, p. 5.

[16] ICANN (2011). Beginner's Guide to Internet Protocol (IP) Addresses, p. 5.

[17] Two colons side by side in an IPv6 address means that all the segments between them contain only zeros. If the two colon notation is not used, the address shown in the example becomes 001:0db8:0000:0000:0000:0000:0000:0053.

[18] In several European states a service and content provider within the internet industry can contact, on a voluntary basis, an institutional contact point in order to report either the existence of child sexual abuse material or information relating to child sexual abuse related to its services. The complete list is shown here state by state: Austria: Austrian C4-Cybercrime Competence Centre; Belgium: Central Traficking in Human Beings, Belgian Federal Police; Bulgaria: Intellectual property and illegal content on Internet; Cyprus: Office for Combating Cyber Crime; Czech Republic: Police Presidium, Bureau of Criminal Investigation Service, Cybercrime Department; Germany: German Federal Criminal Police Office (Bundeskriminalamt); Denmark: Danish National Cyber Crime Centre; Estonia: Police and Boarder Guard Board, Intelligence Analysis Division; Spain: Bureau de Investigacion Technologica, Policia Judicial; Finland: Cyber Intelligence Unit, National Bureau of Information; France: O.C.L.C.T.I.C; Greece: Hellenic Cyber Crime Unit; Hungary: National Bureau of Investigation High-Tech Crime Unit; Ireland: Paedophile Investigation Unit, Domestic Violence and Sexual Assault Investigation Unit, National Bureau of Criminal Investigation; Italy: Postal and Communication Police Agency – National Centre for Combating Child-pornography Online – CNCPO; Malta: Malta Police Cyber Crime Unit; Netherlands: Dutch Child Exploitation Team of the National Police of the Netherlands; Poland: Department for Trafficking in Human Beings; Romania: General Inspectorate of the Romanian Police – Countering Organized Criminality Directorate – Countering Computer Crimes Service; Sweden: National Bureau of Investigation; Slovenia: General Police Directorate, Criminal Police Directorate; Slovakia: Slovak Safer Internet Centre; United Kingdom: NCAT Bureau, United Kingdom National Crime Agency; Norway: KRIPOS, National Criminal Investigation Service; Switzerland: CYCO, Federal Criminal Police. Further details about these contact points, in particular their email and phone, can be found in: https://www.europol.europa.eu/report-a-crime/industry-reporting-of-child-sexual-abuse-material.

[19] See J. Davidson (1988). An Introduction to TCP/IP, New York: Springer.

It should be noted that the IP-based identification of the device does not necessarily mean that of those who used it for criminal purposes. This is because the device may be available to several users or may have been stolen, or a hacker may have performed IP spoofing[20]. A further investigation is therefore necessary to identify the offender. In any case, the IP address is always a very important evidence.

III. Retention of IP Addresses and Fundamental Rights

As mentioned above, an IP address can constitute really important evidence. For this reason, the rules of the Member States generally require that the servers store the IP addresses for a specific period of time for the purposes of the prevention, investigation, detection or prosecution of criminal offences or else for the execution of criminal penalties[21].

However, this poses problems with respect to fundamental rights, with particular reference to privacy[22] and the freedom of expression[23]. The fact of being able to

[20] IP address spoofing, or simply IP spoofing, is an attacking technique where the *hacker creates* a false source IP address for the purpose of impersonating another computing system. See M.T. Banday, R.A. Mathangi (2015). Control of IP Address Spoofing – A Comparative Study of IPv4 and IPv6 Networks. Mohammad Tariq Banday (Ed.), Proceedings of 2015 International Conference on Advances in Computers, Communication, and Electronic Engineering, Hazratbal, Srinagar: University of Kashmir, p. 344-351.

[21] Regarding the different problem of the possibility for Computer Security Incident Response Team to keep the IP Address see European Union Agency for Network and Information Security (ENISA) (November 2018), Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary, p. 21-22: "Under Article 6.1 a) of the GDPR, the processing of personal data, including IP addresses, is permitted for a specific, necessary and proportionate purpose (purpose of legitimate interest pursued by the CSIRTs, as specified on Article 6.1 f) if the data subject (the person concerned, the person whose personal data are processed) gives consent. In the event of an IT incident, there is no consent from the data subject (e.g. IP address holder) who caused the incident. However, according to the GDPR (see Article 13.3) and to Recital 49 it can be considered that the personal information, under certain circumstances, can be processed by the CSIRT even without consent. Recital 49 indeed provides that 'The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), CSIRTs, by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping "denial of service" [DoS] attacks and damage to computer and electronic communication systems."

[22] The Right to privacy was initially conceived as the right to be let alone (see S.D. Warren, L.D. Brandeis (1890). The Right to Privacy. *Harvard Law Review*, 4, p. 193). Subsequently, this right was extended to include the right to have control over access to one's personal information. In essence, a dynamic meaning of privacy was added to the static one. The European Convention on Human Rights provides in Article 8 (Right to respect for private and family life) the protection for both the meanings of privacy. Instead, the Charter of Fundamental Rights of the European Union separately protects private and family life (Article 7) and personal data (Article 8).

[23] See Court of Justice, 8th April 2014, Digital Rights Ireland and Others, Joined Cases C-293/12 and C-59412, paragraph 28. Moreover, see Court of Justice, 21 December 2016 (requests for a

identify those who placed certain information on the Internet, apart from being a violation of people's privacy, can give rise to restrictions on the freedom of expression. In addition, the fact that data storage creates costs for Internet Service Providers should be taken into account.

The preservation of IP addresses is important for both prosecution and defence purposes. As mentioned above, it serves to prevent and combat crimes. Furthermore, it can also be useful for defence purposes since an IP address could also be used by a suspect to prove his innocence.

The need to balance various rights makes it difficult to identify the ideal data storage time of the IP address in accordance with the principle of proportionality. The risk is to lean towards extremes. On the one hand, the exclusive protection of security could lead to the threat of a totalitarian drift. On the other hand, the exclusive attention to privacy could prevent or seriously hinder the prosecution of serious crimes such as the sexual abuse and the sexual exploitation of children.

At the European level there are no directives or regulations establishing a well-defined retention period for the IP addresses. Article 6 of Directive 2006/24/EC generically provided that the period of retention should be "not less than six months and not more than two years from the date of the communication". However, the Court of Justice, 8 April 2014, Digital Rights Ireland and Others, declared Directive 2006/24/EC invalid due to the violation of the principle of proportionality. This important judgement contributed to creating greater sensitivity at the European level towards the respect of fundamental rights, in particular the right to the Protection of personal data.

However, this judgement of the Court of Justice also caused an unforeseen and unwanted consequence, due to the fact that some Member States introduced or interpreted the regulations on data retention too restrictively[24]. The corresponding national regulations were such as to hinder or even prevent the right of defence or, more often, investigative activities. In particular, in some cases, the investigations aimed at combating the sexual abuse and/or the sexual exploitation of children were hindered by unavailability of the necessary IP addresses. This is because the states to which these IP address were requested had already deleted these data due to the too short retention period provided by their own acts. Section 113b German Telecommunications Act is a significant example, worthy of being described in detail. It requires data to be retained for only ten weeks[25]. Such a short retention period has an admirable purpose, namely the protection to the highest degree of fundamental rights, including the right to the protection of personal data. However, European investigative practice has shown that this law causes the violation of other fundamental rights such as child protection, due to the hindering of the prosecution of crimes.

---

preliminary ruling from the Kammarrätten i Stockholm and the Court of Appeal (England & Wales) (Civil Division) — Sweden, United Kingdom) – Tele2 Sverige AB v Post- och telestyrelsen (C-203/15), Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15), joined Cases C-203/15 and C-698/15.

[24] In reference to the first amendments to national data retention laws after the Digital Rights Ireland judgment, see Council of the European Union (6 November 2017), Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15 – Report; European Union Agency for Fundamental Rights (FRA) (2017), Fundamental Rights Report 2017, chapter 6 Information society, privacy and data protection, p. 155-172.

[25] In case of location data the retention period is even shorter, i.e. four weeks.

The experience gained thanks to this German law should be the starting point for serious reflection on the subject. It is necessary to take into account the fact that data retention is an extremely sensitive issue and that privacy is a right to be protected to the highest degree. However, this right must be balanced with security and other relevant rights, such as the right of defence.

IV. Searching for a Balance Between Retention Period of IP Address and Fundamental Rights

The Treaty of Lisbon[26] enhances the protection of the right of privacy in many respects. First of all, Article 6 of said treaty provides that the Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union (CFR), which assumes the same legal value as the Treaties. In particular, with the Treaty of Lisbon also Article 7 CFR (Respect for private and family life) and Article 8 CFR (Protection of personal data) reached a stronger meaning. Moreover, the protection of data is dealt in Article 16 of the Treaty on the Functioning of the European Union (TFEU), which provides that "Everyone has the right to the protection of personal data concerning them".

The directive on data protection in the police and justice sectors[27] emphasises the inescapable significance of the protection of personal data in these sectors as well. Moreover, such a directive states that an adequate regulation of the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties contributes to the accomplishment of an area of freedom, security and justice[28]. The fact that the directive seeks to ensure some protection of personal data in the case of data processing for the purpose of prevention and repression of crimes appears appreciable. This is because it is possible to state that "The biggest threat to individual freedom and dignity stems from the excessive informational power of certain companies, or controllers, and the wider, incompressible ecosystem of trackers, profilers and targeters that are able to gather and use this information"[29].

In light of the above, the basic problem is to answer the question: What could be an IP address retention period that guarantees both the protection of personal data as well as that of other needs, in particular, that of security?

In order to answer the question, the author of this article conducted two analyses at the European level.

---

[26] See E. De Busser (2014). European initiatives concerning the use of IT in criminal procedure and data protection. *International Review of Penal Law,* p. 115-116.

[27] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. See S. Signorato, S. (2017). The contribution of Directive UE 2016/680 in the implementation of an area of freedom, security and Justice: potential and challenges. International Criminal Law Association (Ed.), *Principi vladavine prava,* Tara: Intermex, p. 417-428.

[28] Directive (EU) 2016/680, recital 2.

[29] European Data Protection Supervisor (2018). Annual Report 2018, p. 8.

a) First of all, the regulation on the retention of IP addresses of each Member State was examined. This analysis showed that retention periods are extremely different between countries and are often too short (e.g. six, twelve, eighteen months). This fact causes many difficulties in those cases where it is necessary to carry out the collection of the IP address in states different from the one carrying out the investigations. It often happens that the State that receives the IP address request has already deleted it on the basis of its own data retention rules.

b) Moreover, the period of time which typically passed between the commission of the crime and the request for IP addresses by investigators was examined. This study showed that IP addresses are often required even after some years from the commission of the crime.

On the basis of this research it emerged that the retention period of the IP address compatible with investigative needs is somewhere in the range between six and ten years. The useful standard for data retention determined by the analysis is very long and, therefore, could cause a significant violation of the right to the protection of personal data.

For this reason, a further analysis was carried out. In particular, it was assessed whether the need to request the IP address after many years following the commission of the crime was related to the crime itself or due to other factors. In this way, it was discovered that, in many cases, such dilated times were due to investigative dysfunctions (e.g. reduced investigator staff, difficulties in coordination between investigators, difficulties in investigative cooperation between States, inadequate legal framework, lack of funds to meet investigative needs) However, it is important to emphasize that the retention period cannot be adapted to investigative dysfunctions. Instead, the investigative dysfunctions must be eliminated or at least reduced, taking into account the laws on data retention.

On the basis of the results of these analyses, it is proposed that the retention period of IP addresses be at least three years or, preferably, four years. This standard seems able to balance the various fundamental rights without compromising the outcome of possible future investigations.

V. Conclusions

The sexual abuse and the sexual exploitation of children, which include child pornography, are very serious crimes, often transnational, that cause enormous suffering to the victims. Furthermore, they also violate the United Nations Convention on the Rights of the Child. This Convention provides, on the one hand, the rights of children to the protection and care necessary for their well-being and, on the other, that the States Parties take the necessary measures to protect children from all forms of sexual exploitation and sexual abuse. These crimes must therefore be combated to the highest degree. At present, however, the effectiveness of investigations is often weakened by certain legal obstacles.

Since these crimes generally cross the borders of single States, as well as those of the European Union, their effective prevention and combat require international rules. In the absence of such rules, it is necessary at least to introduce as soon as possible a legal act of the European Union that allows a rapid collection of evidence between Member States, adequate to guarantee the integrity of evidence and its admissibility in

a Criminal Trial. In addition, new rules on IP address retention are urgently required. This is because the IP address can be a very important evidence in combating these crimes.

However, the drafting of a new regulation regarding IP addresses is complex because the corresponding retention of data, which is necessary for the prevention and the fight against crime, causes a violation of fundamental rights. In order to establish a retention period that respects both investigative needs and fundamental rights, the law on data retention and the investigative practices of each Member State were analysed. The ideal benchmark seems to be reached with a retention period of IP addresses of three or, better still, four years.

Finally, it would be appropriate the introduction of a legal act of the EU aimed at regulating not only IP address retention, but also data retention in general, providing a specific retention period for each type of data. This is because an effective fight against crime can only be achieved through the existence of adequate legislation, common to all Member States, on data retention. For this reason, the European legislature should intervene in this matter with a regulation and not with a directive[30].

References

1. Anderson, P.; Zuo, Z.; Yang, L.; Qu, Y. (2019). An Intelligent Online Grooming Detection System Using AI Technologies. Paper presented at 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, United States.

2. Bachmaier Winter, L. (2015). Towards the transposition of directive 2014/41 regarding the european investigation order in Criminal Matters. *Eucrim*, p. 47-60.

3. Banday M.T; Mathangi R.A. (2015). Control of IP Address Spoofing – A Comparative Study of IPv4 and IPv6 Networks. Mohammad Tariq Banday (Ed.), *Proceedings of 2015 International Conference on Advances in Computers, Communication, and Electronic Engineering,* Hazratbal, Srinagar: University of Kashmir, p. 344-351.

4. Council of the European Union (6 November 2017), Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15 – Report.

5. Daniele, M. (2015). Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles. *New Journal of European Criminal Law*, p. 179-194.

6. Davidson, J. (1988). An Introduction to TCP/IP, New York: Springer.

7. De Busser, E. (2014). European initiatives concerning the use of IT in criminal procedure and data protection. *International Review of Penal Law*, pp. 115-116.

8. De Hert P., Papakonstantinou V. (2019). Data Protection and the EPPO. *New Journal of European Criminal Law,* v. 10, p. 34-43.

9. European Data Protection Supervisor (2018). Annual Report 2018, p. 8

10. European Union Agency for Fundamental Rights (FRA) (2017). Fundamental Rights Report 2017, chapter 6 Information society, privacy and data protection, p. 155 – 172.

11. European Union Agency for Network and Information Security (ENISA) (November 2018). Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary, p. 21-22.

[30] A directive is a legislative act that sets out a goal that all EU countries must achieve. A regulation is a binding legislative act. See R.E. Kostoris (2018). European Law and Criminal Justice. R.E. Kostoris (Ed.), *Handbook of European Criminal Procedure*. Berlin: Springer, p. 25 ff.

12. Fortino, G.; Trunfio P. (2014). Internet of Things Based on Smart Objects. Berlino: Springer 2014.

13. ICANN (2011). Beginner's Guide to Internet Protocol (IP) Addresses, p. 5.

14. Kostoris, R.E. (2018). European Law and Criminal Justice. Kostoris, R.E. (Ed.), *Handbook of European Criminal Procedure.* Berlin: Springer, p. 25 ff.

15. Mangiaracina A. (2014). A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order. *Utrecht Law Review,* p. 113-133.

16. McAlinden, A.-M. (2012). 'Grooming' and the Sexual Abuse of Children: Institutional, Internet and Familial Dimensions, 1st ed. Oxford: Oxford University Press.

17. Ost, S. (2009). Child pornography and sexual grooming: legal and societal responses. Cambridge: Cambridge University press.

18. Meter (2018). Annual Report. Pedophilia and child pornography, p. 17.

19. Pace, J. (2017). Exchange Relations on the Dark Web. *Critical Studies in Media Communication*, 34(1), p. 1-13.

20. Signorato, S. (2017). Types and features of cyber investigations in a globalized world. Paşca, V., Ciopec, F. (Eds), *Probleme actuale în dreptul penal european*: Universul Juricidic, p. 60.

21. Signorato, S. (2017). The contribution of Directive UE 2016/680 in the implementation of an area of freedom, security and Justice: potential and challenges. International Criminal Law Association (Ed.), *Principi vladavine prava*, Tara: Intermex, p. 417-428.

22. Torretta P.; Bonucchi C.; Cotroneo M.; D'Amato E. (2016) White paper on child sex offenders. Treatment and diagnostic profile of online sex offenders to the detriment of minors for the prevention of and fight against this phenomenon (CSE Project HOME/2012/ISEC/AG/4000004373, Co-funded by Prevention of and Fight against Crime Programme of the European Union), p. 10-25.

23. Warren, S.D., Brandeis L.D. (1890). The Right to Privacy. Harvard Law Review, 4, p. 193.

Videoconference in Criminal Proceedings – Between Ideal and Current Social Reality

***Dr. Matei-Ciprian Graur*[1]**

Abstract

The need to implement technology in the criminal process has become increasingly acute with the change in the paradigm in which human interaction is being thought at this time. The current social order, given the need for physical separation imposed by the medical reality, has prompted judicial bodies to adopt modern measures to prosecute criminal proceedings.

Also, the fast pace at which the contemporary world is turning into an "information" one marks all areas of society. In this context, judicial proceedings cannot stay away from technology involvement. Although justice is done by the people and for the people, the use of technology is a reality of today, having the advantages of reducing the costs of judicial proceedings, speeding up, but also making it easier for the individual to have access to them. As a result, new information technologies determine the adaptation of the working methods of the "actors" of justice, but also mark a reconsideration of the ways of exercising the rights of parties involved in judicial proceedings[2]*.*

Also, the current social context, which often involves the need for a physical distance, has prompted judicial bodies to "modernise" the criminal process.

An interesting and topical aspect concerns the use of videoconferencing in criminal proceedings. Videoconferencing has the advantage of facilitating distance hearings, thus avoiding unnecessary travel, reducing the costs of criminal proceedings, shortening deadlines and avoiding security issues. For these reasons, the use of videoconferencing has spread across the different justice systems in both domestic and international judicial cooperation procedures[3]*.*

Keywords: *videconference, criminal proceedings, fair trial, physical distance, right of defence*

I. National Controversy

Taking into account the current social situation, especially the risk of infection with the new coronavirus, both the Timişoara Court and many courts in the country have resorted to the trial of cases with detainees by videconference.

---

[1] Center of Research in Criminal Sciences, West University Timisoara, Romania. Contact: matei.graur88@e-uvt.ro.

[2] Daniela Dediu, *Videconference in national criminal proceedings and international judicial cooperation in criminal matters. Right to a fair trial*, Pro Lege Magazine, 2018, www.revistaprolege.ro, 28.05.2020.

[3] *Ibidem.*

During the state of emergency there were provisions derogating from the rules laid down in the Code of Criminal Procedure at that time, an example of this being the lack of the consent of the person detained to be heard by videconference.

Once the state of emergency ceases, given that there are no provisions derogating from the provisions of the Code of Criminal Procedure (except for changes to the consent of the detained person[4]), they are fully applicable to such situations.

Thus, the concrete issue relates to the presence of the lawyer – either in the courtroom or in the detention place.

According to Art. 106 par. 2 Code of Criminal Procedure, the person in detention may be heard at the place of detention by videconference, in exceptional cases and if the judicial body considers that it does not affect the proper conduct of the trial or the rights and interests of the parties. According to Art. 106 par. 3 Code criminal procedure, in the case provided under par. 2, if the person heard is in any of the situations provided under Art. 90, the hearing may take place only in the presence of the lawyer at the place of detention.

The legislator's will to guarantee the right of defence, including the need to give a concrete possibility to the person in possession of direct contact with the lawyer.

At the same time, the modern means of conducting the criminal process that we are obliged to resort to in the current social context are at odds with those provisions.

It is obvious that in the context of the trial of a large number of cases with persons detained (cases for parole, appeals to execution, pre-trial arrest checks, complaints against the conclusion of the supervisory judge, applications for merger of sentences, indictments with inmates etc.), it is difficult to imagine a continuous flow of lawyers to the penitentiary in order to put conclusions from this place.

In fact, we consider that the role of the lawyer must be performed in the courtroom, directly before the court, as he is an important actor in carrying out the act of justice.

Thus, we have found that the practice of the courts in the country is that of a lawyer still be present in the courtroom, while the prisoner is heard by videconference.

This was also the practice of the Timişoara Court during the state of emergency.

The legal issue that we consider should be discussed is that of the possible invoking absolute nullity if the lawyer is not present at the place of detention, in relation to the provisions of Art. 281 par. 1 lett. f Code criminal procedure – assisting the suspect or defendant, as well as the other parties, when the assistance is mandatory.

From our point of view, even if the lawyer is present in the courtroom, but the person inmate is offered the possibility of direct video contact with him, without the presence of the judge and prosecutor in the courtroom (if such direct contact is requested), the guarantees of the right of the defence are respected.

Therefore, even if we can formally consider that the provisions of Art. 106 par. 3 Code of Criminal Procedure are violated, it would operate at most the relative nullity of the act thus achieved, and it is necessary to prove any harm.

---

[4] Amendments adopted by Emergency Ordinance 70/2020 on the regulation of certain measures, starting with 15 May 2020, in the context of the epidemiological situation caused by the spread of coronavirus SARS-CoV-2, for the extension of certain deadlines, for the modification and completion of Law no. 227/2015 on the Fiscal Code, the National Education Law no. 1/2011, as well as other normative acts.

However, the injury cannot be proved if the judge of the case ensures that, although the lawyer was present in the courtroom, the person inmate benefited from all the guarantees specific to the rights of the defence.

The problem must also be considered taking into account the social context in which we find ourselves, the multitude of cases that must be judged by videconference, but also the reality of criminal justice at this time, which must constantly anchor itself in concrete needs, but also keep pace with technology in this branch of law.

It is important to note that the Multiannual Action Plan 2014-2018 on European e-Justice[5] established among the objectives that the use of videoconference, teleconference or other appropriate means of distance communication for hearings should be extended, where appropriate, to avoid the need to go to court in order to participate in judicial proceedings, especially in cross-border cases. It is noted that electronic communication between the judicial authorities of the Member States should be further developed, in particular in the framework of instruments adopted in the European judicial area in the field of civil, criminal and administrative law (e.g. via videoconferencing or secure electronic exchange of data).

We note that the conference can be analysed from a double perspective: This can be considered a genuine evidence procedure, thus obtaining means of proof in criminal proceedings, but at the same time the videconference can be considered as a genuine way of conducting criminal proceedings.

The provisions of the Code of Criminal Procedure refer to the hearing of the person in detention, or to listening to them, so the conference is rather the means of carrying out the probation process.

In recent doctrine[6], the videoconference has been included in the category of auxiliary probative processes, along with confrontation.

According to the provisions of Art. 364 par. 1 Code criminal procedure, if heard by videoconference, the person deprived of liberty shall be deemed to be present at the trial.

Hearing by videconference shall also be governed by the provisions of Article 597 (2) ind. 1 of GO 18/2016, as well as Art. 29 of Law 254/2013 on the execution of sentences and custodial measures ordered by the judicial bodies during criminal proceedings.

II. Controversy at European Level

The videconference in criminal proceedings has borne controversy at European level, with the European Court of Human Rights considering how the application of the provisions governing it affects the rights of the defence.

The European Court of Human Rights has shown that the use of videoconferencing in criminal proceedings is in itself compatible with the right to a fair trial, but has paid particular attention to the safeguards accompanying the use of such a procedure in criminal proceedings.

---

[5] Multi-annual action plan 2014-2018 on European e-Justice (2014/C 182/02), published in the Official Journal of the European Union No C182/2 of 14 June 2014, www.eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52014XG0614(01) & from=EN, 28.05.2020.

[6] Gheorghiță Mateut, *Criminal Procedure. The general part*, Ed. Legal Universe, Bucharest, 2019, p. 573.

In a number of cases against Italy relating to trials involving mafia members, the European Court of Human Rights ruled on the compliance of Article 6 of the Convention with the use of videoconferencing[7].

In *M. V. v. Italy*[8], it was found by the European Court of Human Rights that the plaintiff had been accused in Italy on 16 March 1992 of association for the commission of mafia-type crimes and murder and was remanded. Since 2000, the complainant has been placed under a strict solitary regime involving, inter alia, restrictions on contacts with the outside. For this reason, he was no longer transferred from prison to court, but still had the opportunity to attend the trial by means of an audiovisual link with the room where the debates took place.

Before the Strasbourg Court, the applicant complained that he had been compelled to participate by videoconference in the appeal proceedings, alleging infringement of Article 6 (1) and (3) of the Convention, since the use of that technical means caused him difficulties in exercising his rights of defence.

The Court found that although it is not expressly provided for in par. (1) of Art. 6 of the Convention, the possibility of the accused to take part in the trial results from the object and purpose of this article. Thus, from the interpretation of paragraphs c), d) and e) of par. (3) of the aforementioned article, it is apparent that "any accused" has the right "to defend himself", "to ask or request the hearing of witnesses", and "to be assisted free of charge by an interpreter, if he does not understand the language used at the hearing", matters which cannot be conceived without his presence. Article 6 of the Convention, read as a whole, therefore recognises the defendant's right to actually participate in the trial, which includes, in principle, among other things, not only the right to attend, but also to listen to and follow up on the debates.

With regard to the exercise of the rights of the defence, the Strasbourg Court revealed that the applicant was able to enjoy an audiovisual link with the courtroom, which allowed him to see the people who were present and to hear what was being said. He was also seen and heard by the other parties, by the judge and by witnesses, having the freedom to make statements before the court, from the place of detention. It is certainly possible that, due to technical problems, the connection between the courtroom and the place of detention may not be ideal, which may cause difficulties in conveying voice and images. However, in the present case, at no point in the debate on appeal has the applicant sought, himself or through its defenders, to inform the judge of the hearing or visual difficulties.

The Court also pointed out that the plaintiff's defender had the right to be present at the location of his client and to contact him in a confidential manner. This possibility was equally recognised to the defender in the courtroom. Nothing demonstrates that, in the present case, the applicant's right to communicate with his lawyer without being heard by third parties has been infringed.

Regulations in Italian legislation on videoconferencing were also subject to constitutional review[9]. Thus, according to Decision No 342/1999[10], the Constitutional Court of Italy has established that distance participation does not infringe the rights of

---

[7] M. V. v Italy, judgment of 29 June 2006; Case Z. v Italy, judgment of 27 November 2007; Case A. v Italy, Judgment of 27 November 2007, www.echr.coe.int, 28.05.2020.

[8] Extract from Daniela Dediu, *op. cit.*, www. Revistaprolege.ro, 28.05.2020.

[9] *Ibidem.*

[10] Available online at www.giurcost.org, 28.05.2020.

defence guaranteed by Article 24(2) of the Italian Constitution. He rejected the idea that only the defendant's physical presence in the courtroom would ensure the effectiveness of that right. Article 146a does not only regulate the technical means of putting into practice the link between the courtroom and the place of detention, but also requires certain results, including the effective participation of the accused in proceedings with a view to the proper exercise of the rights of the defence. For example, the legislator guaranteed contact between the defendants, the right of the defender to be present at the location of the prisoner and the possibility of consultation between the defendant and his lawyer.

The appearance in person of the accused does not imply the same decisive importance in appeal as at first instance, the application of Art. 6 of the Convention on Appeals depending on the role this appeal plays in criminal proceedings according to the internal legal order.

The Court held that the applicant's participation in the appeal proceedings by videoconference *pursued legitimate purposes in the light of the Convention*, relating to the protection of public order, the prevention of criminal offences, the protection of the rights to life, freedom and safety of witnesses and victims of offences, as well as respect for the requirement of a reasonable period of time for judicial proceedings.

According to the Ordinance of the Constitutional Court of Italy no. 483/2002[11], distance participation has the following objectives: A) the protection of public order with reference to the possible actions of the accused of intimidation in relation to the other parts of the trial; B) to avoid transferring the accused from prison to the courtroom to renew contacts with criminal associations to which he is affiliated; C) accelerating the conduct of complex and long processes taking place in different instances. At the same time, the Italian constitutional court revealed that the system introduced by Law no. 11/1998 guarantees the right of the person accused of crimes of exceptional seriousness to participate in the trial, balancing the requirements of the protection of the community and those of the process.

In *Sakhnovskiy v. Russia's* case[12] the state of affairs was as follows, and in this case the Court found *an infringement of the Convention.*

In 2001, the plaintiff was sentenced to imprisonment for murder. In 2002, the Supreme Court rejected his appeal. In 2007, the presidium of the Supreme Court upheld a review, overturned the judgment in appeal, and returned the case for review, considering that the applicant's right to be assisted by a defender during the appeal hearing had not been respected. In the course of the new appeal proceedings, the plaintiff watched the arrest hearing by videoconference because the Supreme Court rejected his request to appear in person. Prior to the start of the debate, the plaintiff was presented to his newly appointed public defender, who was in the courtroom, and the Supreme Court granted them 15 minutes of confidential meeting by videoconference. The plaintiff tried to refuse to be represented by the lawyer, considering he needed to meet with him personally. The Supreme Court rejected the applicant's objection to his lawyer, finding it unreasonable. The court held that the plaintiff did not apply for a colleague to replace the lawyer or seek permission to choose another lawyer. In a different decision, the Supreme Court decided not to accept the applicant's new statement of appeal and to examine the case file on the

[11] *Ibidem.*

[12] Available online at www.echr.coe.int, 28.05.2020.

basis of the statement lodged in 2002 by the applicant's former lawyer before the previous hearing in appeal proceedings. The same day, the Supreme Court examined the substance of the case and upheld its judgment in 2001.

The applicant alleged, in particular, that the criminal proceedings against him had been conducted in violation of Article 6 §§ 1 and 3 (c) of the Convention, claiming that in the appeal proceedings he had not beengiven free legal assistance and that, moreover, he had been unable to defendhimself effectively because he had communicated with the court of appealby video link.

The Court observes that the original conviction was quashed by the Presidium of the Supreme Court in 2007 specifically because of the breach of the applicant's right to legal assistance. It is thus clear that for the authorities the case was complex enough to require the assistance of a professional lawyer. Given that, as well as the Court's own assessment of the complexity of the issues raised before the appellate court, the Court concludes that the assistance of a lawyer was essential for the applicant in the second set of the appeal proceedings.

The Court has considered the arguments of the Government in support of their position and accepts that Ms A. was a qualified lawyer and that there was no explicit disagreement between her and the applicant on the substance or strategy of his defence. While it is established that Ms A had read the case file, it is unclear how much time she spent on it and the Government have not submitted any specific information or evidence on this point. She was *a priori* prepared to assist the applicant, and this is, without doubt, a relevant consideration. However, these arguments are not decisive; the Court must consider whether the arrangements for the conduct of the proceedings, and, in particular, for the contact between Ms A. and theapplicant, respected the rights of the defence.

The Court emphasises that the relationship between the lawyer and his client should be based on mutual trust and understanding. Of course, it is not always possible for the State to facilitate such a relationship: there are inherent time and place constraints for the meetings between the detained person and his lawyer. Moreover, in exceptional circumstances the State may restrict confidential contacts with defence counsel for a person in detention (see *Kempers v. Austria* (dec.), no. 21842/03, 27 February 1997, or *Lanz v. Austria*, no. 24430/94, § 52, 31 January 2002). Nevertheless, any limitation on relations between clients and lawyers, whether inherent or express, should not thwart the effective legal assistance to which a defendant is entitled. Notwithstanding possible difficulties or restrictions, such is the importance attached to the rights of the defence that the right to effective legal assistance must be respected in all circumstances.

In the present case, the applicant was able to communicate with the newly-appointed lawyer for fifteen minutes, immediately before the start of the hearing. The Court considers that, given the complexity and seriousness of the case, the time allotted was clearly not sufficient for the applicant to discuss the case and make sure that Ms A.'s knowledge of the case and legal position were appropriate.

Moreover, it is questionable whether communication by video link offered sufficient privacy. The Court notes that in the *Marcello Viola* case the applicant was able to speak to his lawyer via a telephone line secured against any attempt at interception. In the case at hand the applicant had to use the video-conferencing system installed and operated by the State. The Court considers that the applicant might legitimately have felt ill at ease when he discussed his case with Ms A.

In addition, in the *Marcello Viola* case counsel for the defendant had also been able to send a replacement to the videoconference room or, conversely, attend on his

client personally and entrust the lawyer replacing him with his client's defence before the court. A similar conclusion was reached in the case of *Golubev* where the Court did not find a violation of Article 6 on account of a hearing via video link because, *inter alia*, "the applicant's two lawyers were present at the appellate hearing [in the hearing room] and could have supported or expanded the arguments of the defence... The applicant was able to consultwith his lawyer in private before the hearing. Furthermore, since theapplicant had two lawyers, he could choose one of them to assist him in thedetention centre during the hearing and to consult with him in private."None of the options described above was available to the applicant in thecase at hand. Instead, the applicant was expected either to accept a lawyerhe had just been introduced to, or to continue without a lawyer.

The Court concludes that the arrangements made by the Supreme Court were insufficient and did not secure effective legal assistance to the applicant during the second set of the appeal proceedings.

III. Cross-border Videconference – Model to be Followed Internally

At European level, the Council of Europe has implemented a Guide on the use of videconferences in cross-border judicial proceedings[13]. This guide has been drafted by the General Secretariat of the Council for information purposes only and is useful for both Member States' legislators and judicial bodies.

It is useful to note that the Guide covers cross-border proceedings, but the aspects contained in it can also be used in domestic cases involving judicial bodies in the Member States.

The guide concerns the use of videoconferencing equipment in cross-border judicial proceedings in the European Union. It examines the uropazeonal, technical and legal aspects of the use of technology for videoconferencing. Furthermore, it analyses the use of equipment in courts and witness rooms, as well as the use of portable equipment. The guideline applies in cases where videoconferencing is used for any part of court proceedings, in particular for obtaining evidence from remote locations in other EU Member States. The guide provides advice and guidance for legal professionals, clerks and technical staff.

It examines practical considerations relating to the use of videoconferencing equipment which is of particular interest to legal professionals and court staff, and then examines technical issues of particular interest to technical staff. Annex I to the Guide provides details on the legal framework for the cross-border use of videoconferencing in criminal matters as well as in civil and commercial matters. The other Annexes describe the technical standards to be taken into account and provide a summary of the key steps to be followed in the use of videoconferencing in cross-border judicial proceedings. The aim of the document is to help users by providing advice and guidance. Does not replace detailed operating instructions or detailed operating instructions. This document mainly concerns the use of videoconferencing in court proceedings of criminal, civil and commercial courts.

However, many of the technical aspects relating to the use of videoconferencing are more generally applicable in the wider justice community. The hearing of

[13] Available online at www.consilium.europa.eu, 28.05.2020.

witnesses and experts does not always take place in the courts and it is possible to establish a connection for videoconferencing between courts and other locations, such as consular and diplomatic representations, prisons, hospitals and asylum centers. This document can be used as such as a basis for the use of videoconferencing in other procedures[14].

IV. Conclusions

Obviously, videconference is and will be used more and more in criminal proceedings. Why? Firstly, due to the need to uropaze procedures in relation to the current social situation. We also note today that the videconference is not only a derived probationary procedure, as it was classified by doctrine, but it is in itself a way of protecting participants in the act of justice.

The need to protect against the new coronavirus during this period has led us to use this probative procedure much more often than before.

Is this a time when justice is changing technologically?

Technology is welcome in the area of justice, a good example being the existence, at this point, of the electronic file, recently implemented in our country.

However, what judicial bodies need to take care of is how the practical application of technological procedures will respect the right to a fair trial. How important, under these circumstances, is the direct, physical contact between the defendant and his lawyer, or between the judge and the defendant?

Therefore, the application of technology to the justice system will have to be carried out without extreme interference with the rights of the defence, and only in this way it will succeed in the criminal proceedings.

References

1. Dediu, D., *Videconference in national criminal proceedings and international judicial cooperation in criminal matters. Right to a fair trial*, Pro Lege Magazine, 2018, www.revistaprolege.ro, 28.05.2020.
2. Mateut, Gh., *Criminal Procedure. The general part*, Ed. Legal Universe, Bucharest, 2019.
3. Multi-annual action plan 2014-2018 on European e-Justice (2014/C 182/02), published in the Official Journal of the European Union No C182/2 of 14 June 2014, www.eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52014XG0614(01) & from=EN, 28.05.2020.
4. www.consilium.europa.eu.
5. www.echr.coe.int.
6. www.giurcost.org.

[14] *Ibidem.*

Juvenile Institutional Criminal Sanctions in The Law System of Republic of Serbia

***Dr. Dragan Jovašević*[1]**

Abstract

All material (corporeal), processing and executive provisions related to criminal law in Republic of Serbia about juveniles are, in the new Law about juvenile committers and criminal law protection of juveniles from 2006. January 1st (LAJCCA), conjoint in one place. That is how the juvenile criminal law has been created. It is characterized as follows: 1) principally, inquest of the juvenile injurers guilt is excluded, 2) among criminal sanctions towards juvenile injurers the priority belongs to the educable provisions comparing to the punishment that presents the exception expressed in juvenile jail implementation. By the way of exception with the juvenile jail can be punished only the older juvenile if he committed a crime for which the proposed punishment is over five years, if he is sufficiently mentally mature that he can understand importance of that crime and he control his acts and if the consequences of the committed crime are that grand, and the extent of guilt that high when the application of educative provisions wouldn't be justified, 3) in the criminal proceeding towards juveniles, prosecution and juridical apparatus have wide authority in terms of starting, processing and terminating the proceeding. Those authorities consist of discrete rights to withdraw prosecution no matter what is the committed crime, if it is considered that it would be useful in terms of education and reeducation of the juvenile delinquent. The principle of utility has the priority than the principle of objectiveness. The court mandates consist of not only a wide scale of optional means and provisions, but of possibility to replace already delivered verdict with some other more convenient provision, if it is required by the specific situation and 4) in juridical system of the Republic of Serbia there are special jurisdictional bodies for struggle against juvenile criminality: special departments for juvenile delinquency in internal affairs agencies, a prosecuting attorney for juveniles and special juvenile council i.e. the juvenile court that supervises the whole criminal proceeding against any juvenile delinquent. The juvenile court is represented with lay judges that have competences and personal qualities whereby can influence the juvenile delinquent. In the process the special role belongs to the authorities of social welfare. The new juvenile criminal law anticipates two basic types of the juvenile criminal sanctions. These are: 1) the educational measures and 2) the juvenile prison. They are legally anticipated

[1] Law Faculty, University of Niš, Republic of Serbia.

measures of the social reaction towards the juvenile committers of the crime activities that are sentenced the legally determined organs (the district court – the judge for the juveniles and the tribunal for the juveniles) in aim to protect the society from the criminality trough the education, reeducation and proper development of the juvenile. Beside and instead of sanctions, the new criminal legislature recognizes also the special type of measures – the educational dictates (orders) as the alternative measures that have the aim the deflecting of the criminal proceeding towards the juveniles (la diversion) to the other measures application. In this paper the author has analysed theoretical and practical aspects of institutional criminal sanctions for juvenile criminal offenders in new criminal law of Republic of Serbia.

Keywords: *code, juvenile, crime, sanctions, measures, prison, education, court*

I. Introduction

New juvenile criminal legislation (substantial, procedural and executive) entered into force in the Republic of Serbia at the beginning of 2006[2]. That opened an entire new chapter in the development of our country's criminal law and represented a radical twist when it comes to the establishment and functioning of a modern legal state and rule of law. Juvenile criminal law[3] is a part i.e. a segment of criminal law that has lately gained a status of an independent legal and scientific discipline in a series of European countries due to a multitude of its specific solutions. It represents a special, coherent and autonomous entity comprised of a number of solutions that differ from those referring to adult offenders.

Juvenile criminal law represents a set of legal provisions that determine the criminal-legal status of juveniles (as offenders but also as the victims of criminal offences)[4]. This term (that legal theory often refers to as a postulate of criminal policy), stands for a branch of law comprised of criminal legal provisions that are applied to juvenile offenders and that depict its particular and specific character. This field of law is focused on the personality of the offender (Taterstrafrecht), rather than on the offence itself (Tatstraftrecht). In other words, it is a set of legal provisions that determine the system of

[2] D. Jovašević, Maloletničko krivično pravo, Niš, 2011. pp. 12-18.

[3] The term "juvenile criminal law" is common in legal theory (G. Marjanovik, Makedonsko krivično pravo, Opšt del, Skoplje, 1998. p. 361. and Lj.Bavcon, A. Šelih, Kazensko pravo, Splošnij del, Ljubljana, 1999. p. 230.). However, the term "criminal law for juveniles" is also used in legal theory for this branch of law. Both terms imply that there is a criminal law of "juvenile character" as a contrast to criminal law that refers to adults. It is worth mentioning that there are standpoints in a part of German legal theory claiming that juvenile criminal law includes the cases of offenders who are under 25.

[4] In Germany (Jugendgerichsgesetz of 1974. with addition of 1990.), France (Ordonnance No. 45-174 du 2. fev.1945. with addition of Law No. 2002-1138 of 2002.), Croatia (Zakon o sudovima za mladež – Official gazette of Republic of Croatia No. 111 of 1997.), Macedonia (Zakon za maloletničku pravdu – Official gazette of Republic of Macedonia No. 87 of 2007.) and Serbia (Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica – Official gazette of Republic of serbia No. 85 of 2005), this branch of law has been officially separated from their Criminal Laws (Codes).

sentences for juvenile offenders[5], but, under specific circumstances, for adult offenders as well, and the procedure for imposing and executing these sentences by competent state authorities. Therefore, it can be said that juvenile criminal law goes beyond the frames of criminal law because it does not include only substantial criminal legal provisions but the provisions of procedural and executive criminal law as well, in the extent in which they deal with juvenile perpetrators.

Juvenile criminal law[6] represents a set (a system) of legal provisions that regulate the position (i.e. rights and obligations) of a juvenile in criminal legal system. These provisions primarily refer to:

a) the definition and the types of juveniles as subjects of criminal law (active and passive),

b) types, conditions, purpose and methods for prescribing and imposing sentences on juvenile offenders,

c) the procedure for imposing sentences on juveniles (that represents a specific type of criminal procedure because of the authorities that are competent for its initiation and conduct as well as for the enforcement and execution of sentences) and, finally,

d) the procedure of the execution of imposed juvenile sentences.

Juvenile criminal law can be singled out from the criminal law that is generally applied to adult offenders because of the character of its numerous provisions. However, it can, by way of exception, be applied to adult offenders as well, if specific conditions determined by the law are met.

II.The Basic Characteristics of Juvenile Criminal Law

When it comes to national criminal law, the Law on Amendments and Changes of the Criminal Code of FNRJ from 1959 was the first to single out the provisions dealing with juvenile criminal sentences in a separate chapter. Furthermore, The Criminal Procedure Code included special provisions dedicated to the criminal procedure against juveniles, whereas the Law on the Execution of Criminal Sentences regulated the procedure, the manner and the conditions of the execution of criminal sentences imposed on juveniles. That was the beginning of the establishment of juvenile criminal law, which nowadays has the following characteristics[7]:

1) Criminal legal provisions do not refer to a person who was under the age of fourteen[8] at the time of commission of an unlawful act provided under law as a criminal offence. (Paragraph 2, ZOMUKD). Such persons are referred to as children (infants) and are not treated as active subjects of criminal law. Criminal legal provisions cannot be applied to them, but provisions of other branches of law (such as Family Law and Social Welfare Law) can,

---

[5] There are standpoints in the history of criminal law according to which the first penitentiary institution for juvenile offenders was established in Rome in 1703 upon the initiative of the Roman Pope Clement IX. Later on, other similar institutions were established in other countries as well, such as Germany, France, Switzerland and United Kingdom.

[6] B. Đukić, D. Jovašević, Kriminalitet maloljetnika i mjere društvene reakcije u Republici Srpskoj, Banja Luka, 2010. pp. 34-45.

[7] D. Jovašević, Krivično pravo, *Opšti deo*, Beograd, 2018. pp. 287-296.

[8] It is worth mentioning that there are standpoints in a part of German legal theory claiming that juvenile criminal law includes the cases of offenders who are under 25 (W. Sauer, *Kriminologie*, Berlin, 1950, p. 108).

2) According to linguistic and grammatical interpretation, the term "juvenile perpetrator of a criminal offence" is not valid, since there is no criminal offence without perpetrator's guilt (according to the objective-subjective theory of criminal offence from paragraph 14 of the Criminal Code of the Republic of Serbia). Also, the term "guilt" is not in accordance with the expressions such as "infant" and "juvenile". That is the reason why the Criminal Code itself uses a rather vague formulation: "a juvenile who has committed an illegal act that is prescribed as a criminal offence by the law". Moreover, the presence and the assessment of guilt during a criminal procedure are excluded in the case of juvenile offenders,

3) Juvenile criminal law, as a consistent system of criminal legal provisions that are applied to juvenile offenders, is unfamiliar with numerous terms and institutions that are commonly present in the "classical i.e. standard" criminal law that is applicable to adult offenders, such as: guilt, punishment, penal and retributive system, the proportion between the punishment and the grade of offender's hazard and the determination of punishment for joinder of criminal offences,

4) The system of juvenile criminal law[9] is supposed to be ruled by the goals of criminal policy such as juvenile offender's education and re-education, emphasizing the principle of education instead of the principle of punishing. This has highlighted the preventive character of this branch of law and led to the abandonment of its previous "therapeutic" concept. In theory, it is pointed out that juvenile criminal sentences primarily represent measures of help and socialization containing a smaller amount of coercion, repression and limitations of rights and freedoms and a greater amount of help, guardianship, supervision, prevention of disturbances and establishment of preconditions for juvenile's normal and uninterrupted development and maturation. This is in accordance with the so-called "Havana Rules", adopted by the OUN in 1990 that insist on exclusion or at least minimization of any form of deprivation of liberty when it comes to juvenile offenders. (Paragraph 11, Point 6),

5) Among criminal sentences applied to juvenile offenders, educational measures are more preferable in comparison to punishment[10] (i.e. juvenile prison sentence) that represents an exception. The Law is familiar with nine educational measures divided into three groups: a) the measures of admonition and guidance (that have replaced former disciplinary measures), b) the measures of intense supervision and c) institutional measures,

6) Juvenile prison sentence can be imposed solely by way of exception on an elder juvenile who has committed a serious criminal offence, for which a penalty of imprisonment exceeding five years is prescribed by the Law. Educational measures are the most common form of society's reaction to juvenile offenders. Yet, the enforcement of educational measures should be conducted gradually. That is the reason why the priority is given to milder educational measures (such as measures of admonition and guidance), whereas more severe ones such as measures of intense supervision and, finally, institutional measures are imposed as subsidiary. Moreover,

---

[9] D. Jovašević, *Maloletničko krivično zakonodavstvo i savremene tendencije krivičnopravne represije*, Zbornik radova, Bijeljina, 2010. pp. 167-186.

[10] According to official statistics, institutional educational measures represent 1-2,7% and juvenile prison sentence represents 0,6-1,7% of the total amount of criminal sentences imposed on juvenile offenders in the Republic of Serbia between 1997 and 2002.

the priority is not even given to criminal sentences but to their substitutes (informal sentences) whose enforcement is also reduced to the smallest possible amount[11],

7) Contemporary criminal legislations (such as Germany, France, Macedonia, Croatia and Bosnia and Herzegovina) are familiar with various measures of alternative character (substitutes of criminal sentences) that can be imposed either along with or instead of criminal sentences. According to the non-intervention theory, their enforcement is recommended, whenever it is possible to avoid the criminal justice system through the diversion of a criminal procedure[12], especially in the case of petty, sporadic, primary, occasional or accidental crime. They include various sui generis measures such as educational orders, instructions, prohibitions or recommendations for juvenile offenders. Actually, the aim of the enforcement of these measures is the diversion of a criminal procedure against a juvenile offender from the field of Criminal Law to other branches of law such as Family Law and Social Welfare Law. Such solution is in accordance with Paragraph 40 Subpart 3 Point 6 of ht OUN Convention on the Rights of the Child that requires the member states to implement all the possible measures in order to deal with children and minors in conflict with the law without initiating a criminal procedure,

8) New legal provisions prescribe judicial protection of juveniles in the process of execution of imposed juvenile criminal sentences instead of former administrative protection,

9) The provisions dealing with the supervision of the execution of educational measures also represent an innovation. The judge for juveniles (who has imposed an educational measure) and the public prosecutor for juveniles supervise the enforcement of the imposed educational measure. They are obliged to: a) keep up with the results of the enforcement of the imposed educational measure, b) visit the juvenile in the institution he is placed into, c) conduct direct inspection and d) review reports on the course of execution of the imposed educational measure.

The competent social welfare centre is also obliged to send his report on the course of execution of other educational measures (special obligations and measures of intense supervision) to the court and to the public prosecutor for juveniles every 6 months. The judge for juveniles can require the social welfare centre to deliver these reports in shorter periods of time, but he can also demand similar reports to be written by other competent persons such as a social worker, a psychologist, a pedagogue or a special pedagogue, if some of them are employed in the court. Finally, the administration of the institution a juvenile is placed into is also obliged to send the report on the results of the execution of the imposed educational measure to the court

---

[11] Although imposing punishments on juvenile offenders represents an exceptional legal possibility, there are criminal legislations prescribing a wide range of punishments that can be imposed on juvenile offenders. For example, Paragraph 87 of Russian Criminal Code prescribes that either a punishment or educational measures can be imposed on juveniles who committed a criminal offence. Several punishments that can be imposed on juveniles are enumerated in its Paragraph 88: a fine, prohibition from practicing a profession, compulsory labor, correctional labor, isolation and deprivation of liberty up to 10 years.

[12] Legal theory disapproves the use of the term "diversion model" of criminal procedure against juveniles, especially when taking into consideration the practical significance of the principle of opportunity in criminal procedure against juveniles that is referred to as "diversion" in German legal theory. Diversion represents a form of turning from a general, common and regular criminal procedure. A diversion model means solely that the procedure ends in a way that differs from the one that is common according to general rules.

and the public prosecutor every 6 months. However, the court can require this report to be delivered in a shorter period of time and

10) The assistance offered to the juvenile after an institutional educational measure or juvenile prison sentence has been executed, is now arranged in a different way. Post-institutional treatment and acceptance of the juvenile are also set differently by emphasizing the significance of the role and the activities of the competent social welfare centre. During the entire period of the enforcement of the imposed juvenile criminal sentences, social welfare centre maintains continuous cooperation and contact not only with the institution the juvenile is placed into but also with his family in order to prepare and enable them to reintegrate the juvenile in his previous social surroundings as well as to infiltrate him in the course of normal and socially acceptable life and activities.

III. Criminal Sentences for Juvenile Offenders

1. The definition and the purpose of juvenile criminal sentences

Juvenile criminal law in the Republic of Serbia from 2006. is familiar with two basic types of juvenile criminal sentences[13]: a) educational measures and b) juvenile prison sentence. They are defined as measures of social reaction to juvenile offenders that are prescribed by the law and imposed by the authorities determined by the law (superior court-judge for juveniles and council for juveniles) in order to protect the society from crime through education, re-education and regular development of juveniles. Educational measures represent the most common type of juvenile criminal sentences. They are imposed regularly i.e. most frequently. They can be imposed on all juvenile offenders, younger as well as elder[14]. Only subsidiary and by way of exception, when the conditions prescribed by the law are fulfilled and when the court comes to the conclusion that the purpose of juvenile criminal sentences cannot be accomplished by the enforcement of educational measures, can the court impose on an elder juvenile a penalty of a special kind-juvenile prison sentence. Such sentence can be imposed solely on an elder juvenile who has committed a serious criminal offence. Therefore, the sentence of juvenile prison is not compulsory; it can neither be imposed on any juvenile offender nor for any criminal offence.

The purpose of juvenile criminal sentences is determined in two ways. Their primary purpose is equal to the purpose of all the other criminal sentences, defined by paragraph 4 of the Criminal Code of the Republic of Serbia and includes suppressing the acts that violate and threaten the values protected by criminal legislation. Therefore, the general purpose of juvenile criminal sentences is the suppression of all types, varieties and forms of crime. Within this general purpose of all criminal sentences (including juvenile criminal sentences), paragraph 10 of ZOMUKD separately defines the purpose of juvenile criminal sentences as: a) influencing juveniles' development and the establishment of their personal responsibility, b) influencing their education[15] and c) regular development of their personality in order

[13] D. Jovašević, *Maloletničko krivično pravo*, Beograd, 2008. pp. 45-59.

[14] J. Hellmar, *Jugendkriminalitaet*, Darmstadt, 1978.pp-78-94.

[15] It is process that includes juvenile's training to build his own attitude towards various social values through gaining knowledge in various fields.

to enable them to reintegrate in the community. Such purpose can be accomplished in three ways[16]: a) through supervision, b) through offering protection and assistance and c) through providing general and professional education. When determining the aim of these sentences, the law highlights education, re-education[17] and regular development[18] of juveniles, particularly through special preventive measures[19].

The Law on Juvenile Justice of Former Yugoslav Republic of Macedonia[20] determines the purpose of juvenile criminal sentences in a similar way-the enforcement of these measures is subordinate to the aims of protection, education, re-education and regular development of juveniles. Namely, Paragraph 29 of this Law defines the purpose of educational measures as providing protection and assistance in order to facilitate juvenile's education and re-education. Finally, Paragraph 5 of the Law on Courts for Juveniles of the Republic of Croatia determines the purpose of juvenile criminal sentences within the general purpose of criminal sentences as "influencing juvenile's education, development of his entire personality and strengthening his personal responsibility through protection, care, assistance and supervision as well as through providing general and professional education"[21].

No matter how preventive the character of these sentences is[22], their coercive and retributive features are not completely excluded because the enforcement of these sentences does not depend on juvenile offender's consent and they do contain certain limitations, prohibitions, conditions and obligations for the juvenile to act in accordance with specific instructions and orders. Besides, the purpose of juvenile prison sentence is to influence a juvenile offender more intensely not to commit

---

[16] The purpose of educational measures prescribed by the law can be accomplished in different ways such as: separating a juvenile from his social surroundings or family because of the negative impact they have on his development and education; guidance and assistance in education or particular medical treatments; supervision conducted by a parent, by an adopter, by a custodian or by a representative of state authority in order to keep up with his activities and notice and attempt to prevent negative influences and causes of his unacceptable behavior; juvenile's professional training that includes obtaining socially useful skills and abilities through various forms of education; the development of juvenile's personal responsibility through a diversity of tasks and duties making the juvenile personally responsible for the quality and the efficiency of their fulfillment.

[17] Such process includes the elimination of harmful consequences of the fact that a juvenile has been educationally neglected. It is conducted through a particular individual or group treatment including various methods and procedures.

[18] It is the creation of an appropriate social ambient in which the juvenile might accept and respect certain rules of behavior.

[19] Croatian criminal law determines the purpose of educational measures in a similar way: to influence juvenile's education, the development of his entire personality and strengthen his personal responsibility through protection, custody, assistance and supervision. Besides, the purpose of these sentences, as well as of the criminal sentences in general, is to provide that the citizens respect the legal system of the state, that nobody commits a criminal offence and that those who have committed such offence do not repeat it (Ž.Horvatić, *Kazneno pravo*, Opći dio, Zagreb, 2003. p. 247).

[20] More: Lj. Arnaudovski, L. Nenev, *Juvenile Penal Code*, Kavadarci, 2001.

[21] Ž. Horvatić, *Kazneno pravo*, Opći dio, Zagreb, 2003. p. 247.

[22] In order to accomplish the purpose of educational measures prescribed by the law, juveniles are supposed to be treated in a special manner that is adjusted to their age, personal characteristics and the type and the gravity of the criminal offence they have committed. Such treatment is based upon contemporary principles of pedagogy, psychology and andragogy. Through the course of diverse treatments for juveniles, it is especially taken into account that a juvenile should be enhanced (encouraged) to participate actively in his education and upbringing, changing his attitudes and habits and developing the sense of responsibility for his own acts.

criminal offences in the future as well as on other juveniles not to commit criminal offences. This means that the purpose of juvenile prison sentence is determined in two ways[23]: a) as special prevention-influencing the perpetrator not to repeat criminal offences and b) as general prevention-influencing other juveniles not to commit criminal offences. That is how the protective model[24] and the justice model[25] (i.e. special preventive purpose of juvenile criminal sentences) have been implemented in new juvenile criminal legislation instead of the previously supported therapeutic conception.

2. Types of juvenile criminal sentences

Basic types of juvenile criminal sentences[26] prescribed by our criminal legislation include nine educational measures divided into three groups. These are the following: a) measures of admonition and guidance, b) measures of intense supervision and c) institutional measures. Although the law does not draw such distinction between them, there are standpoints in legal theory suggesting that educational measures can be divided into milder and more severe measures. Accordingly, measures of admonition and guidance are considered as milder, whereas institutional measures are considered as the most severe ones. Such division of educational measures is in accordance with the principle of their gradual enforcement, which means that a milder measure will be applied whenever it is considered as sufficient to accomplish the purpose of educational measures, whereas more severe measures will be imposed as subsidiary. This differentiation among educational measures is based upon their contents, conditions and criteria for their implementation as well as upon their duration and means of enforcement.

A special form of punishment known as juvenile prison sentence can be imposed on an elder juvenile in particular cases. However, all security measures apart from the prohibition from practicing a profession, activity or duty can be imposed on juveniles under circumstances prescribed by the law (Paragraph 39 ZOMUKD). Security measures can be imposed on a juvenile offender solely as subsidiary or supplementary sentences along with an educational measure or a juvenile prison sentence. In some cases, security measure of compulsory psychiatric treatment and confinement in a medical institution can be imposed on a juvenile as an autonomous sentence provided that conditions prescribed by the law are fulfilled (Paragraph 81, KZRS).

---

[23] B. Petrović, D. Jovašević, A. Ferhatovć, *Krivično pravo 2*, Sarajevo,2016. pp. 189-213.

[24] The protective model emphasizes juvenile's personality, his condition and needs. Namely, it is based upon the standpoint that a criminal offence solely causes the initiation of a criminal procedure against a juvenile, whereas his personality and interests have vital impact on the court's decision. The victim or the injured party is of secondary significance. The duration of criminal sentences in this model is not strictly determined and their effective duration depends upon the results achieved in juvenile's re-education, with the option to replace or suspend the imposed educational measures, which significantly increases court's active role in the process of execution of the imposed juvenile criminal sentences.

[25] The justice model accentuates the victim of the committed criminal offence as well as the interest of the society. Juvenile, his personality and interests have some but not predominant significance for the course of criminal procedure. This model requires the enforcement of alternative measures that lead to the diversion of criminal procedure against a juvenile offender; it rejects the indeterminate duration of the imposed criminal sentences; juvenile's deprivation of liberty is of exceptional character and the purpose of the measures consists of victims' restitution and compensation.

[26] M. Rutter, *Juvenile deliquency*, Harmondswort, 1983. pp. 189-207.

The law has also limited the use of security measure of compulsory alcohol addiction treatment and of security measure of compulsory drug addiction treatment, so these measures cannot be imposed along with an educational measure of admonition and guidance. New juvenile criminal law is also familiar with a particular type of measures-educational orders that can be imposed either along with criminal sentences or instead of them, as alternative measures intended to enable the diversion (la diversion) of criminal procedure and its replacement with other non-penal measures[27].

Among all the criminal sentences prescribed by our criminal law, the following cannot be imposed on juvenile offenders: a) punishments, b) judicial caution and c) suspended sentence. The precondition for the enforcement of a punishment is perpetrator's guilt. Since juvenile's age excludes the presence of guilt as the subjective element of a criminal offence, it is logical that punishments cannot be imposed on juveniles. Within the system of juvenile criminal sentences, the law is familiar with a specific measure of admonition and guidance known as "judicial reprimand", whose contents, manner of enforcement and purpose completely correspond to judicial caution as a criminal sentence for adult offenders. But, it has remained unclear why the legislator excluded the possibility of imposing a suspended sentence on a juvenile offender in spite of the reasons of criminal policy for it to be applied (especially to elder juveniles when it could intensify the exceptional character of juvenile prison sentence).

IV. Definition and Types of Educational Measures

Educational measures represent the most common type of criminal sentences that can be imposed on juvenile offenders as well as on adult offenders (under particular circumstances). The law prescribes these measures in order to suppress the acts that violate or threaten the protected values, by influencing the development and the strengthening of juvenile offender's personal responsibility, his education and regular development of his personality. They are imposed by the court and comprised of limitations or deprivations of juvenile offender's rights and freedoms. The enforcement of these sentences requires two conditions to be fulfilled[28]: a) offender's age at the time of commission (between 14 and 18) and b) the commission of an unlawful act provided under law as a criminal offence.

These are sentences of a remarkably preventive character, but, since being related to a committed or an attempted criminal offence, they inevitably carry certain retributive elements, especially when taking into consideration the fact that they are applied regardless of and against juvenile's consent and include deprivations and limitations of some of his rights or freedoms or choices regarding his behavior, by imposing on him certain prohibitions or conditions i.e. orders and instructions. New juvenile criminal law of the Republic of Serbia is familiar with nine educational measures divided into three groups (Paragraph 11 of ZOMUKD)[29]:

---

[27] D. Jovašević, *Krivično pravo*, Opšti deo, Beograd, 2018. pp. 302-308.
[28] D. Jovašević, *Položaj maloletnika u krivičnom pravu*, Niš, 2010. pp. 127-132.
[29] D. Jovašević, *Maloletničko krivično pravo*, Beograd, 2011. pp. 97-104.

1) measures of admonition and guidance (that have replaced former disciplinary measures):

a) judicial reprimand and

b) particular obligations,

2) measures of intense supervision:

a) intense supervision conducted by a parent, an adopter or a custodian,

b) intense supervision in another family,

c) intense supervision conducted by a social welfare centre and

d) supervision with daily attendance in relevant rehabilitation and educational institution for juveniles (a newly introduced educational measure[30]) and

3) institutional measures:

a) remand to an educational institution,

b) remand to an educational-correctional institution and

c) remand to a special institution for medical treatment and rehabilitation[31].

None of the educational measures is prescribed as a criminal sentence for any of particular criminal offences enumerated in the special part of the Criminal Code of the Republic of Serbia. Therefore, the court is authorized to make a decision whether to impose an educational measure on a juvenile offender, which educational measure to choose in a particular case and to enforce the measure he considers as the most appropriate one to accomplish their purpose. The court is especially obliged to take into consideration the following circumstances enumerated in Paragraph 12 of ZOMUKD:

1) juvenile's age and maturity,

2) other characteristics of his personality,

3) the level of deviation of his social behavior,

4) the gravity of the committed criminal offence,

5) the motives for committing the offence,

6) the environment and the circumstances under which the juvenile has been living,

7) his behavior after the commission of the criminal offence, in particular, whether he prevented or attempted to prevent the harmful consequences of his offence or compensated or attempted to compensate the damage he caused,

8) whether the juvenile has already been sentenced for a criminal offence or a misdemeanor, and

9) all the other circumstances that can have an impact on the determination of the appropriate measure[32].

V. Institutional Educational Measures

Institutional measures i.e. the measures of institutional treatment represent the most severe educational measures. They are imposed when more permanent measures are necessary, including education, medical treatment, training and

[30] This institutional measure has replaced the measure of treatment in a special institution that has not been adequately applied in up to now practice.

[31] Lj. Hadžović, B. Babić, *Zaštita maloletnih delikvenata – priručnik za primenu vaspitnih mera pojačanog nadzora organa starateljstva*, Beograd, 1994. pp. 45-56.

[32] More: O. Matić, *Ispitivanje ličnosti maloletnika kao osnov za određivanje vaspitne mere i tretmana u VP domovima*, Beograd, 1974.

juvenile's complete separation from his former environment in order to influence his behavior more intensely[33]. Institutional measures are imposed as society's last means in the oppression of juvenile delinquency and can last (within the limits determined by the law) only for the period of time that is necessary to accomplish the purpose of educational measures. According to official statistics, the participation of these educational measures in the total number of educational measures imposed on juvenile offenders in the Republic of Serbia is relatively small- ranging from 2.7% in 1998 to 4.2% in 1996 or 4.8% in 2002.

These measures are imposed on juveniles who are so educationally neglected that their education and re-education can be accomplished only through the enforcement of long-lasting measures accompanied by a complete separation from the environment they have previously been living in[34]. The law prescribes 3 institutional measures: a) remand to an educational institution, b) remand to an educational-correctional institution and c) remand to a special institution for medical treatment and rehabilitation. The court does not determine the duration of these measures when imposing them, but decides about that subsequently, within the limits determined by the law.

1. Remand to an Educational Institution

Educational measure of remand to an educational institution (Paragraph 20 ZOMUKD) is imposed when a juvenile offender should be separated from his previous environment and provided with assistance and permanent supervision by expert individuals (expert educators)[35]. This measure is executed by the social welfare centre that sends the juvenile to an opened educational institution for juveniles that provides accommodation and fulfillment of juveniles' needs regarding education, medical treatment, learning and sports activities. A juvenile stays in an educational institution for at least 6 months but no longer than 2 years and every 6 months the court estimates whether there are reasons for the suspension of this measure's execution or for its replacement with another educational measure. A juvenile can stay in such institution until he turns 21[36].

2. Remand to an Educational-Correctional Institution

Remand to an educational-correctional institution (Paragraph 21 ZOMUKD) is imposed on a juvenile who, apart from being separated from his previous environment, also has to undergo intense measures of supervision and particular expert educational programs. A correctional institution represents a special institution with an established regime of re-education intended for more seriously educationally neglected juvenile offenders[37].

When deciding whether to impose this most severe educational measure the court especially takes into account the following circumstances: 1) juvenile's previous

---

[33] B. Petrović, D. Jovašević, A. Ferhatović, *Izvršenje vaspitnih mjera, Pravna riječ*, Banja Luka, No. 7/2006. pp. 371-394.

[34] B. Čejović, *Krivično pravo u sudskoj praksi, Knjiga prva*, Opšti deo, Beograd, 1985. p. 507.

[35] D. Jovašević, *Maloletničko krivično pravo*, Beograd, 2011. pp. 164-165.

[36] J. Vuković, M. Živković, *Izvršenje odgopjne mjere upućivanja u odgojni zavod,* Hrvatski ljetopis za kazneno pravo i praksu, Zagreb, No. 2/1999. pp. 789-813.

[37] D. Jovašević, *Leksikon krivičnog prava*, Beograd, 2011. pp. 617-618.

life, 2) the degree of deviation in his behavior, 3) the gravity and the nature of the committed criminal offence and 4) whether the juvenile has already been sentenced for a criminal offence or a misdemeanor. A juvenile can stay in a correctional institution for at least 6 months but not more than 4 years and every 6 months the court estimates whether there are reasons for the suspension of this educational measure or its replacement. A juvenile can stay in this institution until he turns 23[38].

3. Remand to a Special Institution for Medical Treatment and Rehabilitation

Remand to a special institution for medical treatment and rehabilitation (Paragraph 23 of ZOMUKD) can either be imposed on a juvenile with disorders of psychological and physical development (blind, deaf, deaf-mute, with physical injuries or disability) or on a juvenile with psychological disorders. This measure can also be imposed instead of security measure of compulsory psychiatric treatment and confinement in a medical institution provided that the special institution for medical treatment and rehabilitation can offer confinement and medical treatment of a juvenile and, through that, contribute to the accomplishment of this security measure's purpose prescribed by the law.

In this case, the imposed educational measure can last as long as is necessary for juvenile's treatment or rehabilitation. A juvenile offender cannot stay in the special institution for medical treatment and rehabilitation for more than three years and every six months the court estimates whether there are reasons to suspend the execution of the measure or to replace it with another one. If this security measure is imposed instead of security measure of compulsory psychiatric treatment and confinement in a medical institution, the juvenile can stay in a special institution for medical treatment and rehabilitation as long as it is necessary, but after he turns 21 the execution of the measure is continued in an institution where this security measure is commonly executed (Special prison hospital within the Administration for the execution of institutional sentences).

VI. Juvenile Prison Sentence

1. Definition and Characteristics of Juvenile Prison Sentence

Juvenile prison sentence is the only type of punishments in the system of juvenile criminal sentences in the Republic of Serbia (Paragraphs 28-38 of ZOMUKD). It is a particular type of punishment that includes deprivation of liberty of an elder juvenile, who committed a more serious criminal offence, for a certain period of time determined by a court decision[39]. The form of this punishment is comprised of the deprivation of liberty, which is similar to the prison sentence that the court imposes on adult offenders[40]. However, its purpose makes it seem closer to educational measures.

---

[38] I. Kos, *Izvršavanje maloljetničkih sankcija*, Hrvatski ljetopis za kazneno pravo i praksu, Zagreb, No.2/2006. pp. 807-826.

[39] D. Jovašević, *Maloletničko krivično pravo*, Beograd, 2011. pp. 173-186.

[40] The most serious punishment that can be imposed on juvenile offenders with identical characteristics and conditions of enforcement is present in numerous contemporary criminal laws: Paragraph 101. of the Criminal Code of the Republic of Montenegro, Paragraph 88 of the Criminal Code of the Russian Federation, Paragraph 63 of the Criminal Code of the Republic of Bulgaria.

Fundamental characteristics of juvenile prison sentence are the following[41]:

1) It is the most severe kind of juvenile criminal sentences and the only punishment that can be imposed on a juvenile offender. Nevertheless, this punishment cannot be imposed on any juvenile (but solely on an elder juvenile) and cannot be imposed for any criminal offence (but only for a more serious criminal offence for which the law prescribes more than five years' imprisonment),

2) This sentence is intended to accomplish preventive purposes (special as well as general), since its enforcement makes a more intense impact on a juvenile offender not to commit criminal offences in the future as well as on other juveniles not to commit criminal offences,

3) The enforcement of juvenile prison sentence requires two preconditions to be fulfilled: a) a committed criminal offence and b) a high degree of offender's guilt. This is the only juvenile criminal sentence that obliges the court to estimate the presence and the degree of offender's culpability when imposing it,

4) Juvenile prison sentence is determined according to particular rules. Among them, subjective circumstances related to offender's personality and objective circumstances related to the nature and the gravity of the criminal offence he committed are of special significance,

5) Juvenile prison sentence can be imposed in the period ranging from 6 months to 5 years. It is always determined in full years and months. Apart from this general maximum, the law is familiar with another maximum of 10 years' imprisonment. Juvenile prison sentence lasting up to 10 years can be imposed in two cases: a) when a criminal offence is committed, for which the law prescribes 20 years' imprisonment or a more severe punishment and b) when there is a joinder of at least two criminal offences, for which the punishment prescribed by the law exceeds 10 years' imprisonment. The duration of juvenile prison sentence is limited by the law and cannot exceed the punishment prescribed for the committed criminal offence,

6) In the case of joinder of criminal offences, juvenile prison sentence is determined in line with the following special rules[42]: a) If an elder juvenile has, by one act or several acts, committed several criminal offences for which he is tried concurrently, and the court finds that for each of the criminal offences a juvenile prison sentence should be imposed, the court shall, by its free judgment, determine a single juvenile prison sentence for all committed offences within the limits determined by the law, b) If the court finds that an educational measure should be imposed for some of the criminal offences committed by an elder juvenile, whereas a juvenile prison sentence should be imposed for the others, the court shall impose a single juvenile prison sentence for all the criminal offences in joinder, c) If the court determines a punishment of imprisonment and a juvenile prison sentence for criminal offences in joinder, the court shall impose a single punishment of imprisonment in line with the rules for the determination of punishment in the case of joinder of criminal offences committed by adult offenders (the "asperation" system-Paragraph 60, subpart 4 KZRS) and d) If the court estimates that for one of the criminal offences in joinder an educational measure should be imposed, while for the other a punishment of imprisonment should be imposed, the court shall impose a single punishment of imprisonment. The court shall act in the same way when determining a

---

[41] D. Jovašević, *New juvenile criminal law in the Republic of Serbia*, Free Law Journal, Budapest, No. 3/2006. pp. 181-198.

[42] M. Podrug, *Kriminalistička prevencija*, Policija i sigurnost, Zagreb, No. 3-4/2004. pp. 238-243.

sentence for a previously sentenced person (if after the sentence is pronounced the court finds out that the convict has committed another criminal offence before or after his sentence is pronounced),

7) Juvenile prison sentence does not cause legal consequences of conviction that include the prohibition to acquire particular rights,

8) Under the following conditions, the court may release on parole the person on whom juvenile prison sentence has been imposed[43]: a) if he has served one third of the imposed sentence, but not before a six months' period has expired and b) if the achieved results suggest that he can be expected to behave well while at liberty and that he will refrain from committing criminal offences. Along with the parole, the court can determine some of the measures of intense supervision with the possibility to apply one or more particular obligations. Such parole can be revoked in the manner and under the conditions prescribed for adult offenders,

9) Limitation on enforcement of juvenile prison sentence takes effect after expiry of: a) 10 years since juvenile prison sentence exceeding 5 year's period has been imposed, b) 5 years since juvenile prison sentence exceeding 3 year's period has been imposed and c) 3 years since juvenile prison sentence up to 3 year's period has been imposed,

10) Data on the conviction to juvenile prison sentence can be disclosed only to the following authorities enumerated by the law[44]: a) the court, the state prosecutor and the authority of internal affairs in respect of criminal proceedings conducted against a person with prior convictions, b) the body involved in the procedure of granting amnesty, pardon, rehabilitation or deciding on termination of legal consequences of conviction and c) social welfare authorities, when they need such data to discharge duties under their competence[45],

11) If the court imposes a juvenile prison sentence on an elder juvenile in the course of execution of an educational measure, the educational measure shall be suspended as soon as the execution of the imposed punishment commences. If the court imposes a juvenile prison sentence or a prison from 1 year on an adult offender in the course of educational measure's execution, the educational measure shall be suspended as soon as the execution of the punishment commences. But, if the court imposes a juvenile prison sentence or a prison up to 1 year, the court shall decide whether the execution of the educational measure should be continued after the punishment has been served or completely suspended,

12) The person on whom a juvenile prison sentence is imposed cannot in the course of serving perform electoral functions in state bodies, bodies of territorial autonomy, bodies of local self-government, administrative bodies, executive bodies or other bodies in companies and other organizations legally entrusted to carry out particular public functions,

13) Records on imposed juvenile prison sentences are kept by the Superior court that made the decision in the first degree and

14) Rehabilitation may be granted to a juvenile sentenced to juvenile prison sentence in the same way, under the same conditions and under the identical procedure as those prescribed for adults.

---

[43] D .Jovašević, *Krivično pravo*, Opšti deo, Beograd, 2018. pp. 320-323.

[44] D. Jovašević, *Krivične sankcije za maloletnike u novom krivičnom pravu Republike Srbije*, Bezbednost, Beograd, No. 5/2006. pp. 689-711.

[45] D. Jovašević, *Maloletničko krivično pravo*, Beograd, 2011. pp. 173-175.

2. Conditions for Imposing Juvenile Prison Sentence

Juvenile prison sentence is a "hybrid" criminal sentence. Its form corresponds to penal measures with emphasized repressive elements, whereas its contents, essence and aim make it more similar to educational measures. This criminal sentence was introduced to our criminal law in 1959 with the Amendments of Criminal Code of FNRJ (although imposing punishments on even younger juveniles under particular conditions was possible prior to these amendments)[46]. This punishment can be imposed if the following conditions prescribed by the law (Paragraph 28 ZOMUKD) are cumulatively fulfilled[47]:

1) the perpetrator is an elder juvenile i.e. a person who was between 16 and 18 years old at the time of commission,

2) the juvenile committed a criminal offence for which the law prescribes more than 5 years' imprisonment,

3) the juvenile committed a criminal offence with a high degree of guilt. Such grade of guilt stands above the common, ordinary or average degree of perpetrator's conscious and willing determination towards the committed criminal offence. Whether there is a high degree of guilt of an elder juvenile or not, represents a factual question solved by the judicial council in each individual case. The degree of guilt of such high level is not accomplished if there appear to be some of the subjective grounds for mitigation of punishment (such as substantially impaired mental capacity)[48] and

4) the court is convinced that, due to the nature and the graveness of the committed criminal offence and the high degree of guilt, imposing an educational measure would be inappropriate. The graveness of the criminal offence signifies a greater extent and a stronger intensity of injury or, by way of exception, threat of the protected value. This condition indicates the extent and the intensity of the consequences of the criminal offence. However, this circumstance should also be assessed in the scope of the type of the attacked value and society's need to provide its efficient protection, which indicates the nature of the criminal offence[49].

This condition[50] implies that juvenile prison sentence is imposed only as an exception even if the conditions prescribed by the law are fulfilled. Imposing a juvenile prison sentence requires court's assessment based upon personal and material sources of evidence, according to which the enforcement of an educational measure would not be appropriate in that particular case. Therefore, juvenile prison sentence is a subsidiary punishment and its enforcement is always optional. When the conditions prescribed by the law are fulfilled, the court shall determine juvenile prison sentence for an elder juvenile within the limits prescribed by the law for the committed criminal offence, taking into consideration all the circumstances (extenuating as well as aggravating) and especially: a) the degree of juvenile's maturity and b) the time that is necessary for his education and professional training (Paragraph 30 of ZOMUKD). Juvenile prison sentence imposed by the court cannot last

---

[46] B. Đukić, D. Jovašević, *Kriminalitet maloljetnika i mjere društvene reakcije u Republici Srpskoj*, Banja Luka, 2010. pp. 105-109.

[47] M. Đorđević, Đ. Đorđević, *Krivično pravo*, Beograd, 2016. pp. 98-102.

[48] D. Jovašević, *Krivično pravo*, Opšti deo, Beograd, 2018. pp. 322-323.

[49] I. Simić, M. Petrović, *Krivični zakon Republike Srbije – praktična primena*, Beograd, 2004. pp. 23-25.

[50] B. Čejović, *Krivično pravo*, Opšti deo, Beograd, 2002. pp. 559-562.

longer than the punishment prescribed for the committed criminal offence, but the court is not limited by the minimal measure of the prescribed punishment.

VII. Conclusion

Following the standards proclaimed by a series of universal and regional international documents that have been adopted lately (created under the auspices of The Child's Rights Convention), The Republic of Serbia adopted a special Law on Juvenile Offenders and Criminal Legal Protection of Juveniles in 2005. In that manner, substantial, procedural and executive aspects of the legal position of juveniles as offenders and victims of criminal offences were arranged in a single legal document.

That is the reason why our country conducted the codification of juvenile criminal law in a way similar to the one that other European countries such as: France, Germany, Croatia, Macedonia, Bosnia and Herzegovina and others have been applying in the past couple of years. That initiated an entire new chapter in the development of our country's criminal law in general and represented a radical twist in the establishment and the functioning of a modern legal state and rule of law. Juvenile criminal law is a part, i.e. a segment of criminal law that has lately been gaining the character of an autonomous legal branch and scientific discipline in numerous European countries due to a multitude of its specific solutions. It represents a particular, consistent and autonomous system of legal provisions containing a series of specific solutions that differ from those referring to adult offenders.

Juvenile criminal law is a system of legal provisions that determine the criminal legal status of juveniles (as offenders and as victims of criminal offences). So, this term, that legal theory often refers to as a criminal-legal postulate, represents a branch of law comprised of criminal legal provisions that can be applied to juvenile offenders and that depict its particular and specific character. It is a set of legal provisions that determine the system of criminal sentences for juvenile offenders (that can also be applied to adult offenders under particular conditions) as well as the procedure for the imposing and the execution of these sentences by competent state authorities.

Juvenile criminal law is familiar with two fundamental types of juvenile criminal sentences: a) educational measures and b) juvenile prison sentence. They are defined as measures of social reaction to juvenile offenders that are prescribed by the law and imposed by state authorities determined by the law (superior court-judge for juveniles and council for juveniles) with the aim to protect the society from crime through education, re-education and regular development of juveniles. Educational measures are the most common type of juvenile criminal sentences. They are most regularly and commonly imposed juvenile criminal sentences. They can be imposed on all juvenile offenders (younger as well as elder juveniles). Subsidiary, and only if the conditions prescribed by the law are fulfilled and when the court estimates that the aim of juvenile criminal sentences cannot be accomplished by the enforcement of educational measures, the court can impose a special type of punishment on an elder juvenile-juvenile prison sentence.

References

1. Arnaudovski, A., Nenev, L., *Juvenile Penal Code*, Kavadarci, 2001.
2. Bavcon, Lj., Šelih, A., *Kazensko pravo,* Splošnij del, Ljubljana, 1999.
3. Čejović, B., *Krivično pravo u sudskoj praksi*, Knjiga prva, Opšti deo, Beograd, 1985.
4. Čejović, B., *Krivično pravo*, Opšti deo, Beograd, 2002.
5. Đorđević, M., Đorđević, Đ., *Krivično pravo*, Beograd, 2016.
6. Đukić, B., Jovašević, D., *Kriminalitet maloljetnika i mjere društvene reakcije u Republici Srpskoj*, Banja Luka, 2010.
7. Hellmar, J., *Jugendkriminalitaet*, Darmstadt, 1978.
8. Hadžović, Lj., Babić, B., *Zaštita maloletnih delikvenata – priručnik za primenu vaspitnih mera pojačanog nadzora organa starateljstva*, Beograd, 1994.
9. Horvatić, Ž., *Kazneno pravo*, Opći dio, Zagreb, 2003.
10. Jovašević,D., *New juvenile criminal law in the Republic of Serbia*, Free Law Journal, Budapest, No. 3/2006.
11. Jovašević, D., *Krivične sankcije za maloletnike u novom krivičnom pravu Republike Srbije*, Bezbednost, Beograd, No. 5/2006.
12. Jovašević, D., *Maloletničko krivično zakonodavstvo i savremene tendencije krivičnopravne represije*, Zbornik radova, Bijeljina, 2010.
13. Jovašević, D., *Položaj maloletnika u krivičnom pravu*, Niš, 2010.
14. Jovašević, D., *Maloletničko krivično pravo*, Beograd, 2011.
15. Jovašević, D., *Krivično pravo*, Opšti deo, Beograd,2018.
16. Kos, I., *Izvršavanje maloljetničkih sankcija, Hrvatski ljetopis za kazneno pravo i praksu*, Zagreb, No.2/2006.
17. Marjanovik, G., *Makedonsko krivično pravo*, Opšt del, Skoplje, 1998.
18. Matić, O., *Ispitivanje ličnosti maloletnika kao osnov za određivanje vaspitne mere i tretmana u VP domovima*, Beograd, 1974.
19. Petrović, B., Jovašević, D., Ferhatović, A., *Izvršenje vaspitnih mjera*, Pravna riječ, Banja Luka, No. 7/2006.
20. Petrović, B., Jovašević, D., Ferhatović, A., *Krivično pravo* 2, Sarajevo, 2016.
21. Podrug, M., *Kriminalistička prevencija*, Policija i sigurnost, Zagreb, No. 3-4/2004.
22. Rutter, M., *Juvenile deliquency*, Harmondswort, 1983.
23. Sauer, W., *Kriminologie*, Berlin, 1950.
24. Simić, I., Petrović, M., *Krivični zakon Republike Srbije – praktična primena*, Beograd, 2004.
25. Vuković, J., Živković, M., *Izvršenje odgopjne mjere upućivanja u odgojni zavod*, Hrvatski ljetopis za kazneno pravo i praksu,Zagreb, No. 2/1999.

Some Controversies on Modern Terrorism

***Dr. Nenad Avramović*[1]**
***Dr Marijana Mladenov*[2]**

Abstract

Terrorism is the historical constant of the civilizing process of the development of human society. All the time the act of terrorism was characterized by violence, recklessness, fear production and the political goals of changing or preserving the existing model of social relations. The modus operandi of the manifestation of terror changed in accordance with the requirements of the time in which the changes in the technical and technological prosperity of society manifested and followed. As a socially destructive phenomenon, it has evolved from a national to an international global criminal act and as a multidisciplinary phenomenon is the subject of the study of political science, sociology, security, criminology, criminal law... The criminal laws of national legislations severely sanction terrorist acts without restricting the legitimate use of force as a means. Internationally, despite the significant codification of certain forms of terrorist acts, no consensus has been reached on defining this anti-globalization term. The absence of a universal definition, as the imperative international norm, is the resultant of the desire of the unipolar hegemon to interpret international law and relations in accordance with its own interests.

***Keywords**: terrorism, international law, double standards, terrorist offenses, human rights*

I. Introductory Remarks

The thesis that terrorism has always been a determinant of the history of civilization is more or less generally accepted axiom. It is undisputed, too, that terrorism presents a security threat with a destructive desire to disrupt (which is the majority accepted view) or to provide a valid social system of relationships. One of the contradictions of the concept of terrorism, which the authors will elaborate in the paper, is the thesis that the means and methods of expression have changed and depended on the historical circumstances and the scientific and technological level of development of society.

The international effects and aims of the terrorist acts were also present in the early development of civilization and the fight for freedom and state sovereignty. However, globalization processes, which are intensified in the 20th century and further accelerated by the use of information technologies have further internationalized terrorism, giving it the epitome of a global phenomenon. The media's contribution to the "promotion" of

[1] Faculty of Law for Commerce and Judiciary in Novi Sad, University Business Academy in Novi Sad. Contact: avramovic.n@pravni-fakultet.info.

[2] Faculty of Law for Commerce and Judiciary in Novi Sad, University Business Academy in Novi Sad. Contact: alavuk@pravni-fakultet.info.

terrorism often exceeds the awful consequences which are produced by terrorist acts. Therefore, not without reason, the question arises – whether the public media word is in function of international public and human interest or the destructive goals of the terrorist actors.

It is an indisputable thesis in both legal doctrine and jurisprudence that a terrorist act is violence committed with a politically motivated intention to produce fear of a larger target group, including the general instability of a narrower or wider social group, including the international community. Also, in all national criminal justice systems, terrorism is one of the most serious crimes. In line with the societal danger of terrorist acts, even the most serious criminal sanctions are prevented. However, despite the general consensus at the national level of terrorism as a destructive phenomenon, where is a clear tendency to preserve the existing system of social relations, at the international level there is no universally accepted definition of terrorism.

In this paper we will try to answer the question why, although it is a global phenomenon, there is no universally defined concept of terrorism, despite the fact that it destructively affects the realization of human rights and freedoms as universal internationally accepted values. Of course, this will require an analysis of the causes of the emergence of terrorism, which, in addition to the political, often have their military, religious, ethnic, economic and social dimensions. We will also talk about the phenomenon of terrorism as a kind of resistance to globalization, which imposes an unconditional acceptance of Western stereotypes and renunciation of national and cultural identity, religious and historical genome with increasingly drastic economic stratification to positions rich North – poor South. Of course, in order to present these and some other controversies that accompany contemporary terrorism, we will first look at its historical development.

II. Terrorism Through the History of Civilization

The historical roots of terrorism, despite its temporal distance and inadequate sources, are seen by many authors as a manifest form of resistance to the ancient tyrannies of the Greek and Roman states. Thus, Luis Rene Bere notes that terrorism is an appearance older than the ancient civilizations of Greece and Rome, and provides an example of the assassination of Gaius Julius Caesar by Marcus Brutus, a Roman noble and politician, 44 BC, and examples of the Sicarli religious sect and the struggle Zilota (a Jewish sect that openly fought Roman rule in Palestine from about 6 BC to the fall of Jerusalem), and acts of secret large-Islamic armed groups in the 12th and 13th centuries[3].

The activity of the Tagi religious sect in the seventh century appears to some authors without sufficient argument as a precursor to terrorism. The violent Hindu sect of Tagi represents a religious group that used violence, namely robbery, and the victims of the robbery were sacrificed in honor of the goddess Kali. An analysis of the workings of the tags provided by outstanding British sources gives a comprehensive and reliable insight into not only their ritual actions, customs, lifestyles and content of

[3] Louis Rene Beres: *Terrorism and Global Security: The Nuclear Threat*; Westview Press / Boudler, Colorado, p. 8 Cited by R. Gaćinović, "Roots of Modern Terrorism," Legal Life, Journal of the Association of Lawyers of Serbia, Belgrade, no. 9, 2005, page 60.

the moral code, but also their criminal activities[4]. However, the activity of the sect indicates religious fanaticism, which is an integral part of modern terrorism, the indoctrination and recruitment of terrorists today. By the way, the British Empire, to which Tagi had inflicted political instability and economic losses, devastated the Tagi group after several centuries of persistent struggle.

In the nineteenth century, the Assasini or Hashashini[5] religious sects operated for almost two centuries in Iran, whose military-political goals were to conquer Baghdad and the surrounding regions, based on religious fanaticism and drug use. Members of the sect were recruited from the poorest sections of the society, and through the process of irresponsible religious affiliation and obedience, with drug addiction, they became fanatical killers who, through assassinations and robberies, for the purpose of obtaining property gain, built up their social status. Their religious extremism introduced martyrdom into practice, but the sect's activities, despite some common features, cannot be identified with modern-day terrorism. Because, the motive for joining a sect was not only religious fanaticism based on religious doctrine, but the "boon" of drug addiction and worldly indulgence.

III. On Religious and State Terrorism

In addition to these instances of religious terrorism of particular groups that have emerged within Judaism, Islam, and Hinduism, history also record the emergence of religiously inspired institutionalized terror. An example of this is the Inquisition of the Catholic Church in the Middle Ages[6]. The Inquisition was first introduced as a religious legal institute by Pope Lucy III in the twelfth century as a means of combat against heretics, or persons who deviate from the official teaching of the Catholic Church. The inquisitors had the right to find, accuse and convict persons suspected of heresy and to use cruel torture by integrating both investigative and judicial functions in their activities. Thus, until the second half of the eighteenth century, history records events interpreted as a kind of precursor to terrorism, based on religious extremism and the religious policies of radically militant social groups.

Denominatal terrorism (or as many call it religious) is carried out by religiously blinded terrorist groups based on religious indoctrination. The goal of religious fanatics is to fundamentally change the ruling social-political relations and establish a state-political system on religious grounds. It is manifested as terrorism by fanatic groups that carry out terrorist acts to establish religious values in society[7].

All of the manifested forms who are considered to be precursors to acts of terrorism have taken place without the concept of terrorism being recorded in political doctrine and national legal systems. The emergence of this term, according to

---

[4] Simenunović, D.: *A Critical Review of the Determination of the Time of the Emergence of Terrorism and Its Precursors "*, Military Work, No. 1. page 315.

[5] The Hashishini sect was founded by Hasan Ibn Sabah, who introduced himself as God's envoy on Earth, with the intention of pursuing military-political goals, with strict adherence to religion and enjoying hashish.

[6] Dictionary of Middle Ages ed Joseeph R. Stayer (New York: Shareles Scribner,s Sons. 1985)p. 483-489.

[7] Italian M.: *Security Management in Countering Terrorism and Combating Terrorism*. Media Center Defense, Belgrade, 2012, page 39.

some authors[8], refers to the French bourgeois revolution of 1789 as a repressive means of the newly constituted authority established to restore public order in the post-revolutionary years. The new revolutionary government of Robespierre and Mara carried out acts of terror from the positions of state authorities, which suggests that this was state terrorism. Thus, the political motive of the new Jacobin government was to preserve the social-economic and political system of newly established relations, and the means of protection by its repressive threats and fears of terrorism were dubbed terrorist[9]. Terrorist measures were also applied during the American struggle for independence from the British Crown and against the British, as well as their sympathizers among the colonists. Terrorism, which until then was mainly related to political non-supporters of the current government, is taking on a new dimension – terrorism on behalf of the state.

Assassination, as a powerful political weapon introduced into the Assassini criminal practice throughout the Middle Ages, was again promoted in the second half of the nineteenth century, but now by anarchists, who gave it an international dimension. "With the advent of the new century, the nursery of international terrorism became imperial Russia, while the second focal point was Barcelona, where more than 80 explosive devices exploded between 1903 and 1909. In response, the government is following the strengthening and modernization of police forces and a tougher immigration policy[10].

Recent history has also brought to light the examples of terrorism owed to Israel, Cyprus, Kenya and Algeria for their independence, as the political movements of these countries used terrorism against the colonial authorities. The Palestinians had launched rebellions against the British authorities before World War II, led by the Jewish terrorist organizations Irgun and Stern Gang. There were no rebellions during the war, but as early as 1944, three simultaneous bombings took place, and in 1946 the King David Hotel was mined, where the central office of the United Kingdom was located. These actions achieved their goal. The whole world paid attention to the struggle of these groups for independence, which aroused pity and support from powerful allies, which led to the end of Britain's rule over Palestine in 1948 and the establishment of the State of Israel[11].

In the aftermath of World War II, terrorist acts are dubbed international and often become a strategy and a means of combat for political interests. Terrorist interventions are extremely violent, targets are unpredictable, targets are innocent people, acts with numerous victims and are adequately publicized by the media, and political motives with a wide variety of weapons and weapons of mass destruction with intention to cause fear.

When it comes to terrorist organizations, there is a steady increase in the number of individuals and organizations willing to carry out terrorism. Since the 1990s, recruitment of terrorists around the world, the establishment of terrorist training camps, the unification of militant groups in Indonesia, the Philippines, Singapore,

---

[8] Hoffman Bruce: *Domestic Terrorism*, Alpha National Book, Belgrade, 2000, page 11.

[9] During the first few years of the Jacobin rule, led by Robespierre, nearly 40,000 French aristocrats ended up on the guillotine.

[10] Hanhimaki, J.M.: Blumenau, B.: *An International History Of Terrorism – Western and Non – Western Expiriences,* Oxon; Routledge, 2013., page 353.

[11] centar za bezbednost.org/terorizam-osnove-i-nastanak/.

Malaysia, Thailand and Myanmar has been evident. There is a tendency for terrorist organizations to organize online. The best example is the "Al Qaeda" terrorist network. "Al Qaeda" terrorist cells are located in Southeast Asia, where there is the largest concentration of "Al Qaeda" members outside the borders of Afghanistan and Pakistan, in which its stem cells are located. "Al Qaeda" operative terrorist cells are located in 35 countries around the world[12].

Finally, the "Al Qaeda" terrorist action on September 11, 2001 in the United States, has added to the modern terrorism the epithet and the global plagues of the modern world. The terrorist attack was accompanied by official representatives of the United States authorities, symbols of their world economic and military power, as well as other countries of Western neo-imperial domination, so that terrorist actions did not bypass Germany, Japan, Britain, France and Spain. The terrorist attacks have not bypassed the Russian Federation or traditionally unstable regimes in the Middle East.

IV. Definition of Terrorism

As a historical category, terrorism is the result of the social, political, religious and economic determinants that generate its emergence. The violence of terrorism as a civilization constant in different epochs has been interpreted differently, so depending on the ruling political stance, it has been a criminal event, a war of aggression or a liberating battle. The political context as the cause of the event, which should cause fear, of the projected goal as a consequence and of course of interpretation, was undeniable. Hence, terrorism has its linguistic, political, criminological, security, criminal and, more recently, international dimension.

Etymologically, the term terrorism is rooted in the word *terror*, which is Latin, in origin, meaning to cause fear, trembling, horror, and violence, while terrorism signifies the pursuit of terror, tyranny, and control of intimidation[13]. In most of the world's leading languages, such as English, French, Russian and German, terrorism is defined by the terms of perpetration of violence or terror driven by political goals.

The multidisciplinary notion of terrorism in any of the sciences that study it has no diametrical positions in its definition. Such a political definition of terrorism states that it is "an act of violence undertaken for political reasons to intimidate and mercilessly break the resistance of the one targeted"[14]. From the criminology point of view, terrorism is "the doctrine, the method and means of inciting fear and insecurity in the citizens through the systematic application of violence for the pursuit of political ends"[15].

Similarly, terrorism is defined as a security phenomenon, with state authorities being mentioned as potential perpetrators. It is "a method of devising systematic use of violence for the sake of spreading fear among people, implemented by state authorities or organized groups to achieve specific political goals."[16] As a pragmatic science, criminology looks at terrorism as a criminal activity, that is, "a form of

---

[12] Bošković M.: *Criminological Lexicon*, Matica Srpska and University of Novi Sad, Novi Sad, 1999.
[13] Vujaklija Milan, *Lexicon of Foreign Words and Expressions*, Education, Belgrade, 1970. page 947.
[14] Political Encyclopedia, Contemporary Administration, Belgrade, 1975, page 1079.
[15] Bošković, M., *Criminological Lexicon*, Matica Srpska, Novi Sad, 1999, page 354.
[16] Djordjević, O., *The Lexicon of Security*, Partisan book, Belgrade, 1989, page 482.

organized criminal activity characterized by the commission of acts of violence, the execution of assassinations and abductions, the setting up of explosives and fires and the taking of dangerous acts"[17].

Given that contemporary terrorism has acquired the attribute of international, it defines the doctrine of international law as "a form of political struggle conducted through individual terror, that is, violence and intimidation, which goes beyond the borders of a state"[18].

V. Academic Definitions of Terrorism

Certainly, the definitions of terrorism are derived from the research efforts of the theorists of the social sciences i.e. sociologists, political scientists, criminologists, experts in international law, criminal law... In addition to the characteristics of the scientific – theoretical field that defines them, they also carry the individualities of their creators. But, despite the differences arising from the multidisciplinary nature of the institute, which has the widest range of manifestations, both nationally and internationally, terrorism has essentially the same defining premises.

So theorist Petit Robert says "Terrorism is the use of violence to achieve political effects, individual or collective assassinations, overthrows in the form of conquering, preserving or exercising power directed by certain political bodies that seek to produce fear and insecurity"[19]. Professor at Georgetown University and Former senior RAND Corporation manager, both theoretically and practically concerned with terrorism, Bruce Huffman under terrorism means "intentionally creating and exploiting fear by violence or threatening violence to effect political change"[20]. Western theorists of terrorism, while respecting the unrestricted manifestation of acts of terrorism, have generally provided concise and general definitions. And Walter Laqueur from the Center for Strategic and International Studies in the United States also states that terrorism is "an unlawful use of violence, which causes panic and accomplishes political goals and innocent people represents target of attack"[21]. In international theory, however, there have been scholars who have tried to sublimate the constituent elements of terrorism and accurately demonstrate their involvement and significance in this deviant phenomenon.

Alex Schmit, one of the world's leading researchers on terrorism and violence, sought to formulate a consensus-based academic definition of terrorism in the early 1980s by analyzing 109 academic definitions, extracting key elements from them: Violence 83.5%, political component 65%, fear 47.5%, psychological effects 41.5%, victim-goal differentiation 37.5%, planned systematic action 32%, strategy, method of combat 30.5%, contempt rules 30%, extortion of consent, coercion 28%, publicity 21.5%, arbitrariness, random character, non-discrimination 21%, civilians, outsiders as victims 17.5%, intimidation 17%, expressed innocence of victims 15.5%,

---

[17] Aleksić, Z., Milovanović, Z., *Lexicon of Crime*, Vrelo, Belgrade, 1995, pp. 301-302.

[18] Mrivokapić B., *Lexicon of International Law*, Official Gazette, Belgrade, 2010, page 1064.

[19] White, R. Johnson: *Terrorism* (Translated by Roksanda Cirović), Alexandria Press, Belgrade, page 42.

[20] Hoffman B.: *Inside Terrorism*, Columbia University Press, New York.2006, p. 40.

[21] Walter Laqueur, *Postmodern Terrorism*: New Rules for an Old Game, Forin Affairs, 1996, pp. 340-341.

collectivity, organization as executor 14%, symbolic aspect, demonstration to others 13,5% unpredictability, suddenness of violence 9%, covert nature 9%, repeatability, incidence of violence 7%, crime 6%, demands placed on third parties 4%[22].

Given that the political component of terrorism is the dominant motive for executing, the greatest number of academic definitions has been provided by the authors of the political province. Thus, Simeunović defines terrorism as a multidimensional social phenomenon as "a complex form of organized group and less frequent individual or institutional political violence characterized only by frightening brachial physical and psychological, but also sophisticated technological methods of struggle, which are usually in times of political and economic crises, and rarely in conditions of achieved economic and political stability of a society, systematically try to achieve "big goals" in a morbidly spectacular way, and inappropriately given conditions, above all the social situation and historical possibilities of those who use it as a political strategy[23].

Of course, the point of view of jurists also starts from the most important elements of the concept of terrorism, with each author starting from the aspect of view that is the subject of his interest in defining the phenomenon. Thus, Vojin Dimitrijević under terrorism considers "an act of physical violence, which object is chosen to provoke strong psychic reactions, first of all fear, in a wider circle of people, in the hope that they will help to maintain or change behavior that is important for achieving a political goal, if such an act is not justified by the general interests that are determined independently of it and if it is not executed according to the rules normally applicable to the social aspects of the exercise of power"[24].

According to criminologist Djordje Ignjatović, terrorism is "a form of struggle by social groups that do not have the power to influence social movements or at least not by the way it is defined by positive law"[25]. Criminal law dimension has the statement "Terrorism is a form of political crime characterized by the use of violence against civilians in the intention of intimidating the public and political decision-makers and forcing them to act or abstain in order to fully or partially achieve political or other social goals"[26].

There are, therefore, no diametrically opposed opinions on the academic definition of terrorism. Although there is no generally accepted definition in the international scientific public, the formulation put forward by Kaseze as the "acceptable definition" of international terrorism has been rather differentiated: "A crime committed in order to provoke a state of fear in the public, among groups of people or certain individuals from political initiatives, for which it has no justification under any circumstances whatsoever, regardless of the political, philosophical, ideological, racial, ethnic, religious or other views which may be invoked for its legitimacy"[27].

---

[22] Simeunović, D.: *Terrorism*, Edition Krimen, Belgrade, 2009, page 25.

[23] Simeunović, D.: *Terrorism*, Second Edition, Faculty of Law, University of Belgrade, Belgrade, 2009, page 80.

[24] Dimitrijević, V.: *Terrorism*, Workers' Press, Belgrade, 1982, page 37.

[25] Ignjatović, Dj.: *Criminology* (Eighth Edited Edition), Official Gazette, Belgrade, 2007, p. 283.

[26] Milošević, M.: *Terrorists: Victims and Criminals – Factors of Criminal Motivation*, University of Belgrade-Faculty of Security, Belgrade, 2009, page 48.

[27] Kaseze, A.: *International Criminal Law*, Belgrade, Belgrade Center for Human Rights, Belgrade, 2005, page 449.

Positive-legal solutions to the criminal legislation of more or less all countries in the world also hold such views. Thus, the Federal Law on Counteraction against Terrorism of the Russian Federation states: "terrorism denotes the ideology of violence and the practice of influencing decision-making by state authorities, local governments or international organizations related to intimidation of the population and / or other forms of illegal acts of violence"[28].

The US criminal law regulations define terrorism as “an activity involving the use of violence or acts of danger to human life, which violate the criminal laws of the United States or of the States and are intended to: a) intimidate or coerce the civilian population; b) influence government policy through intimidation and force politics; and (c) influence the exercise of authority by means of massacres, assassinations or abductions"[29].

The UK Terrorism Act, which, like the US, is one of the most common targets of terrorist attacks, provides similar criminal justice solutions. Terrorism means "The use or threat of taking an act to influence a government or an international organization through intimidation of the wider or only part of the public for political, religious or ideological reasons, and such action implies or causes the following: serious violence against persons; great material damage; endangering human life; serious health risk and security threat to the public, or serious interruption or interruption of the electronic system[30].

The Criminal Code of the Republic of Serbia also interprets the crime of terrorism in a similar way. Article 391 “who intends to seriously intimidate the population, or to compel Serbia, a foreign country or an international organization to do something or not to do it, or to seriously endanger or violate the basic constitutional, political, economic or social structures of Serbia, a foreign country or international organizations: 1) attack the life, body or freedom of another person; 2) abduct or take hostages; 3) destroy a state or public facility, traffic system, „common good or private property in a way that could endanger people's lives or cause significant damage to the economy; 4) hijack aircraft, ships or other essential transportation or carriage of goods; 5) manufactures, possesses, procures, transports, supplies or uses nuclear, biological, chemical or other weapons, explosives or radioactive materials or devices; 6) discharges dangerous substances or causes fire, explosion or flood...; 7) interrupts or suspends the supply of water, electricity or other basic natural resources that may endanger human life"[31].

Even from a superficial comparative analysis of the above mentioned positive national criminal law formulations of terrorism, it follows that mandatory constitutive features of the crime are present in all laws. Reasons for different legal determinations are the product of specific national interests and the aspirations of states to sanction certain behaviors, while not only limiting the legitimate use of force in the suppression of terrorist activities. Often, due to the international dimension of

---

[28] Federal Anti-Terrorism Law No. 35-F 2006/2014, Russian Federation. http://legislationline.org/topics/country/7/topic/5/04.03.2020.

[29] 18 USC Ch.113B:TERRORISM, Internet: uscode.house.gov/view.xhtml?path=prelim@title18part1/chapter113B&edition=prelim.

[30] Terrorism Act 2000, (Internet: http://www.legislation.gov.uk/ukpga/2000/11contents, 04.03.2020.

[31] Article 391 paragraph 1 of the CC of Serbia, Official Gazette of the Republic of Serbia No. 85 / 2005, 88 / 2005,107 / 2005, 72/2009, 111 / 2009,121 / 2012, 104/2013, 108/2014, 94/2016, and 35 / 2019.

terrorist activities, their "operational" definition is based on the practical measures taken by the competent services of some countries.

Thus, the US Federal Bureau of Investigation (FBI), as the leading federal counterterrorism, criminal investigations and counterintelligence service, refers under the terrorism "international violent offenses committed by individuals and / or groups inspired or affiliated with certain foreign terrorist organizations" or "States", while domestic terrorism means "violent crimes committed by individuals and / or groups for the purpose of effecting ideological changes of a political, religious, social, racial or environmental nature that carry other domestic options"[32]. The interesting thing is that "its own" definitions of terrorism has The US Department of Foreign Affairs, the US Department of Defense, and even have the US Army counterterrorism manual. Each of these administrative definitions starts from its own competencies and tasks in the fight against terrorism dictated by the national strategy and interests of the United States.

VI. Terrorism as an International Phenomenon

In the late nineteenth and early twentieth century, the assassinations of prominent statesmen in Europe and in America were the dominant *modus operandi* of anarchist groups and individuals. The assassination of Yugoslav king Aleksandar Karadjordjević, which took place on October 9, 1934. in Marseille by the Ustasha movement and the pro-Bulgarian wing VMRO one of the first classic acts of modern international terrorism. In November 1937, the League of Nations adopted two conventions on the prevention and punishment of terrorism in Geneva, but they did not enter into force because they were not ratified by the requisite number of states, and soon the World War II began, which put international terrorism aside.

The entire development of international criminal law is related to the constitution of the international community, and the first international criminal justice experience for the work of *ad hoc* military tribunals in Nuremberg and Tokyo sentencing German and Japanese generals charged with war crimes, crimes against peace and crimes against humanity committed during World War II. The United Nations codification activity in the post-war years resulted in the adoption of the Convention on the Prevention and Punishment of the Crime of Genocide (1948) and the Geneva Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva Convention II for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Geneva Convention III Relative to the Treatment of Prisoners of War, Geneva Convention IV Relative to the Protection of Civilian Persons in Time of War (1949)...

History, therefore, confirms that the formation of criminal international law legislation has arisen as a result of a severe disruption of international order. The rule that international crimes and criminal behaviors are *post festum* styled as prohibited conduct in international instruments is present in the decades-long practice of the United Nations. An egregious example is the beginning of the work of the International Criminal Court, the establishment of which has taken more than half a century of work by the UN Commission on International Law. The formation of the Court was initiated

[32] FBI Official Website, (Internet: http: //www.fbi.gov/albuquerque/about-us/what-we-investigate, 03/04/2020).

after the Second World War, and the Court began operations in 2003 without leading States of the world, United States, China, Russia, India, and a number of others have not ratified the Rome Statute and thus neither accepted the jurisdiction of the Court nor enacting legislation.

The creation of a universal international counter-terrorism treaty law was even more inefficient. Although resolution 177/II was adopted at the UN General Assembly in 1947, ordering the International Law Commission to make draft of a crime against peace and security of humanity, no international consensus has been reached to date on defining terrorism or a general treaty on anti-terrorist *ius cogens* content has been adopted. However, frequent terrorist offenses committed in aircraft were the reason for the adoption of the 1963 Tokyo Convention on Offences and Certain Other Acts Committed on Board Aircraft, and the 1971 Convention on the Suppression of Unlawful Hijacking of Hague Aircraft and the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation adopted in Montreal in 1971. By adopting these conventions *stricto sensu*, a global anti-terrorist codification of the regulations governing air traffic misconduct has been carried out.

When Western diplomats became targets of assassins, it was a signal that a UN Convention on the Prevention and Punishment of Crimes against Persons enjoying International Protection, including Diplomatic Agents, should be adopted within the UN. Until the 1970s, diplomatic and consular representatives of the SFR Yugoslavia were the targets of the assassination of Ustasha emigration, with international western power centers explaining it as the activity of political dissenters, rejecting the demands of Yugoslav diplomacy to pass a special convention on the protection of diplomats. Similar motives were the reason for the adoption of the 1979 International Convention against the Taking of Hostages, the 1997 Convention on the Suppression of Terrorist Attacks, the 1999 International Convention for the Suppression of the Financing of Terrorism, and the 2005 International Convention for the Suppression of Acts of Nuclear Terrorism.

Unlawful behavior in international relations is manifested not only through armed conflicts, but also through various forms of discrimination. Although the UN Corps of International Documents on Human and Civil Rights passed after the end of World War II, it took more than 20 years to adopt the Convention on the Elimination of All Forms of Racial Discrimination (1965) and the Convention for the Suppression of the Punishment of the Crime of Apartheid (1973). And, the Declaration for the Prohibition of Trafficking Black People was passed in 1815 at the Congress of Vienna, and the adoption of international rules guaranteeing racial and any other equality of people would endanger the economic interests of the leading colonial forces of the 19th and 20th century. Hence the "delay" with the adoption of the above mentioned acts.

The impact of regional international organizations on the creation of anti-terrorist regulations are also present but not effective enough. In 1977, the Council of Europe adopted the European Convention on the Suppression of Terrorism[33], and in 2003 the First Additional Protocol expanded the catalog of incriminations to deny the character of a political offense and a politically motivated crime and to simplify the procedure for amending the Convention[34]. The Council of Europe adopted the new

[33] The Convention has been ratified and- Official Gazette of the FRY – International Treaties No. 10/01.

[34] See more in S. Mijalković, M. Bajagić, On the Amendments to the Provisions of the 1977 Convention on the Suppression of Terrorism, page 485.

Convention on the Prevention of Terrorism in 2005 and obliged States to amend their criminal legislation by criminalizing part of the preparatory actions for committing the act of terrorism. The Council has not adopted a unique definition of terrorism, and its efforts to unify anti-terrorist regulations across Europe have more political than legal scope. Within the European Union, there is a consensus on the fight against terrorism, but it is also more a political guideline than a peremptory norm. The EU Council Framework Decision on Combating Terrorism laid the foundations for the criminal law notion of terrorism and the main manifestations of manifestation as a starting point for harmonizing the substantive criminal law of the Member States of the Union.

Although the UN has the international legal capacity to pass imperative regulations and in the field of counterterrorism, which would achieve unification on a global level, it did not go beyond political consensus.

UN Security Council Resolution 1377, adopted in 2001, states: "The Security Council, represented at the ministerial level of member states, declares that acts of international terrorism present a challenge to all states and to humanity... that acts of terrorism everywhere threaten the dignity and security of people, undermine social and the economic development of all states and on a global scale undermine stability and prosperity, "and that the Security Council is" concerned about the recorded rise in terrorist acts in different world religions, motivated by intolerance and extremism"[35].

VII. Interests Interference to the International Consensus

The reasons why the international community has not adopted a unique universal definition of terrorism are complex. First of all, it is a social phenomenon that represents a historical dialectical social phenomenon whose manifestation forms are dictated by general social relations, first on the internal, but also on the regional, and today, on the global level. Second, the level of technical and technological progress dictated forms of manifestation of terrorist acts, but temporal constants have always been violence as a method of arousing fear and achieving a political goal as the ultimate intention of the perpetrator. Third, terrorism is a multidisciplinary institute and as such is the subject of political science, sociology, criminology, security sciences, criminal law... and each of these scientific disciplines treats it in accordance with its value judgments, which make a compromise definition objectively very complicated.

Fourth, by *default*, terrorism means the violent activity of an individual or marginal social group directed by the impetus of the existing state system. However, the history of civilization *per se* is full of examples of the fact that sovereigns for the sake of survival in power often applied terror to their own people or to the people and countries they subjugated. The use of terror as a mode of government, typical of some autocratic regimes, raises the question of the existence of the state, that is, political terrorism, and Walter Laqueur points out with the reason that "acts of terrorism perpetrated by police states and tyrannical authorities, in general, have killed thousands of times and caused more damage than all the pieces of individual terrorism combined"[36]. This observation is certainly true from the point of view that

[35] Gaćinović, R., *Terrorism*, Draslar Partner, Belgrade, 2005, page 47.
[36] Laqueur Walter, *The Age of Terorism*, Boston: Little, Brown Co. & Co. 1987, page 146.

even the smallest state, with its coercive apparatus, has far greater potential terrorist capacity than the most organized terrorist groups. But on the other hand, it opens up a philosophical-political dilemma: if the undemocratic government emerged through a legitimate electoral process, who has the moral right to challenge the legality of acts of state bodies, except for the electoral base. Another form of state terrorism, in the broader context, is to provoke and even participate in low-intensity conflicts in other countries to achieve certain political or economic goals. These activities are generally secret because they are contrary to international law. In the event of a "break-in", a country that has engaged in terrorist activity will display it in front of the domestic and international public, depending on the situation, or as a legitimate act of war or retort. Of course, the role of the global media in the world will be to justify the intervention taken to protect democratic values and fight against terrorism. And, precisely, the policy of the double standards of the world's leading powers is one of the key reasons why no international consensus has been reached on establishing a generally accepted notion of terrorism.

Although terrorism is formally condemned by everyone in the world, in practice it has been confirmed that terrorism is nevertheless an effective weapon for achieving the political goals of particular national communities. History recalls that the UN organization formally condemned the operation of many terrorist organizations in the world, but the great powers did not always respect international law, because at some point they supported and strengthened the activities of terrorist organizations in many regions. Terrorist organizations are being unfairly treated as liberationists, with mass publicity creating a skewed opinion in the world. In this way, concrete assistance is provided to terrorist organizations, and the victim country is declared a creature of terror. This deprives her of the legal and legitimate right to fight terrorism in her territory. This is the case with the “KLA” and the “ANA” in Kosovo and Metohija. If this trend of double standards continues, the threat of modern terrorism will increase dramatically in many countries in the world"[37].

Finally, did the path of development of the greatest 21st-century terrorist, Osama bin Laden, who was a United States project during the Taliban's struggle against Soviet influence and founder of “Al Qaeda” and then became the largest US opponent, not *exempla docent* that terrorism is desirable while pursuing in goal of pursuing the interests of the great. And it was precisely Bin Laden and the terrorist attack on the United States on September 11, 2001 directed by him that led to the US declaration of a global war on terror, based on state retaliation. Anti-terrorist war involves preventive and repressive military action on the territory of states that cannot independently eliminate the terrorist threat, and often is the way to bring down undemocratic regimes in those countries. Such military interventions are, as a rule, acts contrary to international *ius cogens* norms that cause "collateral" innocent human casualties and great material damage. Thus, among other things, the absence of a universal definition, as an imperative international regulation, presupposes the supremacy of the great powers and the violent change of situation in international relations in accordance with their own interests, with "minor" disrespect for international law.

The global war on international terrorism is a kind of *cintadictio in adjecto*, as it threatens the basic values of the liberal democratic society of the West. The modern

[37] Gaćinović R.: *Why Terrorism is Hard to Define*, Proceedings of the Synergy Scientific Conference, Bijeljina 2010, page 430.

democratic state of the West is committed to respecting fundamental human rights and freedoms, multiculturalism and minimalist regulatory authority of national institutions in organizing the social community. However, in order to protect the individual from security terrorist risks, the modern Western state neglects and does not respect the fundamental human rights of freedom, privacy and the right to diversity. For example, "4.2 million surveillance cameras or one camera per 14 people have been set up in the UK. The world is gradually becoming a global "*Big Brother*" in which there will be absolute control and surveillance over each individual. If this tendency continues, Beck states, in the country of the Statue of Liberty, as well as in other democratic countries, there will no longer be unattended phones, uncontrolled emails or generally uncontrolled individuals. Today, justification is anti-terrorism, but such an expansion of power can, at any time, be applied to all other possible purposes"[38].

Therefore, the modern anti-terrorist struggle derogates from the universal human rights, not only of terrorists, but also limits the rights of ordinary citizens to potential victims of terrorist acts from developing countries. In this way, the protagonists of mondialism and universal rules negate the neoliberal concept of the development of the modern world based on the assumption of the universally accepted civilizational values of the West. Globalization is an ideological concept that, through the construction of a new international world order, has resulted in the creation of an even greater gap between the developed and rich North and the underdeveloped and poor South. The consequence of the unfair distribution of world wealth is based on universal standards that ensure the hegemony of the Western world. Building standards threatens the economic and social, and then national, linguistic, cultural, and even religious, historical identity of "small" nations and states. If there is resistance to the "democratic" acceptance of general civilization standards, they are ultimately imposed by force and produce marked inequality in the North-South relation, which some authors call neo-colonialism. Undoubtedly, one of the most extreme forms of resistance to globalization is terrorism as a socially deviant phenomenon.

VIII. Concluding Remarks

Terrorism is, no doubt, a socially deviant phenomenon in the history of human society. As such, in accordance with social circumstances and time of manifestation, he changed his *modus operandi*, but his violence, unscrupulousness, production of fear and political goals were and remain a constituent element of the term. With the development of science and technology and the intensification of international relations, it receives, in addition to the national, the epitome of an international social problem. As political science, sociology, criminology, criminal law, security science, international law are involved in terrorism... it is evident that this is a multidisciplinary social phenomenon. In addition to the constituent features of the crime, national criminal legislation contains specific forms of manifestation and does not limit the legitimate use of force in the suppression of terrorist activities. Modern

[38] Brčić Marita: *Terrorism and the Liberal Democratic State*, Proceedings of the Faculty of Philosophy in Split, 2007, page 16.

terrorism has become a global phenomenon today, but at the international level, despite the efforts of international organizations, no consensus has been reached on a generally accepted definition. The leading world powers with US on the lead, codify certain types of terrorist acts under international treaties, but avoid adopting *ius cogens* rules that would uniquely define the term terrorism. In the absence of universally accepted imperative norms of superpower, international law is interpreted in accordance with its political and economic interests, thereby creating a policy of double standards.

Descriptively describing contemporary terrorism (including state) and as an anti-globalization act, Noam Chomsky, alluding to US imperialism, describes in his work[39] the encounter of Alexander the Great who "haunts the whole world" and the ordinary sea pirate who "haunts one small sea", pointing out that the difference is between the two, only in the fact that Alexander the Great conquers the world with a large fleet, which makes him emperor, and the other an ordinary pirate ship, which makes him an "ordinary scoundrel".

References

1. Aleksić, Ž., Milovanović, Z., *Lexicon of Crime*, Vrelo, Belgrade, 1995.
2. Beres Louis Rene: *Terrorism and Global Security: The Nuclear Threat*; Westview Press / Boudler, Colorado, p. 8 Cited by R. Gacinovic, "Roots of Modern Terrorism," Legal Life, Journal of the Association of Lawyers of Serbia, Belgrade, no. Sep 9, 2005
3. Bošković, M., *Criminological Lexicon*, Matica Srpska, Novi Sad, 1999.
4. Brčić M., *Terrorism and the Liberal Democratic State*, Proceedings of the Faculty of Philosophy in Split, 2007.
5. Chomsky Noam: *Pirates and Emperors, Old and New* – International Terrorism as It Really Is, Sources, Zagreb 2004.
6. Dictionary of Middle Ages ed Joseeph R. Stayer (New York: Shareles Scribner, with Sons. 1985) p. 483-489.
7. Dimitrijević, V., *Terrorism*, Workers' Press, Belgrade, 1982.
8. Gaćinović R., *Why Terrorism is Hard to Define*, Proceedings of the Synergy Scientific Conference, Bijeljina 2010.
9. Gaćinović, R., *Terrorism*, Draslar Partner, Belgrade, 2005.
10. Djordjević, O., *The Lexicon of Security*, Partizanska knjiga, Belgrade, 1989.
11. Hanhimaki, J.M., Blumenau, B.: *An International History of Terrorism – Western and Non-Western Expiriences*, Oxon; Routledge, 2013.
12. Hoffman Brus, *Internal Terrorism*, Alpha National Book, Belgrade, 2000.
13. Hoffman B., *Inside Terrorism*, Columbia University Press, New York, 2006.
14. Ignjatović, Dj., *Criminology* (Eighth Edited Edition), Official Gazette, Belgrade, 2007.
15. Kaseze, A., *International Criminal Law*, Belgrade, Belgrade Center for Human Rights, Belgrade, 2005.
16. Krivokapić B., *Lexicon of International Law*, Official Gazette, Belgrade, 2010.
17. Laqueur W., *The Age of Terrorism*, Boston: Little, Brown Co. & Co. 1987.
18. Laqueur W., *Postmodern Terrorism*: New Rules for an Old Game, Forin Affairs, 1996.

[39] Noam Chomsky, *Pirates and Emperors, Old and New – International Terrorism as It Really Is*, Sources, Zagreb 2004, page 7.

19. Mijalković S., Bajagić M., *On the Amendments to the Provisions of the 1977 Convention on the Suppression of Terrorism*.

20. Milošević, M., *Terrorists: Victims and Criminals – Factors of Criminal Motivation*, University of Belgrade-Faculty of Security, Belgrade, 2009.

21. *Political Encyclopedia*, Contemporary Administration, Belgrade, 1975.

22. Simeunović, D., *A Critical Review of the Determination of the Time of Emergence of Terrorism and Its Precursors "*, Military Work, No. 1.

23. Simeunović, D., *Terrorism*, Krimen Edition, Belgrade, 2009.

24. Simeunović, D., *Terrorism*, Second Edition, Faculty of Law, University of Belgrade, Belgrade, 2009.

25. Talijan M., *Security Management in Countering Terrorism and Combating Terrorism*. Media Center Defense, Belgrade, 2012.

26. White, R. Johnson, *Terrorism* (translated by Roksanda Ćirović), Alexandria Press, Belgrade. security center.org/terrorism-basics-first/

27. Vujaklija M., *The Lexicon of Foreign Words and Expressions*, Education, Belgrade, 1970.

28. The Convention on the Suppression of Terrorism has been ratified and-Official Gazette of the FRY – International Treaties No. 10/01.

29. Criminal Code of the Republic of Serbia, Official Gazette of the Republic of Serbia No. 85 / 2005,88 / 2005,107 / 2005, 72/2009, 111 / 2009,121 / 2012, 104/2013, 108/2014, 94/2016, and 35 / 2019.

30. Federal Anti-Terrorism Law No. 35-F 2006/2014, Russian Federation. http://legislationline.org/topics/country/7/topic/5/04.03.2020.

31. Terrorism Act 2000, (Internet: http://www.legislation.gov.uk/ukpga/2000/11contents, 04/03/2020).

32. 18 USC Ch.113B: TERRORISM, Internet: uscode.house.gov/view.xhtml?path=prelim@title18part1/chapter113B&edition=prelim.

33. FBI Official Website, (Internet: http: //www.fbi.gov/albuquerque/about-us/what-we-investigate, 03/04/2020).

The Importance of Thought Experiments

***Dr. Dragana Ćorić*[1]**

Abstract

Living in the world of legal norms seems to be easy: you have rules of conduct that guides you how to behave in a lot of life situations, and what will happen to you if you do not obey. Legal norms are predicting the future, in a certain way, and giving us the guidelines how to avoid punishment for breaking the rules.

But what happens when there are no specific guidelines how to react in certain situations? Although the legal system tends to cover with its rules all areas of social life, there is always a gap, a situation that could not been foreseen at the time of making that regulation. These gaps could be spanned by subsequent editing, i.e. by adopting subsequent rules of conduct. In order to predict an event that may occur, and to predict human behavior in these situations as well as human response to punishment that threatens to violate a rule, it is good to conduct a thought experiment.

The basis of a thought experiment can be a completely fictitious and even currently impossible event, or a variation of some of the known and possible events. Laying such a foundation is further important because of the prediction of people's behavior in certain situations, human response to certain external and internal stimulis, especially when it comes to punishment. In order to properly conduct a thought experiment, we need to precisely define the premise, which are the event and behavior we want to examine. That is why the key question when formulating a thought experiment is "what if". The answers to this question can be numerous, but each will start with "then it is possible", "then it will be", "it could be" or something similar. The answers will differ in terms of content only on the basis of the values, beliefs and attitudes of the one who answers the question "what if".

In our paper, we will briefly present the concept of a thought experiment, its internal structure, types and, by giving some examples, encourage readers to be more informed about this topic.

Key words: *thought experiment, imagination*

I. Introduction

Our scientific practice is rich of thought experiments, although their results may be subject to further empirical testing. A great part of ethics, philosophy of language, and philosophy of mind is based on the results of thought experiments in a way that seems very similar to scientific thought experiments (though some might contest this), including Searle's Chinese room, Putnam's twin earth, and Jackson's Mary the

[1] Assistant Professor, Faculty of Law, Novi Sad, University in Novi Sad. Contact: dragancica2@gmail.com.

colour scientist[2]. Philosophy, more than other sciences is fully enriched with thought experiments and their results, that even some authors say that without them, a great portion of philosophy wouldn't exist.

But what is the thought experiment?

A lot of definitions of thought experiments were made, or just tried to be made. All of them have the same, simplest idea that thought experiment is *"an experiment carried out in thoughts only"*[3], not in reality, in some laboratory or somewhere else outside. It is the use of an imagined scenario to help us understand the way things really are. The understanding comes through reflection on the situation. *"Thought experiments are performed in the imagination"*[4], says James Robert Brown*". We set up some situation, we observe what happens, then we try to draw appropriate conclusions"*[5]. They are *"what ifs"* – drivers of our thinking about something. Yeates says that "*a thought experiment is a device with which one performs an intentional, structured process of intellectual deliberation in order to speculate, within a specifiable problem domain, about potential consequents (or antecedents) for a designated antecedent (or consequent)"*[6]. In short, during the thought experiments we gain new information by rearranging or reorganizing already known empirical data in a new way, looking over from another perspective. In such a way we stimulate thinking, using our imagination, and we are testing our values, beliefs and standpoints.

Although the history of use of thought experiments are long and dates form Plato' cave or even earlier[7], it is considered that Hans Christian Ørsted was the first to use the German term *Gedankenexperiment* (lit. thought experiment) circa 1812[8]. Ørsted was also the first to use the equivalent term *Gedankenversuch* in 1820[9]. Ernst Mach used the term *Gedankenexperiment* in a different way, to denote exclusively the imaginary conduct of a real experiment that would be subsequently performed as a real physical experiment by his students[10]. After those two experiments, one that is conducted in reality and the same, conducted only in imagination, with words, not with actions, Mach interviewed students which consequences were more real to them, from the first or form the second experiment. The English term *thought experiment* was coined and first appeared in the 1897. In english translation of one of Mach's papers.

During the mid-1980s, thought experiments were recognized as a central technique in analytic philosophy. Thanks to the activities done especially by Tamara Horowitz and Gerald Massey, philosophers and other scientists started to think about thought experiments again. Few years of dedicated works resulted with conference at

---

[2] The mentioned experiment are just as an example, according to: Brown, James Robert and Fehige, Yiftach, "Thought Experiments", *The Stanford Encyclopedia of Philosophy* (Winter 2019 Edition), Edward N. Zalta (ed.), available on: https://plato.stanford.edu/archives/win2019/entries/thought-experiment/.

[3] https://www.merriam-webster.com/dictionary/gedankenexperiment.

[4] *Ibid*.

[5] *Ibid*.

[6]Yeates, L.B., Thought Experimentation: A Cognitive Approach, Graduate Diploma in Arts (By Research) Dissertation, University of New South Wales, 2004, 150.

[7] Rescher, N. (1991), "Thought Experiment in Pre-Socratic Philosophy", in Horowitz, T.; Massey, G.J. (eds.), Thought Experiments in Science and Philosophy, *Rowman & Littlefield, (Savage*), pp. 31–41.

[8] Witt-Hansen, J., "H.C. Ørsted, Immanuel Kant and the Thought Experiment", Danish Yearbook of Philosophy, Vol.13, (1976), pp. 48.

[9] Witt-Hansen, J.,49. *Versuch* is purely german word, so *gedankenversuch* is considered as the german word in whole. *Gedankenexperiment* is mixed, latin- german word.

[10] Mach, Ernst (1883), The Science of Mechanics (6th edition, translated by Thomas J. McCormack), LaSalle, Illinois: Open Court, 1960. pp. 32-41, 159-62.

the University of Pittsburgh on *"The Place of Thought Experiments in Science and Philosophy"* and with collected works from this conference, published in 1991.

The most important work for popularization of thought experiments in 21st century is book *"What If...Collected Thought Experiments in Philosophy"*, by Peg Tittle, which is published in 2016. It is a brief collection of over 100 classic and contemporary "thought experiments," each exploring an important philosophical argument. All experiments are divided into 9 areas: metaphysics, philosophy of mind, personal identity, philosophy of language, epistemology, logic, ethics, social and political philosophy, and aesthetics. After every experiment, there is a possible solution or explanation of the author, which is not definitive, and it is given as an introduction to further thinking and solving mentioned situation. Everyone, no matter how much they know philosophy, can give their opinion about the behavior of a third person in the context of that experiment or set themselves as the main character and ask themselves, *what if I was in that situation, what would I do.* That is, we can say, the beauty of thought experiments, especially in philosophy, because they can challenge everyone's opinion, at all times.

II. Types of Thought Experiments

According to Yeates, there are seven types of thought experiments[11]:

1. Prefactual[12] thought experiments speculate on possible future outcomes, *What will be the outcome if specific event happens"*[13]. For example, "what would happen to your friend, if you tell his wife everything you know about him". It could happen nothing, or something, in numerous ways.

2. Counterfactual[14] thought experiments speculate on the possible outcomes of a different past, ie if past was different, how would it affect to someone particular. For example, what if I have chosen to study mathematics, would it be possible for me to be an university professor in that area?

3. Semifactual[15] thought experiments speculate on the extent to which things might have remained the same, despite there being a different past. For example, imagine that it is raining and you have an umbrella but is it possible to get wet anyway?

4. Prediction- in this case, we project the circumstances of the present into the future. Some authors say that scientific prediction takes two forms[16]:

(1) Using known principles of nature, we predict what might happen

---

[11] Yeates, L.B., "Thought Experimentation: A Cognitive Approach", *Graduate Diploma in Arts (By Research) Dissertation*, University of New South Wales, 2004, available on: https://ia803100.us.archive.org/4/items/TECA2004/TECA-%282004%29.pdf. We list the types of thought experiments in order as it is done in Yeates' dissertation.

[12] The term *prefactual* was coined by Lawrence J. Sanna in his 1998 work: Sanna, L.J., "Defensive Pessimism and Optimism: The Bitter-Sweet Influence of Mood on Performance and Prefactual and Counterfactual Thinking", *Cognition and Emotion*, Vol.12, No.5, (September 1998), pp. 635-665.

[13] Yeates, p. 143.

[14] The term counterfactual was coined by: Nelson Goodman, "The Problem of Counterfactual Conditionals", *The Journal of Philosophy*, Vol.44, No.5, (27 February 1947), pp. 113-128.

[15] The term semifactual was also coined by Nelson Goodman, "The Problem of Counterfactual Conditionals".

[16] Sarewitz, D. & Pielke, R., "Prediction in Science and Policy", *Technology in Society*, Vol.21, No.2, (April 1999), pp. 121-133.

(2) Using suites of observational data and sophisticated numerical models in an effort to foretell the behavior or evolution of complex phenomena.

5. Hindcasting involves running a forecast model after an event has happened in order to test whether the model's simulation is valid. It is usually used for weather forecasting.

6. Retrodiction is moving backwards in time, step-by-step, in as many stages as are considered necessary, from the present into the speculated past to establish the ultimate cause of a specific event (e.g., reverse engineering and forensics). It means that *"past observations, events and data are used as evidence to infer the process(es) the produced them" and that diagnosis "involve[s] going from visible effects such as symptoms, signs and the like to their prior causes*"[17]. Retrodiction is kind of post factum analysis and giving the opinion on something.

7. Backcasting[18] is establishing the description of a very definite and very specific future situation. It then involves an imaginary moving backwards in time, step-by-step, in as many stages as are considered necessary, from the future to the present to reveal the mechanism through which that particular specified future could be attained from the present. In literature can be found even more classifications of thought experiments, but we hink that this one is the most accurate and the most comprehensive. The classification itself shows a wide application of thought experiments in various fields of life and science.

III. Inner Characteristics of Thought Experiments

What differs thought experiments from other exclusively laboratory experiments? According to Letitia Meynell, there are six inner characteristics[19]:

1. Imagery, needed for stimulating the imagination and focusing on the very idea that is disscussed. The line of imagination can be very fragile and unstable, so the one who is first imagining the experiment and conducting it must use:

2. Experiential language. He/she must behave as he/she did it in the reality, and have their own experience of what he/she are talking about. As the experiment-teller can more vividly and with a lot of details tell the imagined story, the more can he/she engage others to get involved and give their opinion.

3. An epistemological analysis is also rather important, thinks Meynell, because it shows how the thought experiment justifies (or fails to justify) its conclusion. It is a kind of paradox, that we expect that we can learn something new from the imaginary scenarios. But, if we clarify to ourselves that thought experiments and our solutions of the experiment are connected to our values, beliefs and attitudes, we can learn a lot – about ourselves and about others.

4. The thought experiments have *"the irreducibly imaginative character",* says Meynell. Every solution of this imaginative problem is correct, to the one that has given it. That is why the thought experiments are considered as:

---

[17] Einhorn, H.J. & Hogarth, R.M., "Prediction, Diagnosis, and Causal Thinking in Forecasting", *Journal of Forecasting*, (January–March 1982), Vol.1, No.1, pp. 23-36.

[18] Yeates, L.B., Thought Experimentation: A Cognitive Approach, Graduate Diploma in Arts (By Research) Dissertation, University of New South Wales, 2004,158.

[19] Letitia Meynell, "Imagination and insight: a new account of the content of thought experiments", *Synthese,* Vol.191, Issue 17, 2014, pp. 4149-4168.

5. Instruments of provocation and imagining different interpretations. We learn even by provocation and investigation of something, not only by memorizing pure facts. Every person reflects his/her own values, beliefs and experience, while searching for solutions of the thought experiment.

6. Thought experiments are considered *as objective* even though they are not real (but they might be real). Everyone acts from the position of their standpoint, and for them, their solution is their objective truth.

Having in mind all these characteristics of thought experiments, we may say that they are true and very valuable companion in developing imagination and process of decision-making.

Some thought experiments have the scenario that *could be nomologically possible, or possible according to the laws of nature.* For exampe, John Searle's *Chinese room* is nomologically possible:

"Imagine a native English speaker who knows no Chinese. Locked in a room full of boxes of Chinese symbols (a data base) together with a book of instructions for manipulating the symbols (the program). Imagine that people outside the room send in other Chinese symbols which, unknown to the person in the room, are questions in Chinese (the input). And imagine that by following the instructions in the program the man in the room is able to pass out Chinese symbols which are correct answers to the questions (the output). The program enables the person in the room to pass the Turing Test for understanding Chinese but he does not understand a word of Chinese.

The point of the argument is this: if the man in the room does not understand Chinese on the basis of implementing the appropriate program for understanding Chinese then neither does any other digital computer solely on that basis because no computer, qua computer, has anything the man does not have"[20].

Searl's experiment, throughout decades, has showed that artificial intelligence has the eligibility to think and work without consciousness (when consciousness is defined as something characteristic only for humans) and what could be the results of it. Personal computers, as some authors say, have evolved from vigilant Eliza, and *"have moved from the lab to the pocket and the wrist"*[21]. We are trying rather hard to give those artificial intelligences some consciousness and make them more alike to us. The only thing that is not clear is that we want them so similar to us, because we want to transfer all the burden of thinking and decision-making to them, or to have a neutral observer who will help us in life, at key moments.

Some thought experiments present scenarios that a*re not nomologically possible but are metaphysical possible* For example, Hillary Putnam's thought experiment is one of them:

We begin by supposing that elsewhere in the universe there is a planet exactly like Earth in virtually all aspects, which we refer to as "Twin Earth". (We should also suppose that the relevant surroundings are exactly the same as for Earth; it revolves

---

[20] In the first version of this thought experiment, Searl imagined himself locked in this room, see: Searle, John. R. (1980) Minds, brains, and programs. Behavioral and Brain Sciences 3 (3): 419; Searle, J. 1999, 'The Chinese Room', in R.A. Wilson and F. Keil (eds.), The MIT Encyclopedia of the Cognitive Sciences, Cambridge, MA: MIT Press.

[21] Cole, David, "The Chinese Room Argument", The Stanford Encyclopedia of Philosophy (Spring 2020 Edition), Edward N. Zalta (ed.), available on: https://plato.stanford.edu/archives/spr2020/entries/chinese-room/.

around a star that appears to be exactly like our sun, and so on). On Twin Earth, there is a Twin equivalent of every person and thing here on Earth. The one difference between the two planets is that there is no water on Twin Earth. In its place there is a liquid that is superficially identical, but is chemically different, being composed not of H2O, but rather of some more complicated formula which we abbreviate as "XYZ". The Twin Earthlings who refer to their language as "English" call XYZ "water". Finally, we set the date of our thought experiment to be several centuries ago, when the residents of Earth and Twin Earth would have no means of knowing that the liquids they called "water" were H2O and XYZ respectively. The experience of people on Earth with water and that of those on Twin Earth with XYZ would be identical. Now the question arises: when an Earthling (or Oscar for simplicity's sake) and his twin on Twin Earth say 'water' do they mean the same thing[22]?

The result of this is that the contents of a person's brain are not sufficient to determine the reference of terms they use, as one must also examine the causal history that led to this individual acquiring the term. (Oscar, for instance, learned the word 'water' in a world filled with H2O, whereas Twin Oscar learned 'water' in a world filled with XYZ.)Meaning isn't just in head, says Putnam, but also in experience of a person and his/her understanding of the circumstances in which he/she is, in his/her own environment.

In some cases, the hypothetical scenario might be considered *metaphysically impossible, or impossible in any sense at all*. Such thought experiment was conducted by David Chalmers[23], regarding existence of zombies, or persons who are physically identical to us in every way but who lack consciousness. Disputes about their conceivability goes for few decades and the result of these debates is fairly uniform as there are authors who think that the existence of a zombie as a person without any consciousness and conscience is entirely possible, while some authors firmly deny such a possibility. One thing is for sure, the Hollywood film industry supports the efforts of those who believe that zombies exist and that due to the physical deficiency of the brain in which all functional centers are situated, we already have these zombies somewhere next to us[24].

For thought experiment, there is also important their orientation in time[25]. They can be either:

– *Antefactual speculations:* experiments that speculate about what might have happened prior to a specific, designated event. For example, Richard Sylvan's experiment *"Last man argument"*[26], about possible behavior of the last man standing on Earth is an antefactual one experiment. Sylvan thinks about the behavior of the last

---

[22] Hilary Putnam (1973): "Meaning and Reference". In: Journal of Philosophy 70, pp. 699–711; Hilary Putnam (1975/1985): "The meaning of 'meaning'" In: Philosophical Papers. Vol. 2: Mind, Language and Reality. Cambridge University Press.

[23] Chalmers, D. J., 1996, "The Conscious Mind: In Search of a Fundamental Theory", New York and Oxford: Oxford University Press.

[24] Kirk, Robert, "Zombies", The Stanford Encyclopedia of Philosophy (Spring 2019 Edition), Edward N. Zalta (ed.), available on: https://plato.stanford.edu/archives/spr2019/entries/zombies/.

[25] Yeates, L.B., p. 160.

[26] Routley, Richard, 1973, "Is There a Need For a New, an Environmental, Ethic?", Proceedings of the XVth World Congress of Philosophy, Varna, 1: 205–10; reprinted in M. Zimmerman et al. (eds.), Environmental Philosophy: from Animal Rights to Radical Ecology, Englewood, NJ: Prentice Hall: 1993, pp. 12-21.

man on earth from different points of view of environmental ethics. If the last man on earth accepts an instristic view of the value of everything, whether living or non-living, just because it exists, his last hours spent on earth will be focused on maintaining his life and the life and survival of other species. If, on the other hand, the last man accepts the anthropocentric opinion that only man is worth living because he has the consciousness and power of thinking and planning, such a last man will activate the button for self-destruction of the whole planet and all other plant and animal species, survivors of the cataclysm, because their survival is of no importance to him who is dying.

– *Postfactual speculations:* experiments that speculate about what may happen subsequent to (or consequent upon) a specific, designated event. Although it is not enlisted fully as thought experiment, but more as example of game theory, The Prisoners' Dilemma can be observed in this context:

"Two members of a criminal gang are arrested and imprisoned. Each prisoner is in solitary confinement with no means of communicating with the other. The prosecutors lack sufficient evidence to convict the pair on the principal charge, but they have enough to convict both on a lesser charge. Simultaneously, the prosecutors offer each prisoner a bargain. Each prisoner is given the opportunity either to betray the other by testifying that the other committed the crime, or to cooperate with the other by remaining silent. The possible outcomes are:

If A and B each betray the other, each of them serves two years in prison

If A betrays B but B remains silent, A will be set free and B will serve three years in prison

If A remains silent but B betrays A, A will serve three years in prison and B will be set free

If A and B both remain silent, both of them will serve only one year in prison (on the lesser charge)"[27].

The thought experiment can be here done by asking a question: *You are one of those two criminals, what would you do and what would you think that your best friend and companion in crime would do in this kind of situation?*

Also, we can say that there are thought experiments that are they *past-oriented* and *future-oriented*. Firstly, past oriented thought experiments are dealing with possible outcomes in the future if the initial events in the past were different. For example, If I would studied mathematics, would my life be different today? Or, like Ludwig Wittgenstein presumed in his thought experiment called *"The Big Book"*[28] about the nature of ethics and the verifiability of ethical knowledge:

"No statement of fact can ever be, or imply, a judgment of absolute value. Suppose one of you were an omniscient person and therefore knew all the movements of all the bodies in the world dead or alive and that you also knew all the states of mind of all human beings that ever lived, and suppose you wrote all you knew in a big book, then

---

[27] Firstly disscused by Merrill Flood and Melvin Dresher in 1950, as part of the Rand Corporation's investigations into game theory, this dilemma is fully defined Albert Tucker. More about it: Kuhn, Steven, "Prisoner's Dilemma", The Stanford Encyclopedia of Philosophy (Winter 2019 Edition), Edward N. Zalta (ed.), available on: https://plato.stanford.edu/archives/win2019/entries/prisoner-dilemma/.

[28] First mentioned in Wittgenstein's work *Lecture on Ethics,* published in 1929. We used, for the purpose of this paper the 1997. reprinted version of this experiment in: Darwall, Gibbard, and Railton, "Moral Discourse and Practice: Some Philosophical Approaches, New York: Oxford University Press, p. 67.

this book would contain the whole description of the world; and what I want to say is, that this book would contain nothing that we would call an ethical judgment or anything that would logically imply such a judgment".

The second*, future-oriented* experiments are trying to presume what could happen in the future if something happens now, or if something that it is not possible now to happen, could happen and how it could affect on other future events. We can mentioned as, an example here, *The Case of Speluncean Explorers*, done by Lon Fuller in 1949, which was examining the behavior of five speluncean explorers trapped in a cave, and decisions of judges, who conducted proceedings against the surviving explorers after their release from the cave[29]. The specific of this thought experiment is that it happens in year 3400, that there are some rules of conduct that didn't exist at the time Fuller wrote it and that he was imagining everything- the plot, the rules and the solutions.

IV. Concluding Remarks

Thought experiments are product of the imagination. Yet they are important in every science, because their use enhances the knowledge in specific way. We find them in biology, economics, history, mathematics, philosophy, and physics. We find them in sociology, ethics, law. And every time, no matter how many times they've been disscused so far, we disscus about them with new energy, ideas and widened beliefs.

Are they mandatory instrument in gaining new knowledge? No, but they are rather fun, innovative and seems to be – never ending. Sometimes we can even save the world thinking about imagined scenarios and trying to predict people's behavior. But how can we learn about reality (if we can at all), just by thinking in such a way? We think that we can, only if we learn how to better perceive the world around us and listen to what it tells us. Using thought experiments, we can, maybe, achieve more effective form of mental perception and make bonds to other people and to our environment more efficient than we are doing it now.

Thought experiments are allowing us to open the doors of perception, imagination and think about solutions that are in our subconscious. We hope that this paper would open new doors to its readers and inspires them to explore hidden knowledge in ourselves, buy using thought experiments.

References

1. Brown, J.R., Fehige, Y., "Thought Experiments", The Stanford Encyclopedia of Philosophy(Winter 2019 Edition), Edward N. Zalta (ed.), available on https://plato.stanford.edu/archives/win2019/entries/thought-experiment/.

2. Chalmers, D. J., *The Conscious Mind: In Search of a Fundamental Theory*, New York and Oxford: Oxford University Press, 1996.

3. Cole, D., *The Chinese Room Argument*, The Stanford Encyclopedia of Philosophy (Spring 2020 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/spr2020/entries/chinese-room/.

[29] Lon L. Fuller," The Case of the Speluncean Explorers", Harvard Law Review,Vol. 62, No. 4, February 1949, available on: http://w.astro.berkeley.edu/~kalas/ethics/documents/introduction/fuller49.pdf.

4. Einhorn, H.J. & Hogarth, R.M., *Prediction, Diagnosis, and Causal Thinking in Forecasting*, Journal of Forecasting, (January–March 1982), Vol.1, No.1, pp. 23-36

5. Fuller, L.L., *The Case of the Speluncean Explorers*,Harvard Law Review,Vol. 62, No. 4, February 1949, http://w.astro.berkeley.edu/~kalas/ethics/documents/introduction/fuller49.pdf

6. Goodman, N., *The Problem of Counterfactual Conditionals*, The Journal of Philosophy, Vol.44, No.5, (27 February 1947), pp. 113-128.

7. Kirk, R., *Zombies*, The Stanford Encyclopedia of Philosophy (Spring 2019 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/spr2019/entries/zombies/.

8. Kuhn, S., *Prisoner's Dilemma*, The Stanford Encyclopedia of Philosophy (Winter 2019 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/win2019/entries/prisoner-dilemma/.

9. Mach, E., The Science of Mechanics, 1883 (6th edition, translated by Thomas J. McCormack), LaSalle, Illinois: Open Court, 1960.

10. Meynell, Letitia, *Imagination and insight: a new account of the content of thought experiments*, Synthese, Vol.191 Issue 17, 2014, pp. 4149-4168.

11. Putnam, Hilary, *Meaning and Reference,* in Journal of Philosophy 70, (1973): pp. 699–711.

12. Putnam, Hilary, *The meaning of 'meaning* (1975/1985), in Philosophical Papers. Vol. 2: Mind, Language and Reality. Cambridge University Press

13. Rescher, N., *Thought Experiment in Pre-Socratic Philosophy*, in Horowitz, T.; Massey, G.J. (eds.), Thought Experiments in Science and Philosophy, Rowman & Littlefield, (Savage), 1991, pp. 31-41.

14. Routley, R., *Is There a Need For a New, an Environmental, Ethic?,* Proceedings of the XVth World Congress of Philosophy, Varna, 1: 205–10,1973; reprinted in M. Zimmerman et al. (eds.), Environmental Philosophy: from Animal Rights to Radical Ecology, Englewood, NJ: Prentice Hall: 1993, p. 12–21

15. Sanna, L.J., *Defensive Pessimism and Optimism: The Bitter-Sweet Influence of Mood on Performance and Prefactual and Counterfactual Thinking*, Cognition and Emotion, Vol.12, No.5, (September 1998), pp. 635-665.

16. Sarewitz, D., Pielke, R., *Prediction in Science and Policy*, Technology in Society, Vol.21, No.2, (April 1999), pp. 121-133.

17. Searle, J.R., *Minds, brains, and programs*. Behavioral and Brain Sciences 3 (3),1980.

18. Searle, J., *'The Chinese Room'*, in R.A. Wilson and F. Keil (eds.), The MIT Encyclopedia of the Cognitive Sciences, Cambridge, MA: MIT Press, 1999,

19. Wittgenstein, L., *Lecture on Ethics*, reprinted in Darwall, G., Railton, *Moral Discourse and Practice: Some Philosophical Approaches*, New York: Oxford University Press,1997.

20. Witt-Hansen, J., *H.C. Ørsted, Immanuel Kant and the Thought Experiment*, Danish Yearbook of Philosophy, Vol.13, (1976),

21. Yeates, L.B., *Thought Experimentation: A Cognitive Approach*, Graduate Diploma in Arts (By Research) Dissertation, University of New South Wales, 2004. available on: https://ia803100.us.archive.org/4/items/TECA2004/TECA-%282004%29.pdf

22. https://www.merriam-webster.com/dictionary/gedankenexperiment.

Requirements for Criminal Law

Dr. Ervin Belovics[1]

Abstract

The study is focusing on the rule of law requirements for criminal substantive law. The fundamental aspects of the rule of law guarantees for criminal substantive law gained attention after the change in the political regime. It was in the resolutions of the Constitutional Court in particular where the basic principles that are the indispensable prerequisites of the rule of law started to appear. Resolving the confrontation between legal certainty and equity gave a permanent task for the Constitutional Court after the political changes. Upon examining decisions with criminal law aspects – as well as analysing the German legal practice – the author expresses his opinion of disagreement. Throughout the introduction of fundamental criminal law principles, the author analyses them in details and also synthesizes the consequences resulting from them. In the final part of the essay, the author is looking for an answer whether the expectations that governments should protect their citizens from others by providing legal shelter for them against the actions of unlawfully acting wrongdoers is a criterion of the rule of law principle.

Keywords: *prohibition of analogy, rule of law guarantees in criminal law, legal certainty, justifiable defence, equity, retroactive force (ex tunc temporal scope), ultima ratio*

I. Introduction

The rule of law as a concept first appeared in the German legal literature in the first half of the 19th century (e.g. in the work of Friedrich Julius Stahl, Karl Welcker, Rudolf von Gneist and Robert von Mohl) with the aim to represent the antithesis of the police state symbolizing the dictatorship and to demonstrate that the power structure – including the functioning of the State organs – should be governed by law. In this concept, the basic criteria of the rule of law is the fact that power is also obliged to comply with provisions of law, and to make its functioning transparent and predictable, and to ensure that the rights of citizens prevail. I would note that the principle of the English Rule of law invested with the current meaning by Albert Venn Dicey (Venn Dicey, 1902) also expresses the absoluteness of the rule of law, nevertheless, with regards to the special attributes of the common law in the field of criminal law the concept of Rechtstaat calls for completely different requirements. For this reason, it is necessary to consider the basic facts of the German legal literature in relation to criminal law in the framework of the development of continental law.

[1] Prof. dr., Head of Department, Faculty of Law and Political Science of the "Pázmány Péter" Catholic University, Budapest, contact: belovics.ervin@jak.ppke.hu.

II. The prerequisites of the rule of law in the field of criminal law in the relation of the State and citizens

By the second half of the 19th century in the attitude of citizens, the expectation of the order provided by State organs was gradually substituted by the desire for freedom, which restricts the rights of the executive power. Consequently, the concept of rule of law „prevail in the relation of the State and the citizen, the rule of law is not supposed to protect its citizens from each other. It is not a criterion for the rule of law that the State prosecutes thieves and robbers but it is a criterion that the State provides for its citizens the freedom of expression, of access to information, of assembly and gathering and the freedom of property as well as the security and liberty thereof". (Békés, 2006)[2] I will later come back to the question whether the restriction of the concept of the rule of law to the relation of the State and the citizen in the field of criminal law is still valid or not.

2.1. The Practice of the Hungarian Constitutional Court

From its formation – but particularly in its early years, at the beginning of the 1990s – the Hungarian Constitutional Court paid special attention to defining the prerequisites of the rule of law in the field of criminal law.

During its analyses and examinations – since the products of the legislation of the former dictatorship required conceptual resolutions over and over again – the determination of the substantive and procedural component of the rule of law in the field of criminal law as well as the evaluation of the relation of these two pillars played a crucial part. How one of the prerequisites of the concept of rule of law, the legal certainty, defined as the law and order created by the positive written law, and the fairness are interrelated, thus the rules of the law should meet the exigencies of the society, the requirements of reason and moral.

This question was particularly in the center of interest, when on the 4th of November 1991 the Parliament adopted a law on the renewed beginning of limitation periods of certain crimes[3].

The Constitutional Court declared the law, adopted by the Parliament but not promulgated, anti-constitutional[4].

According to the reasoning of the Constitutional Court „The basic element of the rule of law is legal certainty. Legal certainty requires – among others – the protection of the rights obtained, leaving the realized and concluded legal relations untouched, and the restriction by constitutional regulations of the alterability of the permanent legal relationships originated in the past […] Certain legal relationships and legal facts become independent from the norm they derive from, and they do not follow its fate

---

[2] Imre Békés: Criminal Law General Part HVG ORAC Lap- Könyvkiadó Kft. Budapest, 2006. p. 46.

[3] The text of the adopted law is the following: "Article 1 paragraph (1) On the 2nd of May 1990 the statutory limitation period of crimes committed between 21-Dec-1944 and 2-May-1990, and regulated by the laws in force in this period restarted, especially including capital treason, defined by Article 144 (2) of Act IV of 1978; intentional homicide defined by Article 166 (1-2); bodily harm causing death defined by Article 170 (5), if the state did not prosecute them due to political reasons. Paragraph (2) the punishment imposed according to paragraph (1) can be unlimitedly reduced." The President did not promulgate the law, instead on 16-Nov-1991 he sent it for constitutional review.

[4] Constitutional Court Decision 11/1992. (III.5.) AB.

automatically anymore. Otherwise, every amendment of the provisions of law would trigger the revision of the mass of legal relationships. As a main rule, it follows from the principle of legal certainty that the concluded legal relationships cannot be modified in a constitutional way, neither by legal rules, nor by the annulment of those – even if carried out by the legislator or by the Constitutional Court.

An exception to this principle can only be allowed if another constitutional principle, concurrent with legal certainty makes it inevitable, and it does not result in unproportionate damages compared to its aim. Such an exception can be the revision of criminal procedures closed with a final judgment in favor of the defendant if the procedure had been carried out in conformity with a legal provision which was later declared unconstitutional. This is required by constitutional criminal law. The unfair result of legal relations by itself cannot be a reason against legal certainty[5]. […] As far as respect for concluded legal relationships are concerned, difference cannot be made based on the fact how and when the legal regulations in question became unconstitutional. The legislator with regard to every legal relationship is restricted by the limitations of the retroactive nature of legislation. […] Legal cases considered anti-constitutional could only be prospectively and constitutionally remedied by new legislation.

It is unacceptable […] to waive the fundamental guarantees of the rule of law by referring to the justice required by the rule of law. The rule of law cannot be implemented against the rule of law. Factual and formal legal certainty must have priority over the always partial and subjective justice. […] in most cases the fundamental institutions of constitutional criminal law cannot be made conceptually relative, and it is not conceivable to have any other constitutional rights or tasks considered against them. It is because the guarantees of criminal law already contain the result of a consideration, namely that the risk of the failure of prosecution is being carried by the state. […]

For this reason, the presumption of innocence cannot be further restricted by another constitutional right, neither is it possible to enforce it incompletely at a conceptual level; due to the passivity of the state, at the end of the statutory limitation period the unpunishability obtained automatically takes effect, it cannot be retrospectively ››diminished‹‹ or restored; the requirement of nullum crimen sine lege cannot be replaced by any constitutional task aiming to protect others' rights. […] Any exceptions from the guarantees of the criminal law could only be possible by the obvious waiving of these guarantees, however this is excluded by the principle of the rule of law. […] The guarantees of the rule of law cannot be deprived from anyone by law and order of the rule of law. These are fundamental rights for all of us. Based on the values of the rule of law, not even fair demands can be enforced by neglecting the guarantees of the rule of law. Fairness and moral reason can serve as a basis of punishment for someone who deserves it, the legal basis of punishability, however, must be constitutional. […] In the rule of law the state does not and cannot have unlimited criminal power. It is because public authority itself is not unlimited, either. Due to the fundamental constitutional rights and constitutional freedoms public

[5] According to Constitutional Court Decision 9/1992. (I. 30.) AB: "the requirement of the rule of law concerning the substantive fairness can only prevail within the institutions and guarantees serving legal certainty. The Constitution does not (and may not) provide substantive fairness on a universal basis".

authority can only intervene in individual rights and freedoms upon constitutional authorization"[6].

The aforementioned standpoint of the Constitutional Court relied on the omnipotence of the formal element of the rule of law in the field of criminal law, i.e. the principle of legal certainty, when repealed the law on the renewed beginning of the statutory limitation period, which reasoning is not acceptable. It is a determining, crucial feature of all dictatorships that the group in power and their supporters maintaining the dictatorial system are not brought to account, not even when their actions clearly fall under the provision of criminal law, i.e. their conduct is against the criminal law. The primary reason of the erosion of positive written law, i.e. legal certainty, is the omission of state executives, when their passivity enables offending individuals to escape from being held legally accountable. Considering the fact that throughout the existence of such systems the legal accountability of individuals in power is conceptually impossible, thus following the collapse of the dictatorship it is not only the demand for justice that makes the accountability indispensable, but also the reconstruction of legal certainty can only be achieved in that way. In my view, the lack of prosecution after the political changeover against offending individuals of the dictatorial regime was contrary to the values of the rule of law in the field of criminal law.

2.2. The Practice of the German Constitutional Court

In order to reinforce my standpoint, I would like to mention that after the German unification, the criminal accountability of the former leaders of the German Democratic Republic was not a problem at all for German courts and the German Constitutional Court. German courts found guilty several high ranked leaders for intentional murder and sentenced them to long term imprisonment. The judgment was brought in connection with acts committed at the German wall and in the „inner border", when border guards used their weapon against people crossing the border illegally, in order to comply with the command „who violates the border, loses his/her life". After their conviction by court, the defendants turned to the German Constitutional Court. According to the reasoning of the German Constitutional Court „Criminal law established with the guarantees of the rule of law, in principle meet the exigencies of the material justice. It creates a special situation of trust, the prohibition of retroactive effect is based on that. This situation ceases to exist when the State neglects the universally acknowledged human rights by creating grounds for total exemption from criminal responsibility and thus causes the most severe criminal injustice. In this kind of situation, the rule of material justice should be supported against the prohibition of retroactivity effect. […] The concept of the prohibition of retroactivity effect does not prevail when the State encourages its citizens to commit severe criminal injustice and violates the universally acknowledged human rights"[7].

---

[6] In the quoted decision of the Constitutional Court, like in other similar decisions of the Constitutional Court, appears the concept of "constitutional criminal law" drafted by András Szabó. In my opinion, this terminology has no substantive meaning, despite of the fact that it was being used by the majority of the legal experts of that period. In my view it only refers to the requirement that the norms of the criminal law – just like every regulation of each branch of law – must be in conformity with the rules of the Constitution.

[7] Imre Békés: Judgement of the European Court of Human Rights in Streletz, Kessler and Krenz vs. Germany case. KJK-KERSZÖV Jogi és Üzleti Kiadó Kft. Budapest, 2004. pp. 63-64.

Afterwards, the convicts appealed to the European Court of Human Rights. The Court found that the German courts had not violated the European Convention on Human Rights when „they interpreted the legal rules of the German Democratic Republic in force at the time of the commission of the act according to the principles of the rule of law.

It is obvious from these decisions that persons who had committed the most severe crimes between 1944 and 1990 without being prosecuted, could have been convicted in a manner in accordance with the conditions of the rule of law of the criminal law.

III. A Principles of the Rule of Law in the Field of Criminal Law

3.1. Principle of Legality

In the continental legal system, the principle of legality is of utmost importance in the area of criminal substantive law, bearing in mind that all other criminal law principles are based on the principle of legality. The essence of the principle is reflected in Act XXXI of 1993 on the promulgation of the Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and its eight additional protocols. Article 7 of the Act provides that no one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the criminal offence was committed. I would like to point out here that the principle of legality is not a prerequisite for the rule of law. "In the precedent-based Common-law legal systems, not every offence has a written law attached to it. There are precedents which are several hundred years old, and this "law created by the judge" are in force in place of statutory provisions”[8].

3.1.1. With regard to the rule of law, one of the principles of substantive legality, namely the principle of *nullum crimen sinus lege*, plays a decisive role. "If we look back at the history of criminal law, we can see that as a result of considering the effects of the nullum crimen sine lege principle the work of Cristoph Carl Stübel and Anselm Feuerbach in the early 19th century brought the factual element of the crime to the fore. According to this clarification, the act to be punished does not generally infringe the legal order by constituting an unlawful act, but only if it constitutes a precisely defined factual element of the crime. [...] Only the criminal law consisting of criminal acts defined as an element of the crime corresponds to the nullum crimen sine lege principle. [...] A free and loose regulation, which is possible for example in private law, where judges can make their decisions within a wide margin of discretion, is not acceptable in criminal law because of the nullum crimen sine lege principle”[9].

The principle has the following criminal law consequences:

– notwithstanding the provisions of national law, the *ius cogens* criminal acts give rise to criminal liability,

– only a legal provision at the top of the domestic legal source can make a conduct – an act or omission – a crime,

---

[8] Imre Békés: Criminal law – General Part. HVG ORAC Lap- és Könyvkiadó Kft. Budapest, 2006. Pp. 50.

[9] Béla Pokol: Criminal Law Theoretical Analysis Rejtjel Kiadó. Budapest, 2016. pp 58-59.

– the criminalization of an act must already be determined by a law before it is committed,

– no criminal liability can be established for any conduct that was not illegal at the time of the crime,

– a crime can only be committed by an act that corresponds to the legal definition of crime,

– the court can establish criminal liability only for a conduct which corresponds to the statutory definition of the crime,

– if, under the new law in force at the time of the adjudication, the act no longer constitutes a crime, the application of the new law is mandatory.

3.1.2. The second principle of substantive legality is the principle of *nulla poena sine lege*. "A typical derivation of the rule of law is the principle of "no punishment without law", which addresses an aspect of the requirement of predictability, namely the need to warn people in advance that certain types of acts will lead to punishment"[10].

The basic elements of the principle are as follows:

– only a legal provision at the top of the domestic legal source can establish a criminal legal consequence,

– the court may only apply such criminal law consequences that were already assigned by law to the crime prior to the time of the commission,

– in determining the penalty, the court is obliged to comply with the relevant provisions of law regarding the imposed penalty or the applicable measure, i.e. its nature, length or extent must always be determined in accordance with the law,

– if the new criminal provisions in force at the time of the assessment of the crime punishes the crime more severely, the new law does not apply,

– if the new criminal provisions in force at the time of the assessment of the crime provides for a milder penalty, the new law shall apply.

I would like to point out that though the principles of nullum crimen sinus lege and nulla poena sine lege " are not inextricably linked, yet, their origin coincides"[11].

3.2. Prohibition of Retroactive Application of More Severe Criminal Provisions

In continental criminal law, the principle of legality gives rise to the requirement of prohibiting the retroactive application of the more severe criminal provisions. The main rule of criminal law in the continental legal system is that one may only be prosecuted and punished in accordance with the law in force at the time of the offence[12]. Thus, the principles of nullum crimen sine lege and nulla poena sine lege

---

[10] Aubert V. The Rule of Law in „The Rule of Law", issue 1 pp. 62.

[11] József Földvári: Hungarian Criminal Law Osiris Kiadó, Budapest, 2003 pp. 35.

[12] A classic example of the breach of the principle is the "lex van der Lubbe" case. Marinus van der Lubbe, arrested in the Bismarck Hall of the German Parliament (Reichstag) building, which was set on fire on 27 February 1933, admitted the crime during his interrogation. When the Reichstag was set on fire, the Penal Code allowed for life imprisonment for intentional arson. On 28 February 1933, the Secretary of State Ludwig Grauert proposed the introduction of a state of emergency in Prussia, which was extended to the entire German Empire at the request of Minister Wilhelm Frick. The legal consequence of this was that it became possible to impose the death penalty for acts threatened up to that point with life sentence. The law, which entered into force on 29 March 1933, extended the emergency provisions to offences committed between 31 January 1933, and 27 February 1933, on the basis of which it became possible to impose the death penalty.

clearly define the temporal scope of the criminal provisions which, according to the doctrine of the classical school, "assume that the perpetrator was aware of the provisions of criminal law effective at the time of the commission of the criminal offence, but behaved in violation of that law [...] and must therefore bear the adverse consequences of his/her unlawful conduct, even if at the time of the sentencing the norm in force at the time the offence was committed has changed and the conduct is no longer punishable or it contains more favorable provisions for the perpetrator."[13]

However, the prohibition of the application of the *ex-tunc* principle is not universally valid any more, i.e. the retroactive application of the criminal law is not prohibited even in the rule of law; on the contrary, it is expressly stipulated as a prerequisite, but only if the act is no longer a criminal offence or is subject to a milder sentence. As the Constitutional Court has pointed out: "In addition to the explicit prohibition of retroactivity, the requirement of the application of the more favorable rule in sentencing derives from the requirement of the rule of law"[14].

The general fundamental statements relating to ex tunc effect prohibition are as follows:

– crime must be prosecuted in accordance with the criminal law in force at the time it was committed, the latter changes are indifferent,

– no criminal liability can be established for conduct which was not against criminal law in nature at the time of its realization, and it is not possible to apply a legal sanction more severe than the one contained in the substantive criminal law norm due to the commission of a delict/tort, which, at the time of the conduct being against criminal law, was not yet part of the Criminal Code,

– the prohibition does not relate to standards which entered into force after the commission of the crime, and which eliminate the penalization of the act committed, or to legislation which allows for a lighter judgement,

– only apparently is shown the item burdening the defendant that does not preclude the initiation of criminal proceeding and judgement for the act which, at the time of commission, constitutes a criminal offense solely on the basis of generally recognized rules of international law, whereas international ius cogens, as I have already mentioned, provides a basis for criminalization independently from the provisions of domestic law.

3.3. The Ultima Ratio Nature of Criminal Law

The theorem reflects the requirement that for resolving various conflict situations primarily norms of other branches of law should be used. In other words, it is an essential condition for the creation of a criminal law threat that its creation is necessary, i.e. there should be no more lenient way of protecting the right. Given that criminal law also provides the possibility of causing a legal disadvantage which no other branch of law allows, criminal legal consequences can only be applied if the legal protection provided by other branches of law are not sufficient means for protecting the rule of law. Therefore "Criminal law is the ultima ratio in the system of legal

[13] Zsigmond Kiss: Issues of retroactivity in the light of the provisions relating to the temporal scope of the Criminal Code. Faculty of Law and Political Science of the Pázmány Péter Catholic University Budapest, 2000 p. 161.

[14] Constitutional Court Decision 11/1992. (III.5.) AB.

liability. Its social function is to be the sanctioning keystone of the legal system as a whole. The criminal law sanction, the role and purpose of a punishment are to maintain the integrity of law and moral norms when sanctions of other branches of law no longer help [...] It is a substantive requirement that the law maker may not act arbitrarily when determining the conduct to be punished. The need to criminalize any conduct must be judged by a strict standard: the use of criminal law instruments, which inevitably restrict human rights and freedoms in order to protect different life situations, moral and legal standards, is only justified in an absolutely necessary case and to a proportionate extent, if the protection of state, social, economic objectives, values, which are constitutional or traceable to the constitution, is not possible in any other way"[15].

The rule of law requirements arising from the nature of ultima ratio are therefore that

– to resolve conflict situations in society primarily branches of law out of criminal law should be used,

– in the event of an infringement, legal integrity must be ensured by the application of legal sanctions governed by other branches of law,

– only such conduct can be declared contrary to criminal law in the interest of which the establishment of criminal law protection is unavoidable,

– the criminal threat should be proportionate to the risk to abstract society of the conduct declared to be unlawful.

All these requirements show the legislator that criminal legislation must not be arbitrary, neither in criminalising nor in determining the criminal consequences. Thus, it is not possible to expand the scope of crimes without limitation, even if sometimes the ruling power sees the criminalization of unwanted conduct as the only possible way to solve this problem. If the legislator nevertheless does so, it not only infringes the principle of the ultima ratio, but also devalues criminal law by criminalizing minor acts. However, in addition to necessity, the requirement of proportionality must also be taken into account in legislation, therefore, if codification of criminal law becomes essential, the legislator must determine the legal consequences to be imposed on the perpetrator of the crime, taking into account the danger of the crime to society. The latter requirement must, moreover, be enforced by the law enforcement when considering the specific case. „The provisions of the Criminal Code for the imposition of sanctions should be seen as a coherent system in which the relevant rules are applied with respect to each other and in a complementary manner. From a constitutional point of view, the purpose of the normative provisions on the assessment of penalties is to enable the punishment of offenders proportionately and according to the circumstances of the offence"[16]. The requirement of proportionality therefore plays a role both in relation to the risk to the abstract society, which contributes to general prevention, and in relation to individualisation for special prevention.

3.4. The Requirement of the Clarity of Criminal Law

The importance that norms need to be well-defined already occurred in Cesare Beccaria's works, when he explained "The greater the number of people who

[15] See: Constitutional Court Decision 30/1992. (V.26.) AB.
[16] Constitutional Court Decision 13/2002. (III.20.) AB.

understand the sacred law code and who have it in their hands, the less frequent crimes will be, for there is no doubt that ignorance and uncertainty concerning punishments aid the eloquence of the passion"[17]. Laws, however, can only be "held in the hand" if they are accessible. "Predictability is the most important requirement a norm has to fulfil. The first prerequisite of predictability is accessibility, including accessibility in a physical sense"[18]. It is a fundamental requirement for the criminal law governed by the rule of law that crimes should only be defined by the law, whereas it is also a requirement that when criminalzing certain acts, legislation should define the prohibited or expected conducts as precisely as possible, so that they could be adhered to by anyone; the laws "need to be precise, easily interpretable"[19]. It is namely an indispensible prerequisite of conducts complying with norms that the requirement of clarity for norms should be fulfilled; in other words, the content of norms could unambiguously be unfolded by using one of the interpretation types. Due to the rule of law requirement that norms need to be well-defined, laws have to be clear, free of contradictions and easily comprehensible, i.e. the codification of laws should aim at wording criminal law provisions in a simple way, following the rules of the Hungarian language. The exact terminological unity, in other words, the precise definition of technical terms is an equivalently important requirement. When the definition of prohibitions or requirements set forth by criminal law have incomprehensible, inaccurate, different or even contrary meanings, those whom the norms are addressed to cannot determine what kind of conduct is expected of them, what kind of conduct they are to follow. According to expectation of criminal law governed by the rule of law, "provisions which describe conducts prohibited by threat of sanctions need to be definite, clearly defined and formulated. It is also a constitutional requirement that the legislative intent concerning the protected legal object and criminal conduct has to be clearly expressed. It has to present unambiguous messages about cases when an individual is considered to violate criminal law. At the same time, it has to restrict the possibility of arbitrary interpretation of law for those who apply it. It needs to be examined, therefore, whether the range of sanctioned conducts specified by the legal definition of crime is not too wide, whether it is sufficiently clear-cut"[20].

3.5. Prohibition of Analogy Incriminating Perpetrators

The prohibition of drawing analogies is a fundamental principle in criminal law. Several authors (for example József Földvári, Miklós Kádár, György Kálmán) completely dismiss the idea of using analogies, but analogies violate requirements of the rule of law only if they in their completeness are used for a conduct that does not match a legal definition of a crime. In such a case there is in fact a legally regulated and unregulated situation, and by using a legal analogy the applier of law, considering that the decisive elements are the same and disregarding that the secondary circumstances

[17] Cesare Beccaria: Crimes and Punishment. Academy Publishing House, Budapest, p. 62.

[18] Balázs Gellér: Textbook on Hungarian Criminal Law. Volume I. General Part. Hungarian Official Journal Publisher, Budapest, 2008. p. 56.

[19] István Kónya: The State's criminal justice power. National Institute of Criminology-Pázmány Péter Catholic University Faculty of Law and Political Sciences, Budapest, p. 318.

[20] Constitutional Court Decision 30/1992. (V.26.) AB.

are different, extends the scope of the norm to an act which is not regulated by the norm, i.e. by the law. "This, however, means that although the applier of law is aware of the legislative intent expressed by the law as well as of the fact that the legislator's intent undoubtedly must not have covered that situation, he/she still applies the provision of law to the unregulated situation. In this way, the applier of law basically gives the provision of law a broad interpretation. Based on the principles of nullum crimen sine lege and nulla poena sine lege, which are acknowleged and highly valued by the continental law system, the use of analogies resulting in the extension of criminal liability or of the scope of criminal liability is impossible by definition in criminal substantive law"[21].

3.6. Ne bis in idem principle

The principle prohibiting dual criminality is equally applicable to all fields of criminal law in the widest sense, namely to criminal substantive law, procedural criminal law as well as to the enforcement of punishments. It manifests the requirement in criminal substantive law that if the legislator has already given consideration to a particular circumstance, the applier of law cannot consider it as well. Thus, for example, when a sentence is imposed, the fact laying basis for the mitigated case of the crime cannot be considered as a mitigating factor, nor can the modus operandi which establishes the aggravated case of crime be regarded as an aggravating factor. The prohibition of dual criminality thus aims to prevent that importance would be attached to an already considered fact or circumstance.

IV. Requirements of Criminal Law Governed by the Rule Of Law in Relation to Individuals

The already presented statements are based on the theoretical starting point that the requirements of criminal law governed by the rule of law shall prevail in the relation between the State and the individuals. In other words, protecting its individuals from others, providing protection against persons' unlawful conducts in legislation and the application of law are not criteria of the rule of the law.

In my view, while totalitarian features characterized power structures in the western part of Europe at the end of the 19th century and in Middle-Eastern Europe until the end of the 20th century, applying the emphatic elements of the rule of law to the relation between the State and the individuals was indispensable. As a result of social-political changes, however, nowadays even the protective function, namely that criminal law shall protect the established social, economic and state order, the individuals' person and rights, shall be regarded as one of the tasks of criminal law governed by the rule of law.

The same conclusion was drawn by several European legal scholars in the middle of the last century. When analyzing the concept of legal certainty (rettsskkerhet), which is one of the pillars of the rule of law, the Norwegian Johs Andenaes explained that "Two things need to considered in relation to rettsskkerhet. First, the protection of individuals' rights against other individuals. Second, the protection against the

[21] Ervin Belovics: Criminal Law I. HVG ORAC Publishing House Ltd., Budapest, 2017. p. 80.

arbitrary use of state power and against the abuse of such a power"[22]. As Vilhelm Aubert notes "For a criminal lawyer it is natural that the protection of life and property against unlawful attacks should also be included here"[23].

All this means that the legal definitions of crimes in the special part of the Criminal Code should cover the conducts threatening or infringing the mentioned interests and values, and the state shall ensure the right to protection if it is not able to protect its individuals. Establishing the framework of the latter is of special importance because in this context it can be made clear whether the legislator intends to protect the interests of the person acting against the law or the interests of the person trying to avert such an act.

V. Conclusion

A fundamental characteristic of criminal law governed by rule of law is that principles whose existence state organs, in particular legislative bodies and bodies applying law shall guarantee, prevail. These principles constrain legislation and prevent the arbitrariness of the judiciary. In the 21st century, however, the rule of law is intended not only to constrain the legislative and judiciary power, but the protective function shall also prevail in the relations among individuals.

References

1. Andenaes, J., Grunnlov og rettsskkerhet. Michelsens Insitut, Bergen, 1945.
2. Aubert V., The Rule of Law in „The Rule of Law", issue 1.
3. Aubert, V. The Rule of Law, in Rule of Law Journal, Issue 1.
4. Beccaria, C., Crimes and Punishment. Academy Publishing House, Budapest.
5. Békés I., Criminal Law General Part HVG ORAC Lap- Könyvkiadó Kft. Budapest, 2006.
6. Békés I., Judgement of the European Court of Human Rights in Streletz, Kessler and Krenz vs. Germany case. KJK-KERSZÖV Jogi és Üzleti Kiadó Kft. Budapest, 2004.
7. Belovics, E., Criminal Law I. HVG ORAC Publishing House Ltd., Budapest, 2017.
8. Földvári, J., Hungarian Criminal Law Osiris Kiadó, Budapest, 2003.
9. Gellér, B., Textbook on Hungarian Criminal Law. Volume I. General Part. Hungarian Official Journal Publisher, Budapest, 2008.
10. Kiss, Z., Issues of retroactivity in the light of the provisions relating to the temporal scope of the Criminal Code. Faculty of Law and Political Science of the Pázmány Péter Catholic University Budapest, 2000.
11. Kónya, I., The State's criminal justice power. National Institute of Criminology-Pázmány Péter Catholic University Faculty of Law and Political Sciences, Budapest.
12. Pokol, B., Criminal Law Theoretical Analysis Rejtjel Kiadó. Budapest, 2016.

[22] Andenaes J. Grunnlov og rettsskkerhet. Michelsens Insitut, Bergen, 1945. p. 86.
[23] Aubert, V. The Rule of Law, in Rule of Law Journal, Issue 1., p. 62.

Far and Beyond Territory. Lessons for the EU from the US Legal Practice

Dr. Flaviu Ciopec, LL.D*

Abstract

The principle of extraterritoriality in the US law gives the United States the power to enact (legal) standards that may apply to non-US legal subjects, as well. This is particularly the case of international corruption, where the American standards have been settled through the application of the Foreign Corrupt Practices Act ("the FCPA") of 1977. The present study explores the essentials of the FCPA addressing extraterritoriality as a legal principle in order to reveal the former's impact on the architecture of European criminal law. The FCPA imposes inter alia criminal and civil liability for (i) the bribery of foreign (i.e. non-US) officials; (ii) the failure of issuers' to maintain books and records that accurately reflect the disposition of company assets; and (iii) the failure of issuers' to institute proper internal controls concerning the authorization of transactions. The extraterritorial effect of the FCPA may manifest itself by that "covered entities" (i.e. parent issuer corporations and joint venture partners) can be held civilly and criminally liable for improper payments made by their subsidiaries or joint ventures. Such liability becomes possible if, for example, the issuer's subsidiary or joint venture makes improper payments, and the parent, member of the joint venture, or its employees "authorized, directed, or controlled the activity in question". Several European companies have been sanctioned on the FCPA basis: Siemens in 2008, Daimler and Alcatel in 2010, Alstom in 2014, Rolls-Royce in 2017, Ericsson in 2019 and Airbus in 2020. To date, the European Union does not practice its own extraterritoriality, or at least an extraterritoriality equivalent to the United States. It appears that this principle of extraterritoriality, when used as an economic or diplomatic tool, damages European companies and directly affects the sovereignty of the EU member states.

Keywords*: extraterritoriality, FCPA 1977, international corruption, US standards, European criminal law*

I. Introduction

International law, in general, as well as criminal international law, is based on the principle that "a state cannot take measures on the territory of another state by means of enforcement of its national laws without the consent of the latter"[1]. Usually, a sovereign state could grant such a consent to other states or their nationals, within certain limits and

* Associate Professor, Faculty of Law, West University of Timişoara. Contact: flaviu.ciopec@e-uvt.ro.

[1] Dover R., Frosini J., *The Extraterritorial Effects of Legislation and Policies in the EU and US*, 2012, [https://www.europarl.europa.eu/RegData/etudes/STUD/2012/433701/EXPO-AFET_ET(2012)433701_EN.pdf] p. 7.

based on reciprocity, by an international convention. A state acts "in excess of its own jurisdiction when its measures claim to regulate acts, which are done outside its territorial jurisdiction by persons who are not its own nationals and with no, or no substantial effect, within its territorial jurisdiction"[2]. Excessive and abusive assertion of jurisdiction could lead to international responsibility or protests at *ultra vires* acts[3].

Extraterritoriality generally refers to the unilateral use of measures that are taken under a state's sovereign powers to enforce its own law, in a territory other than its own, for actions committed outside its territory by entities or people from other countries.

As the doctrine pointed out[4], the territory is more a legal concept than a geographical one, being possible that one territory as a single legal unit to be composed of multiple geographical units that are not contiguous. Being primarily a legal concept, the territory determines the spatial jurisdiction of one state where its normative system is valid, effective and enforceable. Nonetheless, international law does not prohibit the states to extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory[5]. It is also accepted that a state has enforcement jurisdiction abroad only to the extent necessary to enforce its legislative jurisdiction.

Essentially, extraterritoriality was first conceived as part of criminal law and founded on several principles[6] that are exceptions from the general rule of the territoriality stated above. One such principle is the objective territorial principle also known as the ubiquity principle. According to the former, a state can assert (national) jurisdiction if a particular action has been committed on its own territory even if part of said action or merely its outcome has been performed or has occurred in another state. The jurisdiction of one's state is thus shaped out when any essential constituent of the offence is consummated on state territory. In this case, the jurisdiction extends naturally to all constitutive parts of a single offence, including those actions or results that are territorially linked with the foreign jurisdiction. As a consequence, the extraterritoriality in such cases is merely formal.

The nationality principle imposes that jurisdiction be established by reference (i) to nationality or the national side of the person who commits the offence; or (ii) to a person or the national interest injured by the offence. Similarly, to the above, this is not a genuinely extraterritorial case since nationality is still a strong feature of any sovereign state, where the national law follows a citizen for instance wherever he/she goes or whatever he/she suffers. It is natural that national jurisdiction apply to all persons who are linked from the beginning with that jurisdiction by means of citizenship, permanent residence or incorporation.

The same inference applies to the "substantial connection" principle whereby jurisdiction is established based on the real and substantial connection between

---

[2] Dover R., Frosini J. (2012), cited paper, pp. 7-8.

[3] Dover R., Frosini J. (2012), cited paper, p. 8.

[4] Valentin C., *Drept internațional* [International Law], Bucharest, Universul Juridic, 2010, p. 221.

[5] Permanent Court of International Justice, the case of S.S. Lotus, France v. Turkey Judgment no. 9 of 7 September 1927, para. 46, [https://web.archive.org/web/20101210073754/ http://www. worldcourts. com/ pcij/eng/decisions/ 1927/1927.09.07_lotus.htm].

[6] Redress / FIDH, *Extraterritorial Jurisdiction in the European Union. A Study of the Laws and Practice in the 27 Member States of the European Union*, London / Paris, 2010, [https://www.refworld.org/ pdfid/4d1a0104c.pdf] pp. 16-22.

companies or persons in different jurisdictions. In such case, the extraterritoriality is elusive since the connection is often a link between a parent-company and its subsidiaries or a relationship based on the guidance and direct control of one company/person to another. Acting abroad does not mean that national laws are inapplicable where it could be proved that, for instance, one person aids and abets another person. Substantially, such cases are also covered by the ubiquity principle.

Another exception is that of the universality principle, whereby jurisdiction is established based on the need to deal with certain crimes, usually internationally recognized. The universality principle is a real example of extraterritoriality since the jurisdiction of one state is applicable with no direct connection with the territory. The exception is based on the political will of the states to cooperate in order to prohibit a *de facto* immunity of an offender who commits a crime on a certain territory and escape to another territory. The universality principle determines jurisdiction by reference to the place where the person is held in custody.

However, the extent of the universality principle is limited to that crimes where a reaction is needed based on an international treaty or customary international law. Other crimes that are not part of such large consensus aimed at suppressing them cannot be prosecuted on the basis of extraterritoriality.

In brief, there is not much room for real extraterritoriality which is actually reduced to the cases where the universality principle is applicable. The following study explores the framework behind extraterritoriality in order to reveal if other situations except the universality principle have grown to be justified as real exceptions from the territorial standard. For instance, constituent elements of the federal states – territories, states, provinces – also invoke extraterritoriality. The principles of extraterritoriality developed at inter-state level are similar to those at intra-state level, despite the absence of the aspect of sovereignty in the former[7]. Thus, it is not a surprise that in the United States, a federal state, the legislators have a far stronger preference that their legal codes be enforceable outside the US territorial space.

II. The Foreign Corrupt Practices Act

Foreign Corrupt Practices Act could be interpreted as having an extraterritorial effect. The FCPA, codified at 15 US Code Chapter 2B §§ 78m, 78dd-1, 78dd-2, 78dd-3, 78ff, was enacted by the US Congress in 1977 as part of the 1934 Securities Exchange Act. In enacting the FCPA, Congress originally limited its jurisdictional scope to U.S. companies and individuals.

The FCPA is widely considered[8] being a "by-product of the Watergate scandal that revealed, among other things, certain unreported campaign contributions. This caused the US Securities and Exchange Commission to investigate undisclosed corporate payments to domestic and foreign governments and politicians. As part of a voluntary disclosure program, over 200 corporations (mostly Fortune 500 companies) admitted to making questionable payments to foreign government officials of over USD 300 million. This caused Congress to enact criminal and civil penalties for such illicit foreign payments made in exchange for business".

[7] Dover R., Frosini J. (2012), cited paper, p. 14.
[8] Dover R., Frosini J. (2012), cited paper, p. 24.

In 1988, the FCPA amended §§ 78dd-1, 78dd-2, 78dd-3 and added two very narrow affirmative defenses for (i) the payment, gift, offer, or promise of anything of value that was made, was *lawful under the written laws and regulations* of the foreign official's, political party's, party official's, or candidate's country; and (ii) the payment, gift, offer, or promise of anything of value that was made, was a *reasonable and bona fide expenditure*, such as travel and lodging expenses, incurred by or on behalf of a foreign official, party, party official, or candidate and was *directly related* to the promotion, demonstration, or explanation of products or services, or the execution or performance of a contract with a foreign government or agency thereof.

The 1998 amendments expanded the Act's jurisdiction to include foreign individuals and corporations. Today, the statute imposes criminal and civil liability for (i) the bribery of foreign (i.e., non-US) officials; (ii) the failure of "issuers" to maintain books and records that accurately reflect the disposition of company assets; and (iii) the failure of "issuers" to institute proper internal controls concerning the authorization of transactions.

"Foreign official" under the FCPA is defined as: "Any officer or employee of a foreign government or any department, agency or instrumentality thereof, or of a public international organization, or any person acting in an official capacity or on behalf of any such government, department, agency or instrumentality or for, or on behalf of any such public international organization" [15 USC. § 78dd-1(f)(1)(A)].

This definition includes "individuals appointed by a foreign head of state or by the head of an executive department, individuals whose day-to-day performance is supervised by a governmental authority, foreign legislators, officials of foreign municipalities, accountants, lawyers, other professionals acting on behalf of a government entity (e.g., physicians in publicly-owned hospitals), military officials, officials of state-owned companies and/or consortiums (of particular relevance in oil and gas contexts and circumstances in which privatization is in progress), certain officers of non-governmental organizations, and non-US political parties and candidates for political office outside the United States"[9].

The prohibitions applies to:

- *any issuer* which has a class of securities registered pursuant to 15 US Code Chapter 2B §§ 78l or which is required to file reports under 15 US Code Chapter 2B §§ 78o(d), or for any officer, director, employee, or agent of such issuer or any stockholder thereof acting on behalf of such issuer [15 US Code Chapter 2B §§ 78dd-1(a)];
- *any domestic concern*, other than an issuer which is subject to §§ 78dd–1, or for any officer, director, employee, or agent of such domestic concern or any stockholder thereof acting on behalf of such domestic concern [15 US Code Chapter 2B §§ 78dd-2(a)] where the term "domestic concern" means any individual who is a citizen, national, or resident of the United States; and any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship which has its principal place of business in the United States, or which is organized under the laws of a State of the United States or a territory, possession, or commonwealth of the United States [15 US Code Chapter 2B §§ 78dd-2(h)(1)];
- *any person* other than an issuer that is subject to §§ 78dd–1 or a domestic concern (as defined in §§ 78dd–2), or for any officer, director, employee, or agent of such person or any stockholder thereof acting on behalf of such person [15 US Code Chapter 2B §§ 78dd-3(a)] where the term "person", when referring to an offender, means any

[9] Dover R., Frosini J. (2012), cited paper, p. 25.

natural person other than a national of the United States or any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship organized under the law of a foreign nation or a political subdivision thereof [15 US Code Chapter 2B §§ 78dd-3(f)(1)].

FCPA expressly provide as an alternative jurisdiction that the prohibitions applies also to:

- any issuer organized under the laws of the United States, or a State, territory, possession, or commonwealth of the United States or a political subdivision thereof and which has a class of securities registered pursuant to 15 US Code Chapter 2B §§ 78l or which is required to file reports under 15 US Code Chapter 2B §§ 78o(d), or for any United States person that is an officer, director, employee, or agent of such issuer or a stockholder thereof acting on behalf of such issuer, to corruptly do any act outside the United States [15 US Code Chapter 2B §§ 78dd-1(g)(1)];
- any United States person to corruptly do any act outside the United States [15 US Code Chapter 2B §§ 78dd-2(i)(1)];

A violation of the anti-bribery provisions requires proof of the following constituent elements[10]:

- An issuer, a domestic concern or a person as defined above;
- That makes use of the mails or any means or instrumentality of interstate commerce;
- In furtherance of an offer, payment, promise to pay, or authorization to pay anything of value;
- To any foreign official as defined above, or to any foreign political party or official thereof, or any candidate for foreign political office, or other person while knowing that all or a portion of the payment would be passed on to a foreign official, foreign political party or official thereof or candidate for foreign political office;
- Inside the territory of the United States or, for any US issuer or domestic concern, outside the United States;
- To corruptly influence any official act or decision of a foreign official in his official capacity, induce an action or an omission to act in violation of a lawful duty, or to secure any improper advantage, or to induce a foreign official to use his influence with foreign government to affect or influence any act or decision of such government;
- In order to assist the offender in obtaining or retaining business for or with, or directing business to, any person.

A company that violates the FCPA's anti-bribery or accounting provisions may be subject to criminal fines and punishment, civil fines, and disgorgement.

Specifically, any issuer that violates §§ 78dd-1 shall be criminally fined not more than $2,000,000 and shall be subject to a civil penalty of not more than $10,000 imposed in an action brought by the US Securities and Exchange Commission. Any officer, director, employee, or agent of an issuer, or stockholder acting on behalf of such issuer, who willfully violates §§ 78dd-1 shall be fined not more than $100,000, or imprisoned not more than 5 years, or both. Whenever a fine is imposed upon any officer, director, employee, agent, or stockholder of an issuer, such fine may not be paid, directly or indirectly, by such issuer. Similar penalties are provided for any domestic concern for the violations of §§ 78dd-2 and for any natural person that is an

[10] Tarun R.W., *Basics of the Foreign Corrupt Practices Act*, Chicago, 2006, p. 3 [https://www.lw.com/upload/pubContent/_pdf/pub1287_1.pdf].

officer, director, employee, or agent of a domestic concern, or stockholder acting on behalf of such domestic concern. Similar penalties are also provided for any juridical person for the violation of §§ 78dd-3 and for any natural person who willfully violates that section.

Separately, any person who willfully violates any provision of the 15 US Code Chapter 2B (other than §§ 78dd-1, meaning accounting provisions), or any rule or regulation thereunder the violation of which is made unlawful or the observance of which is required under the terms of the 15 US Code Chapter 2B, or any person who willfully and knowingly makes, or causes to be made, any statement in any application, report, or document required to be filed or any rule or regulation thereunder or any undertaking contained in a registration statement as provided in 15 US Code Chapter 2B §§ 78o(d), or by any self-regulatory organization in connection with an application for membership or participation therein or to become associated with a member thereof which statement was false or misleading with respect to any material fact, shall upon conviction be fined not more than $5,000,000, or imprisoned not more than 20 years, or both, except that when such person is a person other than a natural person, a fine not exceeding $25,000,000 may be imposed; but no person shall be subject to imprisonment for the violation of any rule or regulation if he proves that he had no knowledge of such rule or regulation.

In addition to penalties for violating the FCPA itself, a corporation violating the FCPA exposes itself to a number of related consequences[11]. One of the most significant effects of violating the FCPA is the possibility of administrative sanctions. Indictment of a company can result in a suspension of its right to conduct business with the US government or its agencies. The US government may also revoke licenses and permits necessary to conduct one's business. This may effectively prevent a company from operating until an FCPA investigation is concluded. Indictment for bribery may also result in the suspension of a party from federal financial assistance and other non-financial benefits.

Both the US Department of Justice and the US Securities and Exchange Commission may enforce the FCPA. The Department of Justice has responsibility for all criminal enforcement of the FCPA, including criminal enforcement against issuers. The Securities and Exchange Commission has responsibility for civil enforcement of the anti-bribery and accounting provisions in cases involving issuers.

The past decade has seen increasingly aggressive enforcement of the FCPA. It is the result of a deliberate effort by the Department of Justice and the Securities and Exchange Commission to encourage compliance with the FCPA. The current increase in investigations and prosecutions has resulted from the US government's broad interpretation of the FCPA's text, and its insistence that parent companies are responsible for the actions of their foreign subsidiaries.

The extraterritorial effect of the FCPA manifests itself in that parent issuer corporations and joint venture partners can be held civilly and criminally liable for improper payments made by their subsidiaries or joint ventures. Such liability is possible if, for example, the issuer's subsidiary or joint venture makes improper payments, and the parent, member of the joint venture, or its employees "authorized, directed, or controlled the activity in question". For example, the Department of Justice's Criminal Resource Manual, the manual for federal prosecutors, addresses the

[11] Dover R., Frosini J. (2012), cited paper, p. 26.

scope of the FCPA as follows: "Although this has not yet been interpreted by any court, the Department interprets it as conferring jurisdiction whenever a foreign company or national causes an act to be done within the territory of the United States by any person acting as that company's or national's agent"[12]. Thus, under the Department's interpretation, the United States can bring a felony FCPA prosecution against a foreign national who has never set foot in the United States, provided that the foreign defendant caused some act in furtherance of the offense to take place in the United States[13]. Companies with global operations are clearly affected by enhanced FCPA enforcement[14].

Courts align with the government in the broad interpretation of the FCPA provisions. For instance, they have broadly interpreted the term "obtain or retain business" under the anti-bribery provision to include payments to government officials that are only loosely connected to a business purpose. The leading FCPA decision is in United States v. Kay[15] whereby the court dismissed an indictment for violation of the FCPA after the defendant argued that payments made to Haitian officials to reduce customs duties and sales tax on rice shipped to Haiti were not made to obtain or retain business because no government contract was sought. On appeal, the government successfully argued that such payments were within the scope of the FCPA's statutory language because the FCPA "covers payments that indirectly advance the payer's goal of obtaining or retaining foreign business". The government reasoned that a reduction in duties and taxes is the type of advantage that "always will assist in obtaining or retaining business in a foreign country". Relying on the FCPA's legislative history, the court stated that the FCPA applies "broadly to payments intended to assist the payer, either directly or indirectly, in obtaining or retaining business".

According to the above-mentioned it is reasonable to infer that the FCPA works under the ubiquity and substantial connection principles, and seeks to regulate the interaction between non-US officials and the foreign subsidiaries of US companies or companies organized under the laws of a state of the United States or a territory, possession, or commonwealth of the United States.

A clear manner in which the FCPA works in practice is presented in the following major cases instrumented against European corporations. Today, it appears that the principle of extraterritoriality, when used as an economic or diplomatic tool, damages European companies and directly affects the sovereignty of the EU member states[16].

III. The Siemens Case

According to the press release[17] of 15.12.2008 from the US Department of Justice:

"Siemens Aktiengesellschaft (Siemens AG), a German corporation, and three of its subsidiaries pleaded guilty to a two-count information charging criminal violations of

[12] DoJ / SEC, *A Resource Guide to the US Foreign Corrupt Practices Act*, 2015 [https://www.justice. gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf], p. 107.

[13] Tarun R.W., cited paper, p. 13.

[14] Dover R., Frosini J. (2012), cited paper, p. 26.

[15] United States Court of Appeals, Fifth Circuit, Decision of 4 February 2004, 359 F.3d 738 [https://casetext.com/case/us-v-kay-6].

[16] [http://www.europarl.europa.eu/doceo/document/E-8-2018-006496_EN.html].

[17] [https://www.justice.gov/archive/opa/pr/2008/December/08-crm-1105.html].

the FCPA's internal controls and books and records provisions. Siemens S.A. Argentina pleaded guilty to a one-count information charging conspiracy to violate the books and records provisions of the FCPA. Siemens Bangladesh Limited and Siemens S.A. Venezuela, each pleaded guilty to separate one-count information charging conspiracy to violate the anti-bribery and books and records provisions of the FCPA.

As the charging and plea documents reflect, beginning in the mid-1990s, Siemens AG engaged in systematic efforts to falsify its corporate books and records and knowingly failed to implement and circumvent existing internal controls. As a result of Siemens AG's knowing failures in and circumvention of internal controls, from the time of its listing on the New York Stock Exchange on March 12, 2001, through approximately 2007, Siemens AG made payments totaling approximately $1.36 billion through various mechanisms. Of this amount, approximately $554.5 million was paid for unknown purposes, including approximately $341 million in direct payments to business consultants for unknown purposes. The remaining $805.5 million of this amount was intended in whole or in part as corrupt payments to foreign officials through the payment mechanisms, which included cash desks and slush funds.

Beginning around September 1998 and continuing until 2007, Siemens S.A. Argentina made and caused to be made significant payments to various Argentine officials, both directly and indirectly, in exchange for favorable business treatment in connection with a $1 billion national identity card project. From the date that Siemens AG became listed on the New York Stock Exchange on March 12, 2001, through approximately January 2007, Siemens S.A. Argentina made approximately $31,263,000 in corrupt payments to various Argentine officials through purported consultants and other conduit entities, and improperly characterized those corrupt payments in its books and records as legitimate payments for 'consulting fees' or 'legal fees'. Siemens Argentina's books and records, including those containing the false characterizations of the corrupt payments, were part of the books and records of Siemens AG.

Beginning around November 2001 and continuing until approximately May 2007, Siemens S.A. Venezuela admitted it made and caused to be made corrupt payments of at least $18,782,965 to various Venezuelan officials, indirectly through purported business consultants, in exchange for favorable business treatment in connection with two major metropolitan mass transit projects called Metro Valencia and Metro Maracaibo. Some of those payments were made using U.S. bank accounts controlled by the purported business consultants.

Siemens Bangladesh Limited admitted that from May 2001 to August 2006, it caused corrupt payments of at least $5,319,839 to be made through purported business consultants to various Bangladeshi officials in exchange for favorable treatment during the bidding process on a mobile telephone project. At least one payment to each of these purported consultants was paid from a U.S. bank account.

In connection with the cases brought by the Department of Justice, the US Securities and Exchange Commission and the Munich Public Prosecutor's Office, Siemens AG will pay a combined total of more than $1.6 billion in fines, penalties and disgorgement of profits, including $800 million to U.S. authorities, making the combined U.S. penalties the largest monetary sanction ever imposed in an FCPA case since the act was passed by Congress in 1977. Siemens AG agreed to retain an independent compliance monitor for a four-year period to oversee the continued implementation and maintenance of a robust compliance program and to make reports to the company and the Department of Justice. Siemens AG also agreed to

continue fully cooperating with the Department in ongoing investigations of corrupt payments by company employees and agents".

The short presentation of the case is sufficient to understand the key element of the US jurisdiction: listing of Siemens AG on the New York Stock Exchange on March 12, 2001 and using US bank accounts for improper payments made by Siemens Bangladesh and Siemens Venezuela. Simply stated, it is a federal crime for companies traded on U.S. markets to pay bribes in return for business. There is no extraterritoriality case here, but pure national jurisdiction, which reflects the FBI's dedication to enforce the provisions of the Foreign Corrupt Practices Act.

IV. The Daimler Case

According to the press release[18] of 01.04.2010 from the US Department of Justice:

"Daimler AG, a German corporation, and three of its subsidiaries DaimlerChrysler Automotive Russia SAO, now known as Mercedes-Benz Russia SAO, its German subsidiary, Export and Trade Finance GmbH, and DaimlerChrysler China Ltd., now known as Daimler North East Asia Ltd., each pleaded guilty to criminal information charging the companies with one count of conspiracy to violate the anti-bribery provisions of the FCPA and one count of violating those provisions.

Daimler AG, whose shares trade on multiple exchanges in the United States, engaged in a long-standing practice of paying bribes to foreign government officials through a variety of mechanisms, including the use of corporate ledger accounts known internally as 'third-party accounts', corporate 'cash desks', offshore bank accounts, deceptive pricing arrangements and third-party intermediaries. Daimler AG and its subsidiaries made hundreds of improper payments worth tens of millions of dollars to foreign officials in at least 22 countries – including China, Croatia, Egypt, Greece, Hungary, Indonesia, Iraq, Ivory Coast, Latvia, Nigeria, Russia, Serbia and Montenegro, Thailand, Turkey, Turkmenistan, Uzbekistan, Vietnam and others – to assist in securing contracts with government customers for the purchase of Daimler vehicles. In some cases, Daimler AG or its subsidiaries wire transferred these improper payments to U.S. bank accounts or to the foreign bank accounts of U.S. shell companies, in order for those entities to pass on the bribes. Within Daimler AG and its subsidiaries, bribe payments were often identified and recorded as 'commissions', 'special discounts', and/or 'nützliche Aufwendungen' or 'N.A.' payments, which translates to 'useful payment' or 'necessary payment', and was understood by certain Daimler employees to mean 'official bribe'. In all cases, Daimler AG improperly recorded these corrupt payments in its corporate books and records. Daimler AG admitted that it earned more than $50 million in profits from corrupt transactions with a nexus to the territory of the United States. Daimler AG also admitted that it agreed to pay kickbacks to the former Iraqi government in connection with contracts to sell vehicles to Iraq under the U.N.'s Oil for Food program.

DaimlerChrysler Automotive Russia SAO admitted that it made improper payments to Russian federal and municipal government officials to secure contracts to sell vehicles by over-invoicing the customer and paying the excess amount back to the

[18] [https://www.justice.gov/opa/pr/daimler-ag-and-three-subsidiaries-resolve-foreign-corrupt -practices- act-investigation-and].

government officials, or to other designated third parties that provided no legitimate services to the company. Its employees caused the wire transfer of payments from Daimler AG's bank accounts in Germany to, among other destinations, U.S. and Latvian bank accounts held by shell companies with the understanding that the money, in whole or in part, was for the benefit of Russian government officials.

Export and Trade Finance GmbH admitted that it made corrupt payments directly to Croatian government officials and to third parties, including two U.S.-based corporate entities, with the understanding that the payments would be passed on, in whole or in part, to Croatian government officials, to assist in securing the sale of 210 fire trucks.

DaimlerChrysler China Ltd., admitted that it made improper payments in the form of commissions, delegation travel, and gifts for the benefit of Chinese government officials or their designees in connection with sales of commercial vehicles and Unimogs to various Chinese government customers. The company admitted that in certain cases it used U.S.-based agents to facilitate the bribe payments".

In total, Daimler AG and its subsidiaries agreed to pay $93.6 million in criminal fines and $91.4 million in disgorgement of profits relating to a related civil complaint filed by the U.S. Securities and Exchange Commission (SEC). Moreover, Daimler AG agreed to retain an independent compliance monitor for a three-year period to oversee the company's continued implementation and maintenance of an FCPA compliance program, and to make reports to the company and the Department of Justice.

As in the Siemens case, the relevant elements that entails the US jurisdiction were the trading of the Daimler AG's shares on the exchanges in the United States (meaning that Daimler AG is an issuer in sense of the 15 US Code Chapter 2B §§ 78dd-1(a), abovementioned) and the using US bank accounts for improper payments. All these elements are specific to the territorial approach being unreasonable to claim that the regulations voluntarily admitted by the company when listed to the stock exchange were not applicable, in case of violation.

V. The Alcatel Case

According to the press release[19] of 27.12.2010 from the US Department of Justice:

"Alcatel-Lucent S.A., a French telecommunications equipment and services company, and three of its subsidiaries (Alcatel CIT S.A., Alcatel Standard A.G., and Alcatel de Costa Rica S.A.) faced a criminal information with one count of violating the internal control provisions of the FCPA, and one count of violating the books and records provisions of the FCPA. The three subsidiaries were each charged with conspiring to violate the anti-bribery, books and records, and internal controls provisions of the FCPA.

Starting in the 1990s and prior to its 2006 merger with Lucent Technologies Inc., Alcatel pursued many of its business opportunities around the world through subsidiaries like Alcatel CIT and Alcatel de Costa Rica using third-party agents and consultants who were retained by Alcatel Standard. This business model was shown to be prone to corruption, as consultants were repeatedly used as conduits for bribe payments to foreign officials and business executives of private customers to obtain or

[19] [https://www.justice.gov/opa/pr/alcatel-lucent-sa-and-three-subsidiaries-agree-pay-92-million-resolve-foreign-corrupt].

retain business in many countries. Specifically, Alcatel CIT won three contracts in Costa Rica worth a combined total of more than $300 million as a result of corrupt payments to government officials and from which Alcatel reaped a profit of more than $23 million. Alcatel CIT wired more than $18 million to two consultants in Costa Rica, which had been retained by Alcatel Standard, in connection with obtaining business in that country. According to court documents, more than half of this money was then passed on by the consultants to various Costa Rican government officials for assisting Alcatel CIT and Alcatel de Costa Rica in obtaining and retaining business. As part of the scheme, the consultants created phony invoices that they then submitted to Alcatel CIT. According to court documents, senior Alcatel executives approved the retention of and payments to the consultants despite obvious indications that the consultants were performing little or no legitimate work.

In addition, Alcatel Standard hired a consultant in Honduras who was a perfume distributor with no experience in telecommunications. The consultant was retained after being personally selected by the brother of a senior Honduran government official. Alcatel CIT executives knew that a significant portion of the money paid to the consultant would be paid to the family of the senior Honduran government official in exchange for favorable treatment of Alcatel CIT. As a result of these payments, Alcatel CIT was able to retain contracts worth approximately $47 million and from which Alcatel earned $870,000.

Moreover, Alcatel Standard retained two consultants on behalf of another Alcatel subsidiary in Taiwan (Alcatel SEL) to assist in obtaining an axle counting contract worth approximately $19.2 million. Alcatel and its joint venture paid these two consultants more than $950,000 despite the fact that neither consultant had telecommunications experience. In fact, Alcatel Standard's purpose for hiring the consultants was so that Alcatel SEL could funnel payments through the consultants to Taiwanese legislators who had influence in the award of the contract. Alcatel earned approximately $4.34 million from this contract.

Department of Justice and Alcatel-Lucent reached a settlement in which the corporation consented to pay a combined $92 million penalty to resolve the FCPA investigation into the worldwide sales practices of Alcatel S.A. In addition to the $92 million penalty, Alcatel-Lucent and its three subsidiaries agreed to implement rigorous compliance enhancements. Alcatel-Lucent also agreed to retain an independent compliance monitor for a three-year period to oversee the company's implementation and maintenance of an enhanced FCPA compliance program and to submit yearly reports to the Department of Justice. In a related matter, the U.S. Securities and Exchange Commission asked and obtained a permanent injunction against FCPA violations and the payment of $45,372,000 in disgorgement and prejudgment interest".

VI. The Alstom Case

According to the press release[20] of 22.12.2014 from the US Department of Justice:

"Alstom S.A., a French power and transportation company, pleaded guilty to a two-count criminal information charging the company with violating the FCPA by falsifying its books and records and failing to implement adequate internal controls. In

[20] [https://www.justice.gov/opa/pr/alstom-pleads-guilty-and-agrees-pay-772-million-criminal-penalty-resolve-foreign-bribery].

addition, Alstom Network Schweiz AG, formerly Alstom Prom, Alstom S.A.'s Swiss subsidiary, pleaded guilty to a criminal information charging the company with conspiracy to violate the anti-bribery provisions of the FCPA. Alstom Power Inc. and Alstom Grid Inc., two U.S. subsidiaries, both entered into deferred prosecution agreements, admitting that they conspired to violate the anti-bribery provisions of the FCPA. Alstom Power is headquartered in Windsor, Connecticut, and Alstom Grid, formerly Alstom T&D, was headquartered in New Jersey.

Alstom S.A. and its subsidiaries, through various executives and employees, paid bribes to government officials and falsified books and records in connection with power, grid and transportation projects for state-owned entities around the world, including in Indonesia, Egypt, Saudi Arabia, the Bahamas and Taiwan. In Indonesia, for example, bribes was paid to government officials – including a high-ranking member of the Indonesian Parliament and high-ranking members of Perusahaan Listrik Negara, the state-owned electricity company in Indonesia – in exchange for assistance in securing several contracts to provide power-related services valued at approximately $375 million. In total, Alstom S.A. paid more than $75 million to secure $4 billion in projects around the world, with a profit to the company of approximately $300 million. Alstom S.A. and its subsidiaries also attempted to conceal the bribery scheme by retaining consultants purportedly to provide consulting services on behalf of the companies, but who actually served as conduits for corrupt payments to the government officials".

Alstom S.A. agreed to pay $772 million criminal penalty to resolve foreign bribery charges, being the largest-ever foreign bribery resolution with the Department of Justice. This case is emblematic of how the Department of Justice investigates and prosecutes FCPA cases – and other corporate crimes from the perspective of domestic jurisdiction. Again no reference to extraterritoriality was made, but to the fact that two Alstom S.A.'s subsidiaries were in fact incorporated in US and therefore bound by US regulations.

VII. The Rolls-Royce Case

According to the press release[21] of 17.01.2017 from the US Department of Justice:

"Rolls-Royce plc, the United Kingdom-based manufacturer and distributor of power systems for the aerospace, defense, marine and energy sectors, admitted that between 2000 and 2013, the company conspired to violate the FCPA by paying more than $35 million in bribes through third parties to foreign officials in various countries in exchange for those officials' assistance in providing confidential information and awarding contracts to Rolls-Royce and affiliated entities.

In Thailand, Rolls-Royce admitted to using intermediaries to pay approximately $11 million in bribes to officials at Thai state-owned and state-controlled oil and gas companies that awarded approximately seven contracts to Rolls-Royce during the same time period.

In Brazil, Rolls-Royce used intermediaries to pay approximately $9.3 million in bribes to bribe foreign officials at a state-owned petroleum corporation that awarded multiple contracts to Rolls-Royce during the same time period.

---

[21] [https://www.justice.gov/opa/pr/rolls-royce-plc-agrees-pay-170-million-criminal-penalty-resolve-foreign-corrupt-practices-act].

In Kazakhstan, between approximately 2009 and 2012, Rolls-Royce paid commissions of approximately $5.4 million to multiple advisors, knowing that at least a portion of the commission payments would be used to bribe foreign officials with influence over a joint venture owned and controlled by the Kazakh and Chinese governments that was developing a gas pipeline between the countries. In 2012, the company also hired a local Kazakh distributor, knowing it was beneficially owned by a high-ranking Kazakh government official with decision-making authority over Rolls-Royce's ability to continue operating in the Kazakh market. During this time, the state-owned joint venture awarded multiple contracts to Rolls-Royce.

In Azerbaijan, between approximately 2000 and 2009, Rolls-Royce used intermediaries to pay approximately $7.8 million in bribes to foreign officials at the state-owned and state-controlled oil company, which awarded multiple contracts to Rolls-Royce during the same time period.

In Angola, between approximately 2008 and 2012, Rolls-Royce used an intermediary to pay approximately $2.4 million in bribes to officials at a state-owned and state-controlled oil company, which awarded three contracts to Rolls-Royce during this time period.

In Iraq, from approximately 2006 to 2009, Rolls-Royce supplied turbines to a state-owned and state-controlled oil company. Certain Iraqi foreign officials expressed concerns about the turbines and subsequently threatened to blacklist Rolls-Royce from doing future business in Iraq. In response, Rolls-Royce's intermediary paid bribes to Iraqi officials to persuade them to accept the turbines and not blacklist the company.

Rolls-Royce entered into a deferred prosecution agreement in connection with a criminal information charging the company with conspiring to violate the anti-bribery provisions of the FCPA. Pursuant to the DPA, Rolls-Royce agreed to pay a criminal penalty of $169,917,710, and the amount of penalties of more than $800 million. The company has also agreed to continue to cooperate fully with the department's ongoing investigation, including its investigation of individuals".

This outcome is a reflection of the immense reach and capabilities of the FBI's international anti-corruption squad and the global impact of the anti-corruption program.

VIII. The Ericsson Case

According to the press release[22] of 06.12.2019 from the US Department of Justice:

"Telefonaktiebolaget LM Ericsson, a multinational telecommunications company headquartered in Stockholm, Sweden, has agreed to enter into a deferred prosecution agreement with the department in connection with a criminal information charging the company with conspiracies to violate the anti-bribery, books and records, and internal controls provisions of the FCPA. The Ericsson subsidiary, Ericsson Egypt Ltd, pleaded guilty today to a one-count criminal information charging it with conspiracy to violate the anti-bribery provisions of the FCPA.

[22] [https://www.justice.gov/opa/pr/ericsson-agrees-pay-over-1-billion-resolve-fcpa-case].

Between 2010 and 2014, Ericsson, via a subsidiary, made approximately $2.1 million in bribe payments to high-ranking government officials in Djibouti in order to obtain a contract with the state-owned telecommunications company valued at approximately €20.3 million to modernize the mobile networks system in Djibouti. In order to effectuate the scheme, an Ericsson subsidiary entered into a sham contract with a consulting company and approved fake invoices to conceal the bribe payments. Ericsson employees also completed a draft due diligence report that failed to disclose the spousal relationship between the owner of the consulting company and one of the high-ranking government officials.

In China, between 2000 and 2016, Ericsson subsidiaries caused tens of millions of dollars to be paid to various agents, consultants and service providers, a portion of which was used to fund a travel expense account in China that covered gifts, travel and entertainment for foreign officials, including customers from state-owned telecommunications companies. Ericsson used the travel expense account to win business with Chinese state-owned customers. In addition, between 2013 and 2016, Ericsson subsidiaries made payments of approximately $31.5 million to third party service providers pursuant to sham contracts for services that were never performed. The purpose of these payments was to allow Ericsson's subsidiaries in China to continue to use and pay third party agents in China in contravention of Ericsson's policies and procedures. Ericsson knowingly mischaracterized these payments and improperly recorded them in its books and records.

In Vietnam, between 2012 and 2015, Ericsson subsidiaries made approximately $4.8 million in payments to a consulting company in order to create off-the-books slush funds, associated with Ericsson's customers in Vietnam that were used to make payments to third parties who would not be able to pass Ericsson's due diligence processes. Ericsson knowingly mischaracterized these payments and improperly recorded them in Ericsson's books and records.

Similarly, in Indonesia, between 2012 and 2015, an Ericsson subsidiary made approximately $45 million in payments to a consulting company in order to create off-the-books slush funds, and concealed the payments on Ericsson's books and records.

In Kuwait, between 2011 and 2013, an Ericsson subsidiary promised a payment of approximately $450,000 to a consulting company at the request of a sales agent, and then entered into a sham contract with the consulting company and approved a fake invoice for services that were never performed in order to conceal the payment. The sales agent provided an Ericsson employee with inside information about a tender for the modernization of a state-owned telecommunications company's radio access network in Kuwait. An Ericsson subsidiary was awarded the contract valued at approximately $182 million; Ericsson subsequently made the $450,000 payment to the consulting company and improperly recorded it in its books.

As part of the deferred prosecution agreement, Ericsson has agreed to pay total penalties of more than $1 billion to resolve the government's investigation into violations of the FCPA. This includes a criminal penalty of over $520 million and approximately $540 million to be paid to the U.S. Securities and Exchange Commission (SEC) in a related matter. Ericsson has accepted to continue to cooperate with the department in any ongoing investigations and prosecutions relating to the conduct, including of individuals; to enhance its compliance program; and to retain an independent compliance monitor for three years".

IX. The Airbus Case

According to the press release[23] of 31.01.2020 from the US Department of Justice:

"Airbus SE, a global provider of civilian and military aircraft based in France, has agreed to enter into a deferred prosecution agreement with the department in connection with a criminal information charging the Company with conspiracy to violate the anti-bribery provision of the FCPA and conspiracy to violate the Arms Export Control Act (AECA) and its implementing regulations, the International Traffic in Arms Regulations (ITAR), in the United States. The FCPA charge arose out of Airbus's scheme to offer and pay bribes to foreign officials, including Chinese officials, in order to obtain and retain business, including contracts to sell aircraft. The AECA charge stems from Airbus's willful failure to disclose political contributions, commissions or fees to the U.S. government, as required under the ITAR, in connection with the sale or export of defense articles and defense services to the Armed Forces of a foreign country or international organization.

Beginning in at least 2008 and continuing until at least 2015, Airbus engaged in and facilitated a scheme to offer and pay bribes to decision makers and other influencers, including to foreign officials, in order to obtain improper business advantages and to win business from both privately owned enterprises and entities that were state-owned and state-controlled. In furtherance of the corrupt bribery scheme, Airbus employees and agents, among other things, sent emails while located in the United States and participated in and provided luxury travel to foreign officials within the United States.

In order to conceal and to facilitate the bribery scheme, Airbus engaged certain business partners, in part, to assist in the bribery scheme. Between approximately 2013 and 2015, Airbus engaged a business partner in China and knowingly and willfully conspired to make payments to the business partner that were intended to be used as bribes to government officials in China in connection with the approval of certain agreements in China associated with the purchase and sale of Airbus aircraft to state-owned and state-controlled airlines in China. In order to conceal the payments and to conceal its engagement of the business partner in China, Airbus did not pay the business partner directly but instead made payments to a bank account in Hong Kong in the name of a company controlled by another business partner.

Pursuant to the AECA and ITAR, the Department of State's Directorate of Defense Trade Controls regulates the export and import of U.S. defense articles and defense services, and prohibits their export overseas without the requisite licensing and approval of the authority.

Between December 2011 and December 2016, Airbus filed numerous applications for the export of defense articles and defense services to foreign armed forces. As part of its applications, Airbus was required under the ITAR to provide certain information related to political contributions, fees or commissions paid in connection with the sale of defense articles or defense services. However, the Company engaged in a criminal conspiracy to knowingly and willfully violate the AECA and ITAR, by failing to provide accurate information related to commissions

---

[23] [https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign- bribery-and-itar-case].

paid by Airbus to third-party brokers who were hired to solicit, promote or otherwise secure the sale of defense articles and defense services to foreign armed forces.

The company's payment to the United States was $527 million for the FCPA and ITAR violations, and an additional 50 million Euros (approximately $55 million) as part of a civil forfeiture agreement for the ITAR-related conduct. In addition, the Company has agreed to pay a $10 million penalty to the U.S. Department of State's Directorate of Defense Trade Controls. In related proceedings, the Company settled with the Parquet National Financier in France over bribes paid to government officials and non-governmental airline executives in China and multiple other countries and the Company has agreed to pay more than 2 billion Euros (more than approximately $2.29 billion). As part of this coordinated global resolution, the Company also entered into a deferred prosecution agreement with the United Kingdom's Serious Fraud Office (SFO) over bribes paid in Malaysia, Sri Lanka, Taiwan, Indonesia and Ghana, and the Company has agreed to pay approximately 990 million Euros equivalent (approximately $1.09 billion). As part of the deferred prosecution agreement with the department, Airbus has agreed to continue to cooperate with the department in any ongoing investigations and prosecutions relating to the conduct, including of individuals, and to enhance its compliance program".

The pay combined penalties of more than $3.9 billion is the largest global foreign bribery resolution to date.

The jurisdiction of the US was entailed by passive personality principle according to which international corruption involving sensitive U.S. defense technology presents a particularly dangerous combination. Airbus falsely reported information about their conduct to the U.S. government for more than five years in order to gain valuable licenses to export U.S. military technology. The bribery of government officials, specifically those involved in the procurement of U.S. military technology, posed a national security threat to both the U.S. and its allies. Due to its sensitivity the investigation and prosecution of cases involving the export of military and strategic commodities and technology were supervised by the Counterintelligence and Export Control Section.

X. Conclusions

US legislators use extraterritorial measures to advance US foreign policy interests and political norms, and in defense of domestic market conditions (financial markets and copyright materials). The politics behind these positions are clear: in a globalized world the US believes its interests are universally applicable and thus should be actionable and defensible universally[24].

The FCPA was indirect diplomatic tool, and should be viewed in a wider political, diplomatic (military, and economic), and competitive context. To view these legislative case studies only in terms of their legal function is to miss some of the key ways in which the EU can protect and advance its own interests. To date, the European Union does not practice its own extraterritoriality, or at least an extraterritoriality equivalent to the United States. When the EU intervenes beyond its

[24] Dover R., Frosini J. (2012), cited paper, p. 39.

territorial borders to sanction foreign individuals or entities, it is as a consequence of actions committed on European territory, actions which have a direct effect on the European Union, or actions which concern EU nationals[25]. The EU prohibits European companies to comply with US extraterritorial sanctions, but this regulation has never been applied in practice[26]. Companies are faced with the choice to lose access to the American market or even an American penalty on the one hand, and the threat of a European fine on the other. As no European company that is complying with American embargoes has been sanctioned to date, the choice for companies is clear.

So far EU has refrained from doing so out of a respect for state sovereignty, a founding principle of the current Westphalian international legal order. Nevertheless the EU could build an autonomous extraterritorial system, analogous to the American system: same legal instruments, same organizational structures and same judicial control. The fight against corruption, in particular, could represent a good practice on the issue to the European level. O this matter, the EU could adopt new regulations to improve existing standards and provide them with extraterritorial jurisdiction. Until now, some European governments have enacted similar legislation to regulate the behavior of companies registered in their jurisdiction (e.g. UK Bribery Act 2010, which is compliant with the 1997 Organization for Economic Cooperation and Development Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, which entered into force on 15 February1999.

References

1. DoJ / SEC, *A Resource Guide to the US Foreign Corrupt Practices Act*, 2015 [https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf],

2. Dover R., Frosini J., *The Extraterritorial Effects of Legislation and Policies in the EU and US*, 2012, [https://www.europarl.europa.eu/RegData/etudes/STUD/2012/433701/EXPO-AFET_ ET(2012)433701_EN.pdf]

3. http://www.europarl.europa.eu/doceo/document/E-8-2018-006496_EN.html.

4. https://www.justice.gov/archive/opa/pr/2008/December/08-crm-1105.html.

5. https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case.

6. https://www.justice.gov/opa/pr/alcatel-lucent-sa-and-three-subsidiaries-agree-pay-92-million-resolve-foreign-corrupt

7. https://www.justice.gov/opa/pr/alstom-pleads-guilty-and-agrees-pay-772-million-criminal-penalty-resolve-foreign-bribery

8. https://www.justice.gov/opa/pr/daimler-ag-and-three-subsidiaries-resolve-foreign-corrupt-practices-act-investigation-and.

9. https://www.justice.gov/opa/pr/ericsson-agrees-pay-over-1-billion-resolve-fcpa-case

[25] Jacques Delors Institute, *EU and US Sanctions: Which Sovereignty?* Policy Paper no. 232, Paris, 2018, [https://institutdelors.eu/wp-content/uploads/2018/10/EUandUSsanctionswhichsovereignty-Lamyetalii-Oct18. pdf] p. 2.

[26] Jacques Delors Institute, cited paper, p. 3.

10. https://www.justice.gov/opa/pr/rolls-royce-plc-agrees-pay-170-million-criminal-penalty-resolve-foreign-corrupt-practices-act

11. Jacques Delors Institute, *EU and US Sanctions: Which Sovereignty?* Policy Paper no. 232, Paris, 2018, [https://institutdelors.eu/wpcontent/uploads/2018/10/EUand USsanctionswhich sovereignty-Lamyetalii-Oct 18. pdf].

12. Permanent Court of International Justice, the case of S.S. Lotus, France v. Turkey Judgment no. 9 of 7 September 1927, [https://web.archive.org/web/20101210073754/http://www.worldcourts.com/pcij/eng/decisions/ 1927/1927.09.07_lotus.htm].

13. Redress / FIDH, *Extraterritorial Jurisdiction in the European Union. A Study of the Laws and Practice in the 27 Member States of the European Union*, London / Paris, 2010, [https://www.refworld.org/pdfid/4d1a0104c.pdf].

14. Tarun R.W., *Basics of the Foreign Corrupt Practices Act*, Chicago, 2006, [https://www.lw.com/upload/pubContent/_pdf/pub1287_1.pdf].

15. United States Court of Appeals, Fifth Circuit, Decision of 4 February 2004, 359 F.3d 738 [https://casetext.com/case/us-v-kay-6].

16. Valentin C., *Drept internațional* [International Law], Bucharest, Universul Juridic, 2010.

The Possible Impact of the COVID-19 On Crime Rates in Hungary

***Dr. László István Gál*[1]**

Abstract

The present study aims to make conservative predictions about the future trends of the criminality in Hungary, based on the experiences of the past centuries worldwide. So our initial hypothesis is that criminality is likely to increase from the second half of 2020, and this increase will continue for at least 1-2 years, after 2020. The only question is the extent of the rise and how we can slow or moderate the rise. In the time of the economic crisis the criminal law is a necessary but not sufficient tool for combating crime. If we know the past tendencies, we can prepare for the challenges of the future. We can respond before, during, or after problems arise. The earlier we move, the higher the efficiency can be.

Keywords: *economic crisis, COVID-19, Wuhan, crime, trend, ecomomy, unemployment, GDP, Hungary, criminality*

I. The Signs of World Economic Crises Beginning in 2020

The economists agree that the world epidemic entering 2019 ends from Chinese Wuhan that caused by the COVID-19 virus, better known as the coronavirus will generate a severe economic crisis in 2020. Still, its effects will be sensible in the next years. As always, there is an optimistic, a realistic and a pessimistic scenario. According to some opinions, the world economy will soon recover from the economic crisis; the majority now expect a crisis of greater or lesser duration. Still, in the worst-case scenario, it will be even worse than the Great Depression of 1929-33. The Center for Economics and Business Research (CEBR) has compiled the most pessimistic forecast to date on the short-term outlook for the world economy. Announced: the model calculations prove that this year's global economic recession has become practically inevitable and is expected to be twice as deep as the downturn in 2009. According to the house reviewed forecast the global GDP rate in 2020 will drop at least with 4 percent. The study emphasizes that this would be the deepest global recession since 1931 discounting the wartime years. According to the calculations by CEBR's London analysts, the Italian domestic total output is expected to fall by 11 percentages in this year, the German and the Spanish GDP rate equally with eight percentages, and the performance of the US economy with five percent[2]. We can also

[1] Head of the Criminal Law Department, University of Pécs, Faculty of Law; contact: gal.istvan@ajk.pte.hu.

[2] https://www.portfolio.hu/gazdasag/20200323/figyelmeztettek-1931-ota-nem-latott-valsag-koszonthet-a-vilagra-421466 (2020. 03. 26.)

talk about optimistic, realistic and pessimistic versions about the expected increase in crime. Still, one thing seems inevitable: the number of crimes will increase even according to the most optimistic estimates.

At the beginning of the 21st century seemed that international terrorism would be the cause of main economic troubles, instead of this, at the end of 2007 we were greeted by a "classic" global financial crisis. By 2007-2008, the world economy turned into the descending branch of the so-called Kondratyev cycle, and many disasters worsened the situation. For example, the hurricane in New Orleans. Because of the impregnation of the credit market, banks turned to secondary debtors. There was no severe credit review; real estate prices continuously raised. In 2006, more and more credit collapsed, so several real estate agencies became bankrupted, which also took some banks along with them. Out of these bankruptcies the most well-known is the Lehman Brothers. The crisis soon spilt over into the real economy. The root causes of the crisis are still being debated by leading economists. Yet, President Bush's big tax cuts program, which has suddenly left billions of dollars within the population, has undoubtedly played a role, further boosting credit supply to banks. Since the Great Depression of the 20th century, the situation called the most significant economic crisis emerged in 2008 from a global financial crisis that preceded it. The resultant of this the mortgage crisis in the United States, which affected the real estate market for the first time. The real causes of the economic crisis of 2008 have been explained by several experts in many ways. Investigations have often come to very different and not infrequently contradictory conclusions. Overall, it can be said that a complex process has resulted in a global economic crisis by 2008, which has spread from the Americas to the whole world in a short time. There is also a broad consensus among some theories that the immediate cause of the economic crisis was the collapse of the US mortgage bubble[3].

The global economic crisis that erupted in 2020 first started as a health crisis in China (Wuhan) and according to the already mentioned pessimistic scenario is expected to shake the world economy, and in particular Europe, more than the financial crisis of 2008 or crisis caused by the terrorist attacks on September 11, 2001[4]. What can be seen from the current crisis without any special visionary skills:

1) the coronavirus is expected to claim more deaths worldwide than international terrorism has so far collective in world history,

2) the global economic crisis generated by COVID-19 will be comparable with 2008, and with the 1929-33 crisis. The current situation can be even more severe than the other two downfalls.

---

[3] Halm Tamás: A gazdasági válság. Okok és tanulságok. [The economic crises. Causes and lessons, In: Kommentár 2009/6. p. 97.

[4] IMF, Managing Director, Kristalina Georgieva has painted a devastating picture of the economic impact of the epidemic, according to her even 2021 will not necessarily be about recovery. According to her, the 9 trillion dollars that various governments have already voted for so far will not be enough. Barely a month ago, we had been expecting a definite increase in per capita income in more than 160 of our member states. Today, everything was on top of our heads; we can already see that per capita growth will be negative in more than 170 countries – Georgieva said. The IMF director noted that because it is not known how long the epidemic will last, the outlook is very uncertain, she believes that if the pandemic subsides in the second half of the year, 2021 may already be a year of partial recovery, but the situation may worsen. Investors have already withdrawn more than a hundred billion dollars from these economies, three times as much as during the 2008 economic crisis.

https://index.hu/gazdasag/2020/04/09/imf_igazgato_nagy_gazdsagi_vilagvalsag_ota_nem_volt_ekkora_recesszio_jarvany/ (2020. 04. 10.).

3) Like any economic crisis, this will also have an impact on crime, and the number of known crimes in specific categories of crimes will be increased at least temporarily.

The present study aims to make conservative predictions based on the experiences of the past centuries. So our initial hypothesis is that criminality is likely to increase from the second half of 2020, and this increase will continue for at least 1-2 years, after that. The only question is the extent of the rise and how we can slow or moderate the rise. A recent excellent study that introduces and examines substantive criminal and infringement law rules related to the coronavirus also comes to a similar conclusion: „The coronavirus pandemic means a significant drawback for the life of the whole society, a sin order to protect life and health, we have to give up several of our activities which have been considered natural, and we can only exercise the right to relocate in a minimal extent. We can only hope that we can survive this period with as little human loss as possible until an effective vaccine will be available to protect against the virus. Until then, we must all be prepared for the fact that the emergency will last even longer, which is expected to mean a recession for the economy. This circumstance – for example, due to the loss of many jobs – could also have a criminogenic effect. After the favorable crime trend of recent years, it cannot be ruled out that the number of criminal offences will increase again as a result of the global crisis. Law enforcement authorities and the actors of criminal justice also have to expect this scenario”[5].

II. The Impact of Economic Crises on Crime Over the Last Two Centuries

Looking for a correlation between economic indicators and crime is not a recent research topic. Between 1835 and 1861, based on Bavarian data series, Georg von Mayr showed a quantifiable relationship between changes in grain prices and the number of thefts. The rise in the amount of grain has led to an increase in thefts and vice versa[6].

In the 1880s, Lacassagne, a famous French criminal lawyer and criminologist, also examined the relationship between economic factors and the development of crime. He sought to discover that changes in wheat prices go in parallel with changes in the number of crimes against property and that the effects of economic crises are also evident[7].

Crime statistics indicated similarly during the USA’s economic crisis of the 1890s. “At the start of the crisis, newspapers reported a huge increase in corruption. On January 1, 1895, article, the Chicago Daily Tribune reported the largest number of embezzlement schemes in 1894 since 1878, which had also been a year of serious depression."[8]

---

[5] Ambrus István: A koronavírus-járvány és a büntetőjog MTA Law Working Papers 2020/5. Budapest, 2020. 22. p. file:///C:/Users/USERUJ/Downloads/2020_5_Ambrus.pdf (2020. 04. 11.)

[6] Martens, Ulrich: Wirtschatfliche Krise, Arbeitslosigkeit und Kriminalitätsbewegung. [Economic crisis, unemployment and crime movement]- Freiburg i. Br., 1978. pp. 5-6.

[7] Lacassagne A.: Marche de la criminalité en France 1825-80. [Crime march in France 1825-80.] In: Revue Scientifique, 1881.

[8] Akerlof, George, A. – Shiller, Robert, J., Animal Spirits. Corvina Kiadó, Budapest, 2011. p. 91.

According to German research led by Exner after the First World War,[9] he came to the following correlation: the number of thefts with will increase with ten thousand cases with every one million new unemployed people.

Between 1882 and 1914, rye and bread prices moved almost entirely together with the number of known thefts in Germany, according to research by Eduard Joachim[10].

At the beginning of the 20th century, between the two world wars, Dorothy Swaine Thomas examined the correlation between economic cycles and various categories of crime between 1865 and 1915[11]. Demonstrable links have been found[12] between the cyclical changes of the economy and the following groups of criminal offences:

- every known criminal offence,
- non-violent offences against property,
- violent offences against property,
- intentional vandalism,
- violent offences against the person.

She proved that economic cycles move almost in the opposite direction to each crime category: crime decreases in the case of recovery and increases in a recession.

During the Great Depression of 1929-33, according to research,[13] while crime overall in Germany decreased, the increase after 1929 is clearly visible for certain crime groups.

After the Great Depression, the relationship between economic crises and crime has also been examined in the United States. Thorsten Sellin draws attention to the following exciting contexts in her book on the subject:[14]

1. Not all types of crime respond sensitively to changes in economic indicators; therefore, investigations should be carried out separately for certain types of crime.
2. Economic changes do not affect all areas to the same extent.
3. Not all classes of society are equally adversely affected by the economic crisis. The impact of the crisis is more visible in the crime of groups more affected by the disaster.
4. Finally, it is essential to underline that less potent economic downturns have less effect on crime rates than greater ones.

It is interesting to note that Thomas Robert Malthus had come to the same conclusion centuries earlier as the American author in the first half of the 20th century that not all classes of society are equally adversely affected by economic crises. "Unfortunately, although working classes benefit from the general boom, but not as much as in the general downturn. They suffer the greatest need in times of low wages, but cannot receive adequate compensation in times of high salaries neither. For them, (economic) surges always do more harm than good, and keeping the well-being of the majority of the society in mind, our goal has to be to maintain peace and equal spending. "[15]

---

[9] Exner, F., Krieg und Kriminalität Kriminalistische Abhandlungen. [War and Crime Criminalist Treatises]. Heft 1. Leipzig, 1926.

[10] Joachim, Eduard, Konjunktur und Kriminalität. [Business cycle and crime] Offenburg, 1933. p. 19.

[11] Thomas, Dorothy, Swaine, Social Aspects of the Business Cycle. New York, 1927.

[12] Dorothy Swaine Thomas: Social Aspects of the Business Cycle. New York, 1927. 134. p.

[13] Gleitze, Bruno, Die Konjunkturkriminalität in der Zeit der Weltwirtschaftskrise. [The economic crime in the time of the Great Depression] W. Kohlhammer Verlag, Stuttgart und Berlin, 1941. p. 7.

[14] Sellin Thorsten, Research Memorandum on Crime in the Depression. New York, 1937. p. 19-20.

[15] Cited by Szentes, Tamás, Ki, és miért van válságban? (Who is in crisis and why?). Napvilág Kiadó, Budapest, 2009. p. 108.

After World War II, crime rates and the number and duration of prison sentences increased along with economic indicators. There seemed to be no connection between financial crises and crime.

In 1978 Ulrich Martens analysed the previous research with a critical approach. According to him, "no general statement can be made in time or space that whether and if so, what impact does the economic situation, and in particular, unemployment, have on the development of crime?."[16] In the literature, hesitation can be seen in the 1970s, when researchers began to question the effect of economic crises on crime. "In the early 1970s, as the value system controlling the whole society in financial crises changed, the relationship between economic conditions and crime was again on the list. The most comprehensive research – including international comparisons – was conducted within the framework of the Council of Europe, and its results were published in 1985."[17] Research of the 1970s and 1980s did not prove any correlation between economic crises, recessions, recessions and crime in time, as Katalin Gönczöl points out in a study:

"Contrary to the usual methods of the investigation so far, they have not been based on indicators of the social status of offenders, but have sought to show the impact of changes in the above factors, which are most characteristic of the economies of the countries concerned. The analysis covers the period from 1963 to 1981. During this period, the number of perpetrators per 100,000 people at fault in the Federal Republic of Germany increased from 2,920 to 6,600, in France from 1,350 to 5,370, and in England and Wales from 2,250 to 5,660. In addition to the steady rise in crime, economic development was not even in any country. While national incomes increased to varying degrees between 1950 and 1960, they increased in all three countries, and then declined to a stagnating level in the second half of the 1970s. Unemployment reached 10% and then fell sharply as a result of favourable developments. In the early 1960s, for example, the Federal Republic of Germany did not reach the 1% level. From 1975, however, it rises again, and in 1980 it approached its former highs.

Researchers have found that the cyclical development of the economy has no direct correlation with the evolution of crime. The delayed response to the improvement or deterioration of economic conditions in crime changes is not apparent. Thus, the research did not confirm the hypothesis that the effect of economic terms does not appear in the actual crime, but the statistical series of a later period. Crime has steadily increased in all three countries. This increase, in turn, resulted in countries starting from very different situations in terms of per 100,000 offenders by the end of the investigation period, 1981. Specifically, crime has risen by 400% in France, 230% in the Federal Republic of Germany and 250% in England and Wales in 18 years to reach roughly the same level by 1981. From Katalin Gönczöl: Contrary to the findings of the cited works, international scientific literature based on research completed in the second half of the 1970s once again confirms that crimes against property and economic crime are on the increase during the financial crisis.

---

[16] Martens, Ulrich, Wirtschatfliche Krise, Arbeitslosigkeit und Kriminalitätsbewegung. [Economic crisis, unemployment and crime movement] Freiburg, 1978. p. 36.

[17] Gönczöl, Katalin, Válság – munkanélküliség – büntetőpolitika. [Crisis – unemployment – criminal policy.] p. 3.

http://www.fszek.hu/szociologia/szszda/gonczol_valsag_munkanelk.pdf.

In 1976, UNSDRI (United Nations Social Defense Research Institute), based in Rome, showed that during special economic downturns and disasters, some specific forms of economic crime are increasing. In such cases, effective countermeasures must be taken, which, of course, are not limited to criminal law enforcement.

In 1983, a German study showed the inverse relationship, that is, during the economic boom, the prison population and the number of people in psychiatric treatment decreased.

The author of a monograph published in 1987 found the following correlations between the occurrence of unemployment and certain serious crimes:

- burglary 0.572,
- violent crimes against persons,
- vandalism 0.494,
- theft 0.423
- robbery 0.342
- fraud 0.338
- sexual offences 0.158.

From this, it can be seen that, apart from sex crimes, there is a significant relationship between crises and several types of serious crime. Indeed, high unemployment has a robust correlation with economic recessions, a typical and systemic consequence of the crisis.

Another American study[18] aimed to develop a model that explains the evolution of the crime rate against the property by using economic variables. Dependent variables used to measure the speed of property crime were obtained from the FBI's Uniform Crime Reporting Program. Independent variables include public education, the unemployment rate, the GDP rate, the poverty rate, the average income and the amount of heroin and cocaine seized.

A correlation model was used for dependent and independent variables. With the use of a linear regression model, all independent variables were analysed. The results were as follows:

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, except the negative correlation between the unemployment rate and the rate of crime against property.

After the onset of the economic crisis in 2008, the fear of crimes against property and violent criminality has grown significantly in society. This was also supported by crime statistics, as a significant increase could be seen in thefts, burglaries and robberies. Between 2009 and 2011 the number of known thefts and burglaries grew by 33%-, from 72,658 to 96,925. Meanwhile, robberies increased by 41%, from 4,708 to 6,636[19].

According to a report of the United Nations Office on Drug and Crime 2010, 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

---

[18] Reza Fadei-Ttahraniés Thomas M.Green: Crime and Society (=International Journal of Social Economics Vol. 29. No 10. 2002. p. 785-788.

[19] The politics of crime and the financial crisis in Greece Sappho Xenakis and Leonidas K.Cheliotis, 2 August 2012 http://www.opendemocracy.net/sappho-xenakis-leonidas-kcheliotis/politics- of-crime-and-financial-crisis-in-greece (August 20, 2012).

by statistical models (especially ARIMA models). Volume. This conclusion was reached based on 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 of 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 show a 4-6 month time shift.

5) On average, for three months, you can predict well the prospective future development of crime at the national level or for a city based on historical crime statistics and economic variables[20].

The increase in the number of intentional homicides is clearly visible in the timeline based on Mexican crime statistics data. In the year of the outbreak of the economic crisis, the steadily declining trend visibly broke and turned into growth. So the crisis has also increased the number of intentional homicides. A co-movement of robbery and unemployment has been observed in Canada, with the timeline moving almost entirely together[21].

We agree with the concept that not only economic crises, but economic recovery can often act as a factor in increasing the crime rate.

"A sudden unfavorable change of the economy – the increase in poverty, the increasing number of poor people – can be blamed for the cause of deviance, and rise of crimes, as well as the positive economic growth, if the process is rapid"[22].

III. The Main Tendencies of the Hungarian Criminality After the Regime Change

After the general overview, the Hungarian example is also very instructive, as it confirms the international experiences observed in the last two hundred years: The Hungarian regime as also preceded by a deep economic crisis. After that, there was a global financial crisis in 2008, the effects of which lasted for years. After both crises, the definite and robust increase in crime in Hungary could be seen. It must be noted that criminal statistics data of the period since the regime change only give a limited possibility to compare and to draw conclusions, because of the many amendments to the Criminal Code. For example, in 2007 the petty offence limit of the criminal offences against property grew from 10,000 to 20.000 HUF, and in 2011 to 50,000 HUF: all this

[20] www.unodc.org/documents/data-and-analysis/statistics/crime/GIVAS_Final_Report.pdf (2012. august 18).

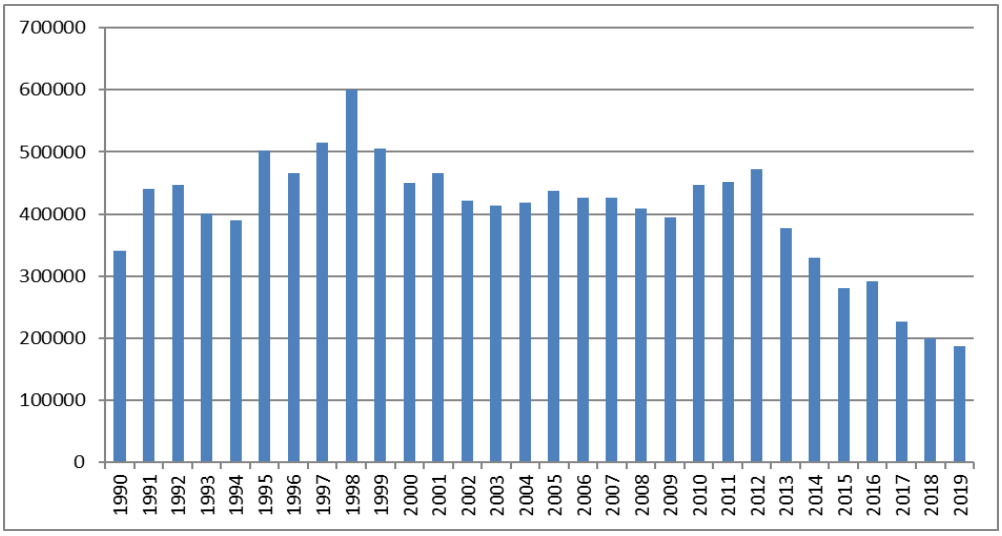
[21] www.unodc.org/documents/data-and-analysis/statistics/crime/GIVAS_Final_Report.pdf (August 18, 2012).

[22] Durkheim É, Az öngyilkosság. (The suicide). Közgazdasági és Jogi Könyvkiadó 1967. p. 250-251.

excludes tens of thousands of crimes previously classified as criminal offences from the scope of criminal law. These acts are still committed just the same but are now only registered as infringements by the statistics, so they are distorted in a favorable direction. (We note that, in addition to the beneficial "optical effect" on the statistical data, these acts can be prosecuted more quickly and perhaps more effectively as infringements, than in the context of the criminal proceedings, that is slower and involves more guarantees.)

Examining the last three decades, it is visible that there was an increasing trend from the regime change to 1998 as a result of the economic crisis that preceded the change of regime and lasted for a few years after that. After this, a decreasing trend could be seen until 2003. In the following years, crime stagnated slightly around the thirty-year average[23] of around 400,000 until 2009, and it can also be said that this was a period of normalization and 'criminal consolidation'. Then, the impact of the 2008 global economic crisis could be felt strongly on the increasing trend from 2009-2012, despite various governments "intervention" in growth in 2007 and 2011 by raising thresholds, which would have been even stronger without the intervention. These legislative changes, as already mentioned, have resulted in a formal reduction in the volume of crime, or would have resulted, because the strong growth rate has nevertheless prevailed.

After all this, we can see a declining trend again, with the number of crimes falling to a low of 186.724, a level is never seen since the change of regime. Among the reasons for this, we can also mention the changes in the legislation, the new Criminal Code and the new Criminal Procedure Code are so modern, and proving to be a useful tool in the fight against crime, with improving economic performance and presumably more valuable tools.



Source: KSH

[23] 404, 371 criminal offences per year, generally, between 1990-2019 in the analysed period.

Other factors have played a role in this process, in addition to stricter criminal policy and more efficient performance of tasks by state bodies involved in criminal proceedings – a significant factor of the drastic increase in the number of Hungarian workers abroad in the 2010s. "Based on the data provided by the Hungarian State Treasury, the number of foreign maternity benefit applications in 2018 was 9.907. According to this, every tenth Hungarian was born abroad." Among Hungarian workers, who are working abroad, young men are overrepresented, who may be the typical perpetrators of crimes from a criminological point of view, so this may also have been a factor in reducing the volume of crime.

In my opinion, the increasing or decreasing trend of crime is influenced by three circumstances:

1) the actual change of the phenomena (increase or decrease of the number of the committed crimes),

2) the role of the formal legal factor (in the case of unchanged crime, the given conduct may be considered a criminal offence due to changes in legislation, or the given conduct may no longer be considered a criminal offence),

3) the efficiency of criminal justice (primarily the work of the investigating authorities plays a crucial role here). That is, to put it, if we see that, according to official statistics, crime is declining over some time (5 or 10 years) in a given area (a city, a county, a country), it may be because fewer crimes are being committed. It may also be the reason as a result of the amendment of the Criminal Code, individual behaviours, which remain unchanged or even increase slightly, are no longer criminal offences but, for example, are offences. Finally, the reason may be that the investigating authority worked less efficiently during the period under review; the population did not trust the police, resulting in fewer reports and higher latency. We should also emphasize that "since latent crime differs from registered crime in both its structure and dynamics, the usefulness of general crime control methods becomes questionable." It is also essential to point out that an increase in the number of known crimes may not indicate a negative trend. If crime statistics show an increase in an offence where latency is estimated to be low (such as intentional homicide), this is a negative trend, as it means that more homicides have taken place. If, on the other hand, there is an increase in the number of crimes according to official statistics with very high latency (such as fraud or corruption crimes), then the increase may not mean an actual improvement. It can also mean that, with an unchanged or even declining number of offences, more is discovered because of the more efficient work of the investigating authority. In other words, to put it, twice as many homicides in official statistics are negative news. At the same time, twice as much bribery or fraud is most likely positive news for those who are expert in criminology.

IV. A Cautious and Moderate Estimate of Hungarian Crime After 2020

The question is not that; there will be a global economic crisis in 2020 or not, economists are only debating how big it will be, whether the pace of growth will slow down, or even the entire world economy could go into recession. Given the impact of the crises of the last two centuries on crime rates, the question is not whether crime will increase, either in Hungary or internationally, but only what its extent will be. We can set up optimistic, realistic and pessimistic scenarios. I will present below the script that I consider to be realistic.

Fortunately, the crisis did not hit the Hungarian economy in a bad situation: "The Hungarian economy – if good things can be found in this fate at all – was hit by the coronavirus in an outstanding state. No matter how big is the catastrophe now, it is true that recent annual GDP growth has ranged from four to five per cent, unemployment has fallen to close to three per cent; employment has reached a historic high. At the same time, the budget deficit has been kept below the EU average, and finally, public debt has also begun to shrink." The initial condition is relatively good. Crime has also declined at an unprecedented rate since the regime change in recent years, at least the number of crimes that have become known has fallen sharply while reaching a record low in 2019, 186.724 crimes that have become known. This number is expected to increase after 2020 as a result of the combined effect of the following factors:

I. from such a low base, some growth could be forecast even without a crisis, all other things being equal,

II. Thousands of Hungarian young, single men who have returned home due to the closure of European countries, from whom typical offenders are excluded in a criminological sense, this is also expected to increase the number of known crimes.

III. the curfew is likely to significantly increase domestic violence and other crimes against persons (life and physical integrity),

IV. if people lose their jobs it will increase the number of crimes against property and violent property,

V. The impact of the economic crisis will be linked to these four factors.

Let's look at the latter, on its own, regardless of the previous four factors[24]. Based on my earlier research in 2012, the following are probable:

1) The crime rates will increase (on average) 4-6 months later after the economic crisis especially in the third quarter of the year of 2020,

2) starting from the crisis of 2008, the number of crimes against persons will increase from the end of 2020, but also in the next 1-2 years,

3) there will be a definite reduction in the name of offences against traffic regulations in 2020 due to travel and travel restrictions as well as quarantine measures and the reduction of tourism to zero,

4) crimes against public order will first show a decreasing (due to quarantine measures) and then an increasing trend (after the lifting of access restrictions),

5) an increase in the number of economic crimes is expected, especially in crimes committed with the help of information technology,

6) crime against the property will first decrease, and then it will also turn into a definite increase, especially from 2021,

7) The number of intentional homicides is also expected to increase as early as 2020.

At the moment, in April 2020, we do not know the extent of changes in the future. The increase (and the decrease in offences against traffic regulations) is already predictable; the question is only to what extent. According to the optimistic scenario, the percentage increase may be small, according to the realist it may be at least double-digit, according to the pessimistic it may reach or exceed 50% for the total crime, and each of the highlighted crime groups examined.

---

[24] Obviously, complete independence is not true, as these explanatory variables may also have some degree of stochastic relationship with each other.

V. Criminal Law as *One of the* Possible Tools of Therapy

As my former professor, József Földvári, often told students in his lectures: "Criminal law is not capable of solving social problems. I go even further: criminal law *alone* cannot solve even criminal law problems."

All we can add to this undoubtedly true finding is that criminal law is a necessary but not sufficient tool for combating crime. If we know the past tendencies, we can prepare for the challenges of the future. We can respond before, during, or after problems arise. The earlier we move, the higher the efficiency can be.

If crime policymakers forecast an increase in crime, first of all, it is possible to consider increasing the number of the investigating authority and raising salaries in connection with the existing staff.

At first glance, the second proposal may seem strange, but an immediate amnesty (pardon law) could also be helpful, in several ways. On the one hand, it would reduce congestion in prisons, which would reduce the likelihood of infection, thereby reducing the risk of the prison staff and the convicted persons to be infected.

The other factor may be that there will also be a need for 'free capacities' from 2021, because, in my view, rising crime rates will only be restrained by a consistently strict criminal policy. There would be a need to build more penitentiary institutions and to accelerate ongoing construction, and to increase the number of workers in prison enforcement and the average monthly income per capita from 2021.

My fourth proposal is to make the statutory provisions of the crimes that are increasing in the Criminal Code more strict. Since Cesare Beccaria's classic work[25] was published in 1764, it has been an axiom in criminal law that two factors deter potential offenders from committing a crime: the severity of the expected punishment and its inevitability (i.e., the mathematical probability of punishment).

In my view, it is vital to make the Criminal Code more strict alongside about strengthening the investigating authorities even though the current Hungarian Criminal Code is already one of the most rigid codes in Europe.

As a formal factor, we could consider raising the value limit for property crimes to 100,000 Forints, instead of the current 50,000 Forints.

This would have a positive effect on future statistics; furthermore, it would partly relieve the investigating authorities in criminal matters. On the other hand, this would, at the same time, increase the workload of the police investigating regulatory offences. (Add immediately: it is faster and easier to deal with theft of HUF 75,000-80,000 as a regulatory offence than in criminal proceedings, it is also more efficient and faster to impose a sanction.) At the same time, the maximum fine that can be imposed in infringement proceedings should be doubled or tripled. The summary of my recommendations are the following:

1. in the case of investigating authorities, we should increase the staff members and the salaries,
2. amnesty for some non-violent offenders to reduce congestion and free up capacity,
3. accelerating the prison construction program, increasing the number of workers in the penal execution from 2021 and raising salaries here as well,

[25] Cesare Beccaria: Dei delitti e delle pene, (On Crime and Punishments) 1764.

4. The make the Criminal Code more strict with regard to criminal offences against individuals, property, public order and economic activities,

5. raising the threshold for crimes against property to 100,000 Forints, in parallel with a firm tightening of the Regulatory Offenses Act and a significant increase in the number of fines.

In addition to all these proposals, as Franz Liszt put it: "The best criminal policy is good social policy." That is, a lot will depend on how the government handles the social policy effects and consequences of the crisis. Together, they will help reduce the negative effects of the crisis on crime and, in the long run, flatten not only the epidemic curve but also the growth waves on time series showing an increase in total offence and individual crimes in the coming years.

References

1. Akerlof, George, A. – Shiller, Robert, J., Animal Spirits. Corvina Kiadó, Budapest, 2011.

2. Ambrus István: A koronavírus-járvány és a büntetőjog MTA Law Working Papers 2020/5. Budapest, 2020. 22. p. file:///C:/Users/USERUJ/Downloads/2020_5_Ambrus.pdf (2020. 04. 11.)

3. Beccaria, Cesare: Dei delitti e delle pene, (On Crime and Punishments) 1764.

4. Durkheim É, Az öngyilkosság. (The suicide). Közgazdasági és Jogi Könyvkiadó 1967.

5. Exner, F., Krieg und Kriminalität Kriminalistische Abhandlungen. [War and Crime Criminalist Treatises]. Heft 1. Leipzig, 1926.

6. Gleitze, Bruno, Die Konjunkturkriminalität in der Zeit der Weltwirtschaftskrise. [The economic crime in the time of the Great Depression] W. Kohlhammer Verlag, Stuttgart und Berlin, 1941.

7. Gönczöl, Katalin, Válság – munkanélküliség – büntetőpolitika. [Crisis – unemployment – criminal policy.]

8. Halm Tamás: A gazdasági válság. Okok és tanulságok. [The economic crises. Causes and lesson In: Kommentár 2009/6.

9. Joachim, Eduard, Konjunktur und Kriminalität. [Business cycle and crime] Offenburg, 1933. p. 19.

10. Lacassagne A.: Marche de la criminalité en France 1825-80. [Crime march in France 1825-80.] In: Revue Scientifique, 1881.

11. Martens, Ulrich: Wirtschatfliche Krise, Arbeitslosigkeit und Kriminalitätsbewegung. [Economic crisis, unemployment and crime movement]- Freiburg i. Br., 1978.

12. Reza Fadei-Ttahraniés Thomas M.Green: Crime and Society (=International Journal of Social Economics Vol. 29. No 10. 2002.

13. Sellin Thorsten, Research Memorandum on Crime in the Depression. New York, 1937.

14. Szentes, Tamás, Ki, és miért van válságban? (Who is in crisis and why?). Napvilág Kiadó, Budapest, 2009.

15. Thomas, Dorothy, Swaine, Social Aspects of the Business Cycle. New York, 1927.

Is Terrorism an International Crime?

***Dr. Ioana Celina Paşca*[1]**

Abstract

Lately, we are witnessing an attempt to define terrorism and sanction it proactively. Unfortunately, the interest of international bodies is limited to the condemnation of the acts of terrorism and, at most, to the provision of obligations upon the states to cooperate with each other in order to investigate such crimes, avoiding any mention of an individual criminal liability in international law.

The lack of a general definition of terrorist offences could have consequences for the international cooperation in criminal matters in this area. Terrorist offences are international crimes and their perpetration could lead to criminal liability for crimes against humanity before an international jurisdiction, be it the International Criminal Court or an International Court against Terrorism.

Keywords: *Terrorism, International Criminal Court, International Court against Terrorism, legal person*

1. Terrorism – Concept, Perspectives and Consequences

As stated in all UN documents, terrorism, "in all its forms and manifestations, is one of the most serious threats to the peace and security of states,"[2] but, nevertheless, one has failed to coagulate the agreement of states in drafting a global convention to define and punish this crime.

This message was reiterated in the UN General Assembly Resolution of December 9th 1994, according to which "acts, methods and practices of terrorism constitute a serious violation of the purposes and principles of the United Nations, which may pose a threat to international peace and security, jeopardize friendly relations among States, hinder international cooperation and aim at the destruction of human rights, fundamental freedoms and the democratic bases of society"[3].

The European Convention on the Suppression of Terrorism, adopted in Strasbourg, in 1997[4], under the auspices of the Council of Europe, lists only the international conventions by which the signatory states undertake the obligation to incriminate in their national law the crimes within them, stating that they will not be considered political crimes, crimes related to a political crime or crimes inspired by political purposes.

---

[1] Senior Lecturer, West University of Timişoara, Faculty of Law. Contact: ioana.pasca@e-uvt.ro.

[2] Resolution No. 1566/2004, adopted by the UN Security Council [2004], Official Journal No. 49 /2010.

[3] Resolution No. 49/60/1994, Measures to eliminate international terrorism, para. I (20), adopted by the General Assembly [1994].

[4] Adopted in Strasbourg [1997], Official Journal No. 34/1997.

The International Convention on the Suppression of the Financing of Terrorism, adopted under the auspices of the UN, in 1999[5], indirectly defines terrorist offenses as those acts defined in one of the treaties listed in the annex thereto[6], as well as "any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act"[7].

The member states of the Council of Europe, through the Convention on the Prevention of Terrorism, signed in Warsaw, in 2005[8], define terrorism "as any of the offenses falling within the scope of one of the annexed treaties"[9].

In a recent European Parliament directive, acts of terrorism have been characterized as "one of the most serious violations of the universal values of human dignity, freedom, equality and solidarity, and enjoyment of human rights and fundamental freedoms on which the Union is founded"[10].

In Romanian criminal law, terrorism is defined as "those actions, inactions, as well as threats that represent a public danger, affect life, bodily integrity or human health, material factors, international relations of states, national or international security, are politically, religiously or ideologically motivated and are committed for the purpose of intimidating the population or a segment of the population, by producing a strong psychological impact or illegitimately forcing a public authority or international organization to fulfil, not to fulfil or to refrain from fulfilling a certain act or the serious destabilization or destruction of the fundamental, constitutional political structures"[11].

The acts of terrorism are transnational if they are committed on the territory of at least two states; are committed on the territory of a state, but part of their planning, training, management or control takes place on the territory of another state; are committed on the territory of a state, but involve a terrorist entity which carries out

---

[5] Official Journal No. 852/2002.

[6] Convention for the Suppression of Illicit Capture of Aircraft [The Hague, 1970]; Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation [Montreal, 1971].

Convention on the Prevention and Punishment of Crimes against International Protected Persons, Including Diplomatic Agents, adopted by the United Nations General Assembly [1973]; International Convention against the Taking of Hostages, adopted by the United Nations General Assembly [1979]; International Convention on the Physical Protection of Nuclear Material [Vienna,1980]; Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Complementary to the Convention for the Suppression of Unlawful Acts against Civil Aviation Security [Montreal, 1988]; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation [Rome, 1988]; Protocol for the Suppression of Unlawful Acts against the Security of Fixed Platforms Located on the Continental Shelf [Rome, 1988]; International Convention for the Suppression of Terrorist Bombings, adopted by the United Nations General Assembly [1997].

7 Article 2 point 1 letter (b), International Convention on the Suppression of the Financing of Terrorism.

[8] Official Journal No. 949/2006.

[9] To the annexed treaties indicated in note 4, this Convention adds two other treaties: the International Convention on the Suppression of the Financing of Terrorism [New York, 1999], and the International Convention on the Suppression of Acts of Nuclear Terrorism [New York, 2005].

[10] Directive (EU) 2017/541 of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, para. (2).

[11] Art. 1 of Law no. 535/2004 on preventing and combating terrorism, Official Journal No. 1161/2004.

activities on the territory of another state, are committed on the territory of a state, but have substantial effects on the territory of another state[12].

Terrorist offences can be sanctioned based on the principle of the universality of criminal law, called the principle of universal repression or of the universality of the right to punish, if a crime has been committed outside the country, the offender is a foreigner or stateless person residing abroad, the act constitutes a criminal offense for which the Romanian state has assumed the obligation to repress it under an international treaty, regardless of whether or not it is provided by the criminal law of the state on whose territory it was committed and the perpetrator to be voluntarily on the territory of Romania[13].

The notion of "international crime", in a broad interpretation (*lato sensu*), includes all crimes which have an element of extraneousness, either regarding the place of their perpetration, or the person of the perpetrator, regardless of the rule that regulates them[14].

In a narrow sense (*stricto sensu*), international crimes (offenses) are only those acts that are within the jurisdiction of international criminal tribunals, as a result of their regulation by the Statute of Tribunals.

The difference between treaty-based crimes and 'true' or core international/ supranational crimes is that "*the treaty-based crimes can only be enforced by states at the domestic level, while true international crimes create a proper, international, individual criminal responsibility*"[15]. Thus, by recognizing this form of responsibility, the individual was removed from the tutelage of the state, becoming the recipient of international legal rules.

Vespasian V. Pella defined the international crime as "an action or inaction sanctioned by a punishment pronounced and executed on behalf of the community of states"[16].

International crimes are acts that undermine the common values of all states, recognized as such internationally, "acts on which the general conviction has been formed that they must be criminally punished"[17].

Article 1 of the Statute of the International Criminal Court, referring to the jurisdiction of the Court, without using the term "international crimes", considers these acts as "the most serious crimes" and which have an "international resonance".

By limiting the jurisdiction of the International Criminal Court to crimes of genocide, crimes against humanity, war crimes and aggression, the traditional system of repression of the international humanitarian law is strengthened; according to this system, the responsibility for the application of punishment rests with the states, its jurisdiction having a subsidiary role to the national one[18].

---

[12] *Ibid*, Art. 3.

[13] Article 11 of the Romanian Criminal Code.

[14] Caracciolo, I., *Dal diritto penale internazionale al diritto internazionale penale*, Editoriale Scientifica, Napoli, 2000, p. 129 ff.

[15] Ambos, K.; Timmermann, A., *Terrorism and Customary International Law*, in: Ben Saul (ed.), Research handbook on international law and terrorism, Elgar, 2014, pp. 23-24.

[16] Pella, V.V., *Criminalitatea colectivă a statelor și dreptul penal al viitorului*, (translated by A. Ciucă, A. Gentimir, R. Boca), Ed. Hamangiu, Bucharest, 2017, p. 263.

[17] Mantovani, F., *Diritto penale*, Cedam, Milano, 2001, p. 986.

[18] Much, C., *The International Criminal Court (ICC) and terrorism as an international crime*, Michigan State Journal of International Law, Vol. 14, No. 1, 2006, p. 133.

Proposals to include the crime of terrorism within the jurisdiction of the Court have been formulated by several states ever since the drafting of the project of Statute of the International Criminal Court, the discussion being resumed at the 2010 Kampala Conference on the revision of the Statute of Rome of the International Criminal Court, but without any success.

The International Criminal Court may exercise its jurisdiction over natural persons for the most serious crimes. Consequently, the jurisdiction of the International Criminal Court was not envisaged as having a limited nature, but with the possibility of being extended to other crimes as well.

For example, terrorist offenses under international conventions for the protection of persons on board ships, aircraft, airports etc. are indisputably international crimes and we consider that they could be considered crimes against humanity in accordance with Article 1 of the Statute, because they represent a systematic attack launched against a civilian population and aware of this attack.

In the practice of the International Criminal Tribunal for Rwanda[19], it was noted that, in order to be considered systematic, the attack must have been planned. Terrorist attacks are indisputably planned acts, often supposing the involvement of sophisticated logistics, ranging from financing actions and procuring the means to carry out actions, to actually planning them. The same court mentions the fact that the author must not have participated in drawing up the plan, but it is enough for him/her to be aware of the general context, respectively of his/her involvement in such context[20].

In the Karemera case[21], the International Criminal Tribunal for Rwanda states that the perpetrator of an attack against the civilian population must be aware of the fact that his/her acts are an integral part of the attack, yet, without the necessity of any form of adherence from their part to the purpose or objectives of the generalized or systematic attack.

The non-inclusion of the crime of terrorism in the jurisdiction of the International Criminal Court was motivated by the lack of a generally accepted definition of this crime. The opponents of the idea of including terrorism within the jurisdiction of the International Criminal Court have said that caution is needed in analyzing the terrorist phenomenon, as terrorism is often an "invective used by states to demonize political opponents, certain groups or states"[22]. The inclusion of terrorism within the jurisdiction of the Court would politicize the institution, which is not desirable.

The international relevance of the crime of terrorism lies in the manner in which it is committed and in its effects. The purpose of each terrorist act, committed both in times of peace and in times of war, is to spread terror among the civilian population, regardless of the motive of the act: political, ideological, philosophical, religious etc. The psychological impact of this crime on the population is long-lasting and causes a long-lasting state of insecurity and constant threat.

By through the non-inclusion of terrorism in the category of serious crimes within the competence of the International Criminal Court, not only the social values

---

[19] ICTR, *Trial Chamber I,* Prosecutor vs. Aloys Simba, Case no. ICTR-2001-76-T, December 13th 2005, para. (421).

[20] *Ibid.*

[21] ICTR, *Trial Chamber III*, Prosecutor vs. Edouard Karemera, Matthieu Ngirumpatse, Case no. ICTR-98-44-T, February 2nd 2012, para. (1675).

[22] Much, C., *op. cit*, note 17, p. 133.

protected by the incrimination of this crime are disregarded, but also the effect that these crimes have on the civilian population. The lack of reaction of the international community might be interpreted by terrorist groups as an inability to repress the phenomenon. The mere national criminal reaction to an international phenomenon could consolidate and create a favorable environment for the development of terrorist organizations, which, knowing the political and repressive mechanism of the state, also know its shortcomings.

On the other hand, in the absence of an international benchmark, the definition and interpretation of the concept of "terrorism" by each state individually would give rise to major discrepancies at the national level, since any form of violence could be classified as terrorist and any form of repression as appropriate[23].

We cannot deny, however, the fact that this crime involves the international community, but, above all, it implies a different approach from the latter towards this crime, with the consequence of affecting democratic principles.

In terms of the fundamental principles of criminal law, there is an extension of the scope of actions which bear individual criminal liability, by sanctioning the preparatory acts or mere participation in such an organization, with or without the intention to participate in the perpetration of the crime-purpose of the terrorist organization.

2. International Court Against Terrorism

Romania, alongside Spain and the Netherlands, have proposed the establishment of an International Court against Terrorism[24]. The proposal was made in the context of the rejection of the proposal to include terrorism within the jurisdiction of the International Criminal Court.

In Romania's opinion, terrorism must be combated by coherent and adequate international repressive means, through a coordinated cooperation of the states, as in the case of the crimes falling within the competence of the International Criminal Court and which infringe the same social values. The approach is legal, as long as the crime of terrorism undermines international peace and security.

The establishment of the International Court against Terrorism could be subsumed under the will of the members of the UN General Assembly, which should adopt an international treaty to that effect. For the sake of efficiency, the idea that the International Court against Terrorism could be established by means of a Security Council Resolution, under Chapter VII of the UN Charter, was also circulated in the same proposal. The establishment procedure would not be a new one, as long as all *ad hoc* criminal tribunals have been established by means of Security Council Resolutions.

Moreover, the establishment of *ad hoc* criminal tribunals by means of UN Security Council Resolutions represents the explicit evidence of the political will of the United Nations to identify and hold accountable those individuals guilty of international crimes.

---

[23] Mariani, L., *Le molteplici possibili definizioni di terrorismo e terrorismo internazionale* (2nd part), Cammino Diritto, No. 1, 2019, p. 17.

[24] www.mae.ro, [Accessed 29 March 2020].

The institution, and, respectively, its Statute, could be configured on the basis of an agreement among several states, thus avoiding the criticisms regarding the legitimacy and impartiality of the institution, formulated against the *ad hoc* criminal tribunals previously established.

The Special Tribunal for Lebanon was the first international jurisdiction established by means of a UN Security Council Resolution[25], competent to decide upon the crime of terrorism.

The establishment of the Special Tribunal for Lebanon has brought the crime of terrorism back into the attention of the international community, "crystallizing, in customary law, the crime of terrorism as an international crime"[26].

2.1. Jurisdiction of the International Court Against Terrorism

One of the fundamental reasons for proposing the establishment of a new body to prosecute the crime of terrorism, distinct from the International Criminal Court, is linked to the relatively small number of states that have ratified the Statute of the International Criminal Court.

According to the provisions of Article 12 of the Statute of the International Criminal Court, the Court may exercise its jurisdiction if one or more of the states involved in the conflict are parties to this Statute or have accepted the jurisdiction of the Court. Given these conditions, the jurisdiction of the Court is relatively restricted and conditioned by the quality of state party to the Statute or by the recognition of the competence of this institution for a certain act.

Beyond the small number of states whose citizens can be prosecuted by the Court, in the case of the crime of aggression, the jurisdiction of the Court suffers a double restriction. The Court may exercise jurisdiction over a crime of aggression, arising from an act of aggression committed by a state party, unless that state party has previously declared that it does not accept such jurisdiction by lodging an express declaration[27]. In respect of a state that is not a party to the Statute, the Court shall not exercise its jurisdiction over the crime of aggression when committed by that state's nationals or on its territory[28].

The jurisdiction of the International Criminal Court in relation to the crime of aggression is, at the same time, subject to a determination from the Security Council. According to Article 15 *bis* para. (6), the prosecutor, before proceeding with an investigation, has the obligation to first ascertain whether the Security Council has made a determination of an act of aggression committed by the state concerned. In such case, the intervention of the Court is subsumed by the UN Security Council, the proceeding of the investigation being based on the latter's decision.

The establishment of a body separate from the International Criminal Court could attract states which have not ratified the Statute of the International Criminal Court, UN members such as the US or Arab states. Many of the states involved in or targeted

---

[25] The Special Tribunal for Lebanon was established by the UN Security Council Resolution no. 1757 of May 30th 2007, in order to put on trial the persons responsible for committing the attack of February 14th 2005 in the Lebanese capital, Beirut.

[26] Cataleta, M. S., *Le Tribunal spécial pour le Liban et le respect des droits de l'homme,* L'Harmattan, Torino, 2012, p. 30.

[27] Article 15 *bis* point (4), ICC Statute.

[28] Article 16 *bis* point (4), ICC Statute.

by terrorist acts have not ratified the Statute of the Court, so, even if the International Criminal Court could prosecute the crime of terrorism, the acts committed on their territory could not be prosecuted by this institution.

Another reason for the establishment of the International Court against Terrorism would be the possibility to prosecute all acts of terrorism. The international community has not reached a consensus regarding the definition of the crime of terrorism. This is also the main reason for which this crime could not be tried by the International Criminal Court. The non-inclusion of terrorism in the Statute of the Court was motivated, mainly, by the lack of a generally assumed definition of this crime, but also by the impossibility of defining it, given the multifaceted nature of this phenomenon.

On the other hand, it is almost impossible to define a sprawling and speculative phenomenon such as terrorism. The phrases used in defining terrorism, such as "any criminal act" (criminal/unlawful under which law?), "spreading fear", and "political purpose", are so complex and so difficult to circumscribe to a particular sphere of incidence that any attempt in defining terrorism would defeat the principle of *lex certa*[29].

Most of the time, terrorist acts are used to overthrow the system of values of a state. However, in domestic political struggles, governments often label any act of violence committed by opponents as "terrorism", while the latter, in turn, declare themselves to be victims of the terrorist methods used by the government in power[30].

Professor Cassese, referring to the material element, classified the crimes of terrorism into three categories: *Sub-category of Crimes against Humanity, Sub-category of War Crimes and Discrete International Crime in Time of Peace*[31]. The latter category includes less serious acts, which have some connection with terrorism, but which cannot be classified as international crimes.

The definition of terrorism in time of peace is consolidated in customary law[32]. The differences concern the definition of acts of terrorism committed in time of war. In fact, the acts of terrorism committed in time of peace can be included in the category of crimes against humanity. Those which cannot be included in this category are singular, politicized, racist or religious acts, which cannot be classified as serious crimes. This was, in fact, the response of several states to the request to include terrorism within the jurisdiction of the Court.

In another opinion[33], terrorism has been categorized as state terrorism or non-state terrorism.

State terrorism involves the use of force by one state against another state, while non-state terrorism involves a manifestation of violence by a non-state body. The distinction is no longer relevant, given the fact that the International Criminal Court prosecutes the crime of aggression.

---

[29] Ambos, K.; Timmermann, A., *op. cit.*, note 14, p. 35.

[30] Orza, D. S., *Terorismul și drepturile omului,* in: Studii și cercetări juridice europene, Universul Juridic, Bucharest, 2018, p. 616.

[31] Cassese, A., *The Multifaceted Criminal Notion of Terrorism in International Law*, Journal of International Criminal Justice, No. 4, 2006, p. 938 ff.

[32] *Ibid*, p. 933.

[33] Todeschini, V., *Ripensare il terrorismo nel diritto internazionale Una ricerca sul concetto giuridico di terrorismo internazionale di Stato*, Jura Gentium, No. 1, 2013, p. 18 ff.

The jurisdiction of the International Court against Terrorism should be complementary to national criminal jurisdictions. The International Court against Terrorism should intervene, in the same way as the International Criminal Court, only when a state has no will or founds itself in a real inability to complete the investigation or the prosecution or has decided not to prosecute the person concerned.

The International Court of against Terrorism would be a complementary institution, but its jurisdiction would be rather subsidiary, as long as it could intervene only when a state has no will or founds itself in a real inability to prosecute a person suspected of having committed international crimes.

In the event of a conflict of jurisdiction between the International Criminal Court and the International Court against Terrorism, the jurisdiction of the International Court against Terrorism would be subsidiary.

2.2. Liability of the Legal Person for the Crime of Terrorism

Despite the fact that history has emphasized the role of legal persons in committing international crimes, the liability of the legal person has been recognized as a general principle only at the doctrinal level[34]. The liability of legal persons was included in the draft Statute of the International Criminal Court, but the regulation did not receive the final vote of the state parties[35].

The will of the states to combat the international criminal phenomenon and the recognition of the right of interference of international bodies within the issue of states remains debatable, as long as the sanctioning of the perpetrators of international crimes is limited to individuals only, and not legal entities or even states. The regulation of the criminal liability of the legal person and of the state in international law is imperative in the case of the crime of terrorism.

Most of the terrorist acts perpetrated so far have been committed by legal entities that have acted upon the initiative or with the consent of the state. Terrorist acts are largely financed by companies, non-governmental organizations or other forms of association with legal personality.

The phrase "terrorist organization", used in all the definitions of the crime of terrorism, whether national or international, refers to the notion of "organization" and the action of organizing serious crimes, among those listed in the same definitions.

As a result, many legislative interventions have been legitimized by reference to the notion of "group crime", following the legal regime specific to the fight against terrorism.

Terrorism is "a strategy by which several people united within an organization use different forms of violence in accomplishing certain claims"[36].

Due to their complexity, terrorist acts, in today's society, can no longer be committed by a small group and require a level of training and coordination at the

---

[34] Konaté, D., *La Cour pénale internationale, Entre nécessité de justice et impératif de paix*, L'Harmattan, Paris, 2018, p. 150: "At present, the doctrine is the one that confers consciousness to the legal persons by supporting the reality of their existence".

[35] United Nations General Assembly, Preparatory Committee for the Establishment of an International Criminal Court, Draft Statute, A/AC.249/1998/L.13, February 4th 1998, Article 17, § 5: "The Court shall also have jurisdiction over legal persons, with the exception of states, when the crimes committed were committed on behalf of such legal persons or by their agencies or representatives".

[36] Mocanu, R. I., *Fenomenul terorist. Analiza legislației anti-teroriste române*, Universul Juridic, Bucharest, 2013, p. 27.

level of an organisation. In itself, the terrorist act has a complexity that can no longer be managed by individuals.

Consequently, the need to identify and hold accountable organizations for terrorist acts planned and committed by means of their members appears to be necessary.

The activities of terrorist groups are as dynamic as possible and oriented depending on the social context, so that, in recent years, terrorist groups have reoriented and invested in the main sectors of activity, such as the economy, real estate, pharmaceuticals, media or non-governmental organizations.

In the lack of a regulation on the liability of the legal person or the state, any international institution, either the International Criminal Court or the International Court again Terrorism would be ineffective, as they could convict only a part of the perpetrators of the crime of terrorism, namely individuals only.

Given these antecedents, in order to defend the values of human dignity, the maintenance of international peace and security, it is necessary to sanction those who commit international crimes, regardless of whether they are natural or legal persons.

The exclusive jurisdiction of national courts in the case of legal persons would be likely to jeopardize the prosecution for international crimes. This would allow a state or some organizations to act by means of entities, be they companies, NGOs or paramilitary groups.

According to Romania's proposal, the International Court against Terrorism should have a jurisdiction complementary to national criminal courts.

The International Court against Terrorism should intervene, in the same way as the International Criminal Court, only when a state has no will or founds itself in a real inability to complete the investigation or the prosecution or has decided not to prosecute the person concerned.

In this situation, if the International Court against Terrorism could ask the states to relinquish the persons under their jurisdiction and prosecute the crime of terrorism committed by them, why could it not prosecute, for the same acts, also the legal persons involved, as long as most signatory states regulate the liability of the legal person? Otherwise, as regards legal persons, the jurisdiction of national courts does not have priority, but is singular, and the principle of complementarity, provided for in the Statute, would be ineffective.

The establishment of the liability of the legal person is also necessary in order to provide a coherent response to all international crimes, especially in the case of terrorism, being difficult to imagine how for the same act a natural person would be prosecuted by the International Court against Terrorism, and a legal person by the national courts. The prosecution by different courts of the same act would give rise not only to sanctioning inconsistencies, but also to discrepancies regarding the establishment of the guilty acts, which should be avoided.

In the case of the crime of terrorism, it is almost impossible to establish an individual liability without ruling on the responsibility of the state or an organization. Terrorist acts are nothing more than a projection of the will of an organization, a projection which is realised by the individuals who participate directly in the actions against the civilian population.

The liability of the legal person thus follows a consequentialist model, which justifies retributivism where there is a potential harm to society as a whole.

3. Conclusions

Terrorism is, beyond any doubt, an international crime. The lack of reaction of international bodies and the lack of cohesion of the states are prone to encourage this transnational phenomenon. The establishment of the International Court against Terrorism would send an important political signal to combat this phenomenon, not only through technical and military means, but also through firm and coherent legal repressive means.

Many conventions define terrorist acts as actions that can "result in the most serious consequences and threaten international peace and security"[37] and that "have the purpose by their nature or context to seriously intimidate a population or unduly compel a government or an international organisation to perform or abstain from performing any act or seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation"[38].

The lack of reaction from the international community would not only encourage the terrorist phenomenon, but could imply that terrorism is not (yet) recognized as an international crime in itself, which would be in clear contradiction to everything previously stipulated in all conventions, UN resolutions or treaties adopted regarding this crime.

The victim of an international crime is not a natural person, but the international community and, as a consequence, the holder of the action *jus puniendi* should not be the state, but a body acting on behalf of the international community. Therefore, the establishment of an international body to repress this crime is imperative. Divergences of opinion on the definition of terrorism could be overcome in the context in which the intention of the international community is to protect the fundamental values and interests of the community.

Some of the terrorist acts can be included in the category of crimes against humanity, but there are also facts which, due to their nature and manner of perpetration, cannot be classified as serious and, therefore, cannot be judged by the International Criminal Court. It is almost impossible to set a threshold and predict which of the terrorist acts are serious and which are less serious. However, it is also impossible for the International Criminal Court to prosecute all terrorist acts. As a result, the establishment of an International Court against Terrorism seems to be the only viable solution at this time for prosecuting the crime of terrorism.

Delaying the decision to set up an international body aimed to hold accountable those responsible for committing this crime does nothing but trivialize the fight against this phenomenon. In doing so, states respond individually, in their own fashion and, of course, transitorily, to exceptional situations which should normally be combated firmly and promptly through international efforts.

---

[37] Preamble to the International Convention on the Suppression of Acts of Nuclear Terrorism [New York, 2005], Official Journal No. 847/2006.

[38] Preamble to the Council of Europe Convention on the Prevention of Terrorism [Warsaw, 2005], Official Journal No. 9449/2006.

References

1. Ambos, K.; Timmermann, A., *Terrorism and Customary International Law*, in: Ben Saul (ed.), Research handbook on international law and terrorism, Elgar, 2014, pp. 20-38.

2. Caracciolo, I., *Dal diritto penale internazionale al diritto internazionale penale*, Editoriale Scientifica, Napoli, 2000.

3. Cassese, A., *The Multifaceted Criminal Notion of Terrorism in International Law*, Journal of International Criminal Justice, No. 4, 2006, pp. 933-958.

4. Cataleta, M.S., *Le Tribunal spécial pour le Liban et le respect des droits de l'homme,* L'Harmattan, Torino, 2012.

5. Konaté, D., *La Cour pénale internationale, Entre nécessité de justice et impératif de paix*, L'Harmattan, Paris, 2018.

6. Mantovani, F., *Diritto penale*, Cedam, Milano, 2001.

7. Mariani, L., *Le molteplici possibili definizioni di terrorismo e terrorismo internazionale* (2nd part), Cammino Diritto, No. 1, 2019, pp. 2-22.

8. Mocanu, R. I., *Fenomenul terorist. Analiza legislației anti-teroriste române*, Universul Juridic, Bucharest, 2013.

9. Much, C., *The International Criminal Court (ICC) and terrorism as an international crime*, Michigan State Journal of International Law, Vol. 14, No. 1, 2006, pp. 121-38.

10. Orza, D. S., *Terorismul și drepturile omului,* in: Studii şi cercetări juridice europene, Universul Juridic, Bucharest, 2018, pp. 615-626.

11. Pella, V.V., *Criminalitatea colectivă a statelor și dreptul penal al viitorului*, (translated by A. Ciucă, A. Gentimir, R. Boca), Hamangiu, Bucharest, 2017.

12. Todeschini V., *Ripensare il terrorismo nel diritto internazionale. Una ricerca sul concetto giuridico di terrorismo internazionale di Stato*, Jura Gentium, No. 1, 2013, pp. 7-41.

13. www.mae.ro, [Accessed 29 March 2020].