Center for Open Access in Science

Open Journal for

Legal Studies

2018 ● Volume 1 ● Number 1

ISSN (Online) 2620-0619

OPEN JOURNAL FOR LEGAL STUDIES (OJLS)
ISSN (Online) 2620-0619
www.centerprode.com/ojls.html
ojls@centerprode.com

Publisher:

Center for Open Access in Science (COAS)
Belgrade, SERBIA
www.centerprode.com
office@centerprode.com

Open Journal for Legal Studies, 2018, *1*(1), 1-50.
ISSN (Online) 2620-0619

CONTENTS

Open Journal for Legal Studies, 2018, *1*(1), 1-50.
ISSN (Online) 2620-0619

Center for Open Access in Science ▪ https://www.centerprode.com/ojls.html
Open Journal for Legal Studies, 2018, *1*(1), 1-8.
ISSN (Online) 2620-0619 ▪ https://doi.org/10.32591/coas.ojls.0101.01001u

Legal Regulation of the Crypto-Currency Taxation

Katsiaryna Ulyanava

Belarusian State University, Law Faculty, Minsk

Received 31 March 2018 ▪ Revised 20 June 2018 ▪ Accepted 11 July 2018

Abstract

At the beginning of the 21st century, we see the emergence of new legal relations related to the massive emergence of crypto-currencies. The natural question is, what to do with the taxation of the crypto-currency, new mining activity. We are analyzed different approaches in the world for this question. In the Republic of Belarus are created conditions for introduction in the economy of the technology of transaction block ledger (blockchain) and legally fixing such complex concepts as crypto currency, mining, digital sign (token). Granting tax holidays for 5 years gives, as advantages in attracting foreign business to the jurisdiction of Belarus, and can contribute to the inflow of illegal money, and therefore it is necessary to strengthen internal control to prevent the legalization of proceeds from crime, and to take an active part in global international initiative – the BEPS Plan (Base Erosion and Profit Shifting).

Keywords: taxation of crypto-currencies, mining, digital sign (token), blockchain.

1. Introduction

At the beginning of the 21st century, we see the emergence of new legal relations related to the revolution in the sphere of money circulation, changes in the world financial market and the ways in which business is conducted, the cause of which is the massive emergence of crypto-currencies. At present, there are more than 2000 crypto-currencies in the world, of which about 100 are known. The most popular ones are Bitcoin, Ethereum, Ripple, Litecoin, etc.

Among the experts of the world community, including lawyers, economists, financiers, there have been numerous discussions on the legal regulation of the crypto-currencies, the activities for their creation, mining, taxation, etc.

In this article, we will consider some aspects of the taxation of crypto-currencies, tokens and mining.

2. Discussion

The Decree of the President of the Republic of Belarus on 21 December 2017, No. 8 *On the development of the digital economy* (1) came into force on 28 March 2018 in the Republic of Belarus, in which the definitions of a crypto-currency, token, mining, were given for the first time. Thus, the Crypto-currency is a bitcoin, another digital sign (token) used in international circulation as a universal means of exchange.

Mining is an activity different from the creating of own digital signs (tokens), the aim of which is the maintaining of the functioning of the transaction block ledger (blockchain) by

Correspondence: Katsiaryna Ulyanava, Schevchenko boulevard 22, appt. 10, Minsk, BELARUS. E-mail: kate.ulianova@gmail.com.

means of the creating of new blocks with information about performed operations in such ledger. A person who carries out a mining process becomes the owner of digital signs (tokens) arisen (mined) as a result of his activity on mining and can get digital signs (tokens) as a reward for the verification of the operations executing in the transaction block ledger (blockchain).

- During last years the blockchain technology as well as different crypto-currencies were invented.
- Due to the fact that these technologies allow to transmit finances, the legal regulations of those are required.
- Several approaches to the concept of crypto-currency are defined in the world: property, assets, decentralized virtual currency, virtual goods, and property rights.
- Belarusian Decree No. 8 On the development of the digital economy proposes the cutting edge legal approaches for working with crypto-currencies.
- The key points in this sphere are: the international collaboration for the development of legislative initiatives and the joining of Belarus to the BEPS Plan.

Digital sign (token) is a record in the transaction block ledger (blockchain), or another distributed information system which verifies that the owner of a digital sign (token) has rights to civil-law objects and/or is a cryptocurrency.

Legal persons and individuals have the right to own tokens and, subject to the specifics established by Decree No. 8, perform a number of operations, for example, mining, storing tokens in virtual wallets, exchanging tokens for other tokens, their acquisition, alienation, etc. Legal persons are entitled to perform through a resident of the Park of High Technologies carrying out a respective activity, to create and place own tokens in the Republic of Belarus of abroad, to store tokens in virtual wallets, through cryptographic platform operators, cryptocurrency exchange operators, other residents of the Park of High Technologies carrying out a respective activity, to acquire, alienate tokens, to perform other transactions (operations) with them. Cryptographic platform operators, cryptocurrency exchange operators are obliged to ensure availability on accounts in the banks of the Republic of Belarus of monetary means in the amount of not less than 1 million Belarusian rubles for a cryptographic platform operator, not less than 200 thousand Belarusian rubles for a cryptocurrency exchange operator.

The activities on mining, acquisition, alienation of tokens, carried out by individuals independently without involving other individuals by labor and (or) civil-law contracts, is not entrepreneurial activity. Tokens are not the subject to declaration.

For purpose of accounting tokens arisen (generated) in the process of mining or acquired otherwise shall be recognized as assets. Placement by legal persons of tokens created by them leads to arising of obligations before the owners of those tokens. For purposes of taxation, alienation of tokens, including by means of their exchange for other tokens, shall be considered as realization of property rights.

In accordance with the clause 3 of the Decree No. 8, with respect to republican taxes, it was decided not to recognize the activities of mining, acquiring (including as a gift), alienation of tokens as objects of taxation until 1 January 2023.

Apart of the creation of crypto-currencies and their mining, the games based on the blocking technology, for example “CryptoKitties” based on the Euthereum platform, are becoming popular.

The essence of the game – the purchase and reproduction of cryptokitties, and their sale at auction. The cost of cryptokitties varies from 0.03 ETH ($14) to 250 ETH (about $117,000). The game “CryptoCelebrities” works roughly the same way: the system generates some cards, the user chooses the “contract” of what celebrity he wants to buy and makes the deal using Ethereum. Then the system generates a new, higher, price for the contract. Another user can buy out the celebrity card, and the contract owner can’t refuse the deal. When the contract is sold, the player gets almost the entire amount; the system takes just a small fee. The more contract is being bought, the higher its cost. Currently the most expensive card is the card of the Ethereum creator,

programmer Vitaly Buterin, its cost is 24.5 ETH ($25,000). It was bought for 31 times. The number of games like CryptoKitties will be only increasing in the future. Based on the Belarusian legislation, they are recognized as digital signs that are not the subject to taxation.

Let's consider the legislative approaches on the issues of the regulation of crypto-currencies, mining and taxation in other countries.

In accordance with the Draft of Federal Law of the Russian Federation *On digital financial assets* (Ministry of Finance of Russia, 2018) crypto-currencies, tokens refer to digital financial assets. Digital financial asset is a property in an electronic form, created with the use of cryptographic means. The ownership of this property is certified by adding digital entries to the digital transactions register. Digital financial assets are not a legal means of payment in the territory of the Russian Federation. Mining is an entrepreneurial activity aimed at the creating of a crypto-currency and/or validation in order to get a reward in the form of a crypto-currency.

Crypto-currency is a type of digital financial asset which is created and considered in the distributed registry of digital transactions by participants of the registry according to the rules of the maintaining of the registry of digital transactions.

Token is a type of a digital financial asset that is issued by a legal entity or an individual entrepreneur (hereinafter referred to as an issuer) in order to obtain financing and is recorded in the registry of digital records.

According to the latest explanation of the Russian Ministry of Finance in November 2017, the Tax Code of the Russian Federation does not provide any special procedure for taxing crypto-currencies and mining bitcoins. Thus, the income of an individual gotten from mining is taxed as a benefit in kind, i.e. at a standard rate of 13%. Russians should calculate the tax independently and submit a tax return to the tax declaration. Profit of a legal entity is calculated at a standard rate of 20%. The income in the form of a digital currency, received as a result of mining, is also a subject to taxation. A controversial issue is the taxation of the value added tax, because at the legislative level, digital money is not defined as a commodity.

As for Ukraine, the draft laws on the settlement of the crypto-currency market are at the stage of discussion. According to the Draft Law No. 7183 *On the circulation of the crypto currency in Ukraine* (Verkhovna Rada of Ukraine, 2018), crypto-currency is a program code (a set of symbols, numbers and letters) which is an object of ownership, which can be used as a barter, information about which is deposited and stored in the block system in the accounting units of the current block-system system in the form of data (program code).

Ukrainian lawmakers have followed the path of Canada and see operations with crypto-currencies equated to barter transactions with the application of the norms of civil legislation regulating the barter agreement. Mining is the computational operations executed by a miner with the help of own and/or leased specialized equipment, in order to ensure the operability and security of the blocking system. Depending on the conditions of the system, a miner receives a reward of the blocking system. The procedure for the taxation of crypto-currencies is planned to be provided for in the future by the Tax Code. Therefore, at present, standard rules of taxation apply to crypto-currency operations in Ukraine. The income of an individual gotten in the form of a digital currency is taxed at the standard rate of 18%, and the profit of legal entities depends on the tax system of specific legal entities. Also, as in Russia, the issue of paying value-added tax is controversial. Crypto-currency is not defined as a commodity at the legislative level.

In the United States, legal regulation of crypto-currency is limited. Starting from 2014, the Internal Revenue Service (IRS) has defined the crypto-currency as property, the transactions with which must be taxed (including mining) in accordance with the principles applied to property taxation. Thus, salaries paid to employees in the crypto-currency are subject to Federal Income Tax and Payroll Taxes. The tax base for wages in bitcoins is calculated on the basis of the rate of the crypto-currency at the date of a payment. Payments for services of a counterparty under a civil law contract in a digital currency are also taxed. US tax residents who sell goods and services in exchange for crypto currency are required to include the cost of the obtained bitcoins in the annual

tax return. It is calculated on the basis of a fair market price in US dollars at the date of the receipt (the exchange rate on that day) (Axon Partners, 2017).

The nature of the profit or loss from the sale or exchange of crypto-currency depends on whether the virtual currency is the main asset of the taxpayer. In accordance with the IRS clarifications, the crypto-currency is considered as a capital asset, similar to shares, bonds and other investment instruments, so the taxpayer is obliged to take profits and losses into account while calculating the taxable base. The profit arises in the case when the sale price in US dollars exceeds the adjusted purchase price. A loss arises when the sale price is lower than the adjusted purchase price. Mining is also a subject to taxation. Miner must include the fair market value of the extracted crypto-currency in his annual gross income.

The information about payments in the crypto currency must be submitted to the Tax Service (IRS). The incomes received by an individual in the crypto-currency, and other objects of taxation must be declared in dollars. Some penalties may be imposed to the residents who violated the tax laws. The control will be carried out on the basis of detailed accounting of all transactions with bitcoins. So, in December 2016, the Federal District Court of the Northern District of California authorized the Tax Service to request data on the bitcoin transactions of Coinbase users. Since January 1, 2018, a ban on tax evasion using crypto-currency is introduced, all transactions are subject to taxation (Axon Partners, 2017).

In Canada, the payment for goods or services using crypto-currency is taxed as a barter transaction. In the case of the sale of a digital currency, Income Tax, Corporation Income Tax or Capital Gains Tax are levied. Crypto-currency, obtained as a result of mining, which was carried out for commercial purposes, is subject to Income Tax. The definition of the commercial component is carried out in each case independently. The wages of an employee gotten in the crypto-currency are subject to taxation (The Eurasian Economic Commission, 2017).

The European Central Bank classifies crypto-currency (in particular, bitcoin) as a convertible decentralized virtual currency. In November 2015, the European Court of Justice decided that bitcoins serve no other purpose than payments, and that there is no VAT while buying or selling bitcoins (in Europe), despite the absence of the legal currency status. Other transactions may be taxed, for example, with income tax or capital gains tax. The procedure for taxation of crypto-currencies and their transactions is regulated by the national legislation of the EU members, depending on the nature of the crypto-currency operation (Axon Partners, 2017).

In Norway, the crypto-currency is subject to Capital Gains Tax at a rate of 24% and Wealth Tax, is exempt from VAT.

In Austria, the crypto-currency is considered by the tax authorities as an intangible asset, and its mining – as an operating activity. Therefore, the income received as a result of its alienation is subject to Income Tax.

In Sweden, the crypto-currency is subject to capital gains tax at a rate of 30%.

In Germany, since 2013, bitcoin is a kind of private money, the analogue of other investment instruments, such as stocks or bonds. As for taxation, a capital gains tax is withheld at a rate of 25%, and only if profits were received within one year after receiving bitcoins. In the case if the sale of bitcoins is carried out more than a year after the purchase, it will not be subject to a capital gains tax, and the transaction itself will be considered as a “private sale”.

In 2013, the Finnish tax authorities issued a special instruction for the taxation of the crypto-currency. Virtual currencies should not be considered “actual, official currencies”, while being the legal means of payment in the same time. The instruction gave two main approaches to taxation of income from operations with crypto-currencies, depending on the type of activity. When making investment or exchange transactions, income and expenses were regarded as an increase or decrease of the capital. In this case, the cost of obtained bitcoins was equated to their price on the exchange at the time of acquisition. At the same time, losses from such activities were not to be attributed to expenses in the tax declaration.

When a taxpayer received bitcoins as the income from mining, the tax authorities expected to charge coins as ordinary incomes. The price of coins was determined at the current

exchange rate. Companies selling goods and services for bitcoins or other crypto-currencies had to pay income taxes based on stock quotes on the day they got coins. If the price on the exchange was not available (if the coin was not yet traded on the exchange), then the price agreed by counterparties in the documents for purchase and sale was accepted. The fees in the crypto-currency could be attributed to the expenses in the declaration (Forklog, 2018)

In November 2014, almost a year before the relevant decision of the European Court, the Finnish regulators recognized bitcoin as a financial service, which is not given the legal status of a currency, and is exempt from VAT.

As for UK lawmaking practice, in 2014 Her Majesty's Revenue and Customs (HRMC) published a policy paper on the taxation of operations with crypto-currency. In accordance with it, the income obtained as a result of the mining of digital money (tokens) and their exchange into the pound sterling or another currency, should not be taxed with the VAT. But VAT must be levied on suppliers of any goods or services sold for crypto-currency. The cost of goods or services subject to VAT should correspond to the value of the crypto currency in pounds sterling at the time of such an operation. Depending on the situation, the income (profit) of the business entity is subject to Capital Gains Tax, Corporate Tax and Income Tax (Axon Partners, 2017).

In Switzerland, the crypto-currency is an asset, not securities. Operations with crypto-currencies do not require special permits (licenses), but some activities, including the purchase and sale of crypto-currency on a commercial basis and on existing trading platforms, may be subject to licensing. Also, the general requirements of the Swiss legislation for combating money-laundering apply to transactions with crypto-currencies.

In Japan in April 2017, crypto-currencies are officially recognized as legal means of payment. The concept of crypto-currency is separated from the concept of electronic money, crypto-currency is recognized not as a monetary means, but as a negotiable asset that can be used as a payment instrument. In this case, the operations for the exchange of crypto-currency for fiat money are not subject to the local analogue of VAT.

Crypto-currencies are equated to assets that can be used for payments and transmitted digitally. Receipts from operations with bitcoins, tokens are considered income from doing business and are taxed at the appropriate rates. The income gotten by an individual as a crypto-currency is subject to Income Tax, and the profit of a legal entity in digital currency is a corporate income tax.

The law of China does not contain special rules for the taxation of digital currency and transactions with it. Crypto-currency is defined as a virtual commodity, a non-monetary digital asset, but not a currency. Thus, the sale of digital money can be taxed with VAT, and income and profits in the crypto-currency are subject to Corporate Income Tax, Individual Income Tax and Capital Gains Tax. Since September 2017, there has been a ban on the public placement of crypto-currencies. At the same time in China, crypto-currency for individuals and crypto-currency transactions between them are allowed (Axon Partners, 2017).

In Singapore, crypto-currency is considered an asset, not a means of payment. In case of compliance with certain criteria they can be classified as securities. Operations with them may be subject to a local analogue of VAT. The very status of the crypto-currency is not regulated in details, but there is legal regulation of certain activities related to the circulation of crypto-currency. In particular, the Monetary Authority of Singapore (MAS) issued a number of regulatory documents governing the public offering of digital assets (tokens), as well as trade in them.

In October 2017, the UAE issued a basic guide to crypto-currencies and their public offering. Mining or spot transactions in virtual currencies are not a regulated activity in its own right. Any licensed companies that provide or use virtual currencies for financial services must adhere to existing anti-money laundering and terrorist financing laws.

Argentina is one of the leading countries in the use of crypto-currency, which is defined there as “the digital embodiment of value that can be used for e-commerce and whose functions are to form an exchange environment and/or a unit of account and/or value storage”. In July 2014, the Department of Financial Information of Argentina (UIF), the authorized body for combating

money-laundering, issued a statement instructing all financial institutions performing operations with "bitcoins and other virtual currencies" to send information about such transactions to the UIF (KPMG, 2017).

In Australia, operations involving bitcoins and other crypto-currencies come under the definition of barter agreements. For tax purposes, bitcoin is considered an asset, not a payment instrument or a foreign currency. The income and profits received from transactions in digital currency are taxed with Income Tax and Corporate Tax. Companies performing transactions in bitcoins must properly document, record and indicate the dates of operations. Companies receiving bitcoins in the form of payments should indicate their value in Australian dollars and be treated as ordinary income. Operations with bitcoins for personal purposes are exempt from taxation when bitcoin is used as payment for goods and services for personal consumption, and when the transaction size does not exceed 10,000 Australian dollars.

The production of bitcoins and exchange for commercial purposes in Australia are considered exchange trades and are taxed accordingly.

If the digital currency is used as an investment, there is no need to pay the Capital Gains Tax. In Australia, there is a legal opportunity to pay wages in the crypto-currency, but only with the mutual consent of the employer and the employee and the existence of a contract between them (The Eurasian Economic Commission, 2018)

In Hong Kong, bitcoins and crypto-currencies are defined as virtual goods, and the tax law does not contain special rules for taxing such transactions.

Thailand, Bangladesh, Ecuador, Vietnam and Bolivia went on the road to a total ban on the use of crypto-currency.

Thus, several approaches to the concept of crypto-currency are defined in the world: property, assets, decentralized virtual currency, virtual goods, property rights.

3. Conclusion

Based on the foregoing, it can be concluded that the Republic of Belarus has adopted a progressive approach, legally defining such complex concepts as crypto-currency, mining, digital sign (token). We believe that in the future it is necessary to differentiate more clearly the notions of "crypto-currency", which will become a means of payment, tokens, including the results of games such as "cryptokitties" and other digital objects, for example, game gold, accounts, websites and etc. Accordingly, the income received from transactions with such objects, in certain conditions, will be subject to taxation.

Granting tax holidays for 5 years gives advantages in attracting foreign business to the jurisdiction of Belarus, and nevertheless can contribute to the inflow of illegal money, and therefore it is necessary to improve internal control to prevent the legalization of money obtained by criminal sources, and to take an active part in global international initiative – the BEPS Plan (Base Erosion and Profit Shifting). We believe that by 2023 it is expedient, based on the experience of the European Union, to free turnover, profit (income) from mining activities, creation, acquisition, alienation of tokens from value-added tax, otherwise apply general taxation approaches. The key points in this sphere are the international collaboration for the development of legislative initiatives and the joining to the BEPS Plan by all countries.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The funding source(s) had not involved.

Conflicts of interest: none.

References

Axon Partners (2018). *Legal regulation of the crypto-currency business*. Retrieved from http://axon.partners/wp-content/uploads/2017/02/Global-Issues-of-Bitcoin-Businesses-Regulation.pdf, Accessed 29 January 2018.

Decree of the President of the Republic of Belarus on Development of Digital Economy No. 8, 21 December 2017 (2017). Retrieved 28 February 2018, from http://law.by/document/?guid=3871&p0=Pd1700008e.

Forklog (2018). *High taxes and a lot of state - how bitcoin business develops in Finland*. Retrieved 29 January 2018, from https://forklog.com/vysokie-nalogi-i-mnogo-gosudarstva-kak-razvivaetsya-bitkoin-biznes-v-finlyandii/.

KPMG (2017). *Review of Legislative Regulation of Crypto-Currency in Selected States*. Retrieved 29 January 2018, from https://assets.kpmg.com/content/dam/kpmg/ru/pdf/2017/11/ru-ru-cryptocurrency-legislative-regulation-worldwide-november-2017-upd.pdf.

Ministry of Finance of Russia (2018). *About digital financial assets*. Retrieved 29 January 2018, from https://www.minfin.ru/ru/document/?id_4=121810&order_4=P_DATE&dir_4=DESC&is_new_4=1&page_4=1&area_id=4&page_id=2104&popup=Y#ixzz55UeD7vF0.

The Eurasian Economic Commission (2018). *Regulation of crypto-currencies: a study of the experience of different countries*. Retrieved 29 January 2018, from http://www.eurasiancommission.org/ru/act/dmi/workgroup/Documents/digest/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82%20%D0%B2%20%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B0%D1%85%20%D0%BC%D0%B8%D1%80%D0%B0.pdf .

Verkhovna Rada of Ukraine (2018). *Draft law on the circulation of cybercriminals in Ukraine*. Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684, Accessed 29 January 2018.


C O A S

Center for Open Access in Science ▪ https://www.centerprode.com/ojls.html
Open Journal for Legal Studies, 2018, *1*(1), 9-24.
ISSN (Online) 2620-0619 ▪ https://doi.org/10.32591/coas.ojls.0101.02009v

Users' Considerations About Possibilities of Self-protection on Social Networks

Vida Vilić

Clinic of Dentistry, Niš

Received 16 February 2018 ▪ Revised 8 May 2018 ▪ Accepted 18 May 2018

Abstract

The modern world of the Internet has changed significantly with the emergence of social networks. With their popularity and a large number of users, social networks have created a kind of "control" of the everyday activities of people, their habits, their movability and socializing. In Serbia, social networks became popular in 2006, while in 2007 the real expansion of social networks begins. The Internet and social networks provide countless opportunities for getting to know new people, acquiring and developing personal and professional relationships, creating different social circumstances; but the opportunities for abuse/misuse of the Internet and social networks also increased. Discussing the abuse/misuse of the Internet and social networks, arose the issue of protecting individual personal rights – the right to privacy, and about how the users of social networks can contribute in prevention of privacy violation. Certain groups of people are more likely to be exposed to privacy violation.

Keywords: social networks, social networks' users, privacy, information privacy, privacy protection.

1. Introduction

1.1 *The scope of perceived problem*

The Internet is being used by many people all around the world, who communicate with each other, enter into different social relations and liaisons, and develop personal and professional relationships for communication, social networking, and participation in different social events. According to the Statistical Office of the Republic of Serbia, 63.2% of households owned a computer in the household in 2014, while 62.8% used the Internet (Statistical Office of the Republic of Serbia, 2014). The invention and development of the computer are one of the most outstanding and fascinating results of human thinking and innovation: computers are omnipresent, absolutely invaluable in all areas of work (Vilić, 2013). The Internet is a global information system in modern society; it is the World Wide Web, or the "network of networks", which consists of a large number of separate computers connected in a network structure. As a global worldwide network, the Internet gives a global dimension to the virtual space, which means that it provides an interface between any two points on the planet through cyberspace (Vilić, 2017: 1). Concurrently, cyberspace represents a social space created by merging two types of communication: communication through computer networks and business communications, supported by a computer system.

Correspondence: Vida Vilić, Zetska 6/63, 18000 Niš, SERBIA. E-mail: vila979@gmail.com.

In the short history of the Internet, one of the most powerful innovations is the emergence of social networks, which further expand the possibilities of communication between people, no matter where they are. Some Internet applications have given rise to issues concerning the protection of privacy, opening the debate whether social networks actually serve commercial interests or create new communication opportunities and connect people around the globe. Individual privacy, on the other hand, encompasses a whole spectrum of different rights, but the most exposed part of the right that relates to personal data is exposed to the abuse on the Internet. The risks of personal data abuse are primarily related to identity theft and theft through the misuse of personal data (online shopping, secure password, secure e-mail), but also on the misuse of personal data for commercial purposes (unauthorized sale, unwanted "spam" e-mails, etc.).

- The use of information technologies worldwide and in Serbia is very widespread and has a tendency for further intensive development.
- The emergence of the Internet and social networks has had a multiplier effect on contemporary life and the development of specific forms of criminal behavior, which is reflected in the abuse of information communication technology and its systems.
- Social networks on the Internet, as widespread and most popular way of communication in the modern world, made private life an integral part of public life since there is no privacy guarantee for data posted on the Internet and social networks.
- The serious lack social networks are the large exposure of users to various forms of abuse, such as identity theft, fraud, digital violence (sexual violence and harassment, peer violence, stalking, cyber mobbing, hate speech), terrorism, vandalism, human trafficking and human organs selling, piracy, as well as the replacement of the real world with virtual followed by pathological dependence on the use and abuse of the Internet.
- Privacy has got a new dimension in one new concept – information privacy, which refers to the collection, processing, storage and sharing of data about an individual.

The subject of this paper is the theoretical and empirical examination of one of the most widespread forms of computer crime, involving the violation of the right to privacy by misuse of social networks, as well as the awareness and attitudes of social network users about their exposure to personal data abuse and potential victimization.

The basic aim of the paper is to contribute to the development of a better system of protection and greater safety of social network users, based on theoretical and empirical research on computer crime and social network abuse. In order to build a better system for protecting social network users from the many types of criminal behaviors they are exposed on a daily basis, it is necessary to point out the need of criminological victim-based study of social networks, given the widespread use and the large number of abuses of data transmitted through these networks, but also the awareness of users about the vulnerability of the personal data that they publish on the Internet, the mechanisms for (self)protecting their privacy and published data, and improving mechanisms that provide protection and sanctions.

1.2 *The right to privacy and social networks – Privacy and information privacy*

In the original sense, privacy signifies the desire of a person not to be disturbed (Nikolić, 2014). In theoretical consideration of the term "privacy" and the content of this term in Anglo-Saxon literature, Judges Louis Brandeis and Lawyer Samuel Waren, firstly in 1890 in the article *The right to privacy* formulated the most accurate and well-defined concept of privacy, as "right to be left alone" (*Harvard Law Review*, Vol. 4, No. 5, in Šurlan, 2015). In this sense, privacy implies the protection of personal autonomy, moral and physical integrity, the right to choose life style and way of life, interaction between people, etc.

The right to privacy is one of the fundamental human rights, both in national and international level, guaranteed by the constitutional law, public law and civil law, which acts towards everyone (*erga omnes*) and protects person from harassment by state authorities and other people. Opposite of publicity, privacy implies secrecy and indifference. It refers to the private life of an individual in which it is justifiable to expect peace, tranquility and intimacy (Surco, 2015). The right to privacy allows an individual to selectively show as much as that individual wants (Jovanović, 2014: 94).

Theoretically, the term "privacy" has not undergone significant changes over time. However, the changes occurred in practical application of this right in the modern era, characterized by global society and information technology. The availability of information, in particular in the form of electronic data, jeopardized the respect of the right to privacy, both by individuals and by the authorities. The privacy in electronic communications involves the collection, processing and provision of user information to third parties, whereby individuals when recording activities and personal data about themselves determine when, how and to what extent the information about their private sphere needs and may be available to others (Jovanović, 2014: 94). The central place of this multidimensional construction is the desire to keep personal data personal and not freely available to other people.

Modern communication systems can fully fulfill their role if they are reliable and also available to users. Confidentiality of information shared by users in virtual space must not be compromised, and the users must be sure of the sender's identity and that the information received must be identical to the sent information. Any departure from this rule diminishes the trust of users.

Privacy can be divided into spatial, communicational and informational privacy (Boban, 2012: 595). Spatial privacy refers to maintaining privacy in someone's home and other space in which people lead their own lives separately from the others. This type of privacy includes the respect of the right to have its own space, both within home and family and in the workplace. Communicational privacy refers to privacy of correspondence and other forms of communication with other people.

Informational privacy is closely related to the development of information technology and refers to collecting personal data about internet users, to managing these data and to their further use. In the narrow sense, informational privacy refers to a need of an individual, a group or an institution to independently decide when, how and what information about themselves they wish to share with others (Vilić & Radenković, 2016: 63). In a broader sense, informational privacy includes informational security, meaning that informational society exists when each individual can decide how to dispose his personal data, regarding his needs and community requirements (Boban, 2012: 582). Informational privacy consolidate legal values of protecting the rights of an individual in society that have developed information technology and the concept of personal data, referred to as "e-privacy" (Boban, 2012: 585).

The right to informational privacy includes the right to be informed, the right to an adequate use of personal data, the right to control these data, the right of correction published data and the right to use legal remedies and appeals (Drakulić, 1996: 65).

The right to privacy, as an individual right, can be defined as a control, editing, managing and deletion of information about any individual, when the owner of the personal information decides (Westin, 1970: 97). In the context of social networks, privacy and personal information include all information that an individual publishes on its profile, which includes pictures, comments, location, and social information (King, Lampinen & Smolen, 2011: 97). Thus, the possibility of abuse of the right to privacy on social networks can be viewed through two conceptual categories: social abuse or organizational abuse of this right (Krasnova et al., 2009: 97).

The most common ways of misuse the right to privacy on the Internet are: unauthorized access, collection and processing of personal data, misuse of collected data, interception of sending information. Likewise, the difficulty is the fact that users voluntarily and on their own initiative publish a large number of their personal data on the Internet, without considering whether this data will be misused or not.

1.3 *Social networks and privacy*

1.3.1 *The concept and development of social networks*

The modern world of the Internet has changed considerably with the emergence of social public networks, which have become one of the most popular services on the Internet. The virtual space was previously full of interesting and useful information, but there were very few opportunities to make this space interactive and to actively participate in the creation of data, which is enabled by the emergence of social networks. Today, there is a growing mass of social network users, who is not well informed and educated about the security risks and protection options in the cyberspace.

As the number and popularity of social networks increased, the number of users also increased, leading to the emergence of negative consequences and special form of criminality that manifests itself through social networks and virtual space in general, as well as creating a new form of dependency – Internet and social network dependency. Nowadays, social networks are connecting people around the globe. By social networking, the world is able to visualize relationships between individuals (*Top 10 Social Networking Sites*, 2012).

In the last few years, the number of social networks has grown rapidly, as the need for this kind of networking and the exchange of various content through social networks has increased. In the Republic of Serbia, available data showed the existence of the same tendency in increasing the number of social networks and their users. A survey on the use of information and communication technologies of the Statistical Office of the Republic of Serbia in accordance with the Eurostat methodology published in the business portal "Economy" (*Poslovni portal "Economy"*, 2012) in early 2012, showed that in Serbia social networks have 92.1% users of the population between 16 to 24 years.

The development of modern technologies greatly jeopardized personal privacy in the virtual space. The very fact that personal data can be collected, stored, distributed, duplicated, published and available to a wide circle of people has created insecurity and a sense of insufficient protection. A decade ago, while computer technologies were still in development, all of these data were transferred from virtual space to various digital media, making "digital files".

Social networks and social networking are the simple act of maintaining and/or strengthening an existing circle of friends and/or acquaintances, and also the tendency of spreading these circles (Kušić, 2010: 103). There are also concepts according to which social networking contributes to the quality of social interactions; complements and encourages communication in the "real" world; encourages the development of tolerance of diversity, by overcoming classical, religious, cultural, political differences; encouraging creativity, academic abilities, social skills, maturation and development of personal identity (Žunić-Pavlović, 2013: 139).

The social network is usually defined as a social structure, consisting from individuals or organizations, called "knots", which are linked to one or more specific types of interdependence, such as values, visions, ideas, financial interests, friendship, kinship, common interest, financial exchange, non-corruption, sexual relations or relationships of trust, knowledge or prestige (Vidanović, 2006: 437-438).

Social networks can also be defined as a set of internet programs that serve to connect people in communication with their friends, relatives, colleagues and clients, where their interests can be social, business or mixed (*Social networking*, 2014). Their purpose is to allow people to be a part of a virtual community in which they can develop different relationships, as well as the form of human interaction, in which, through existing acquaintances, new persons are introduced to create social or business contacts (*Sigurnosni rizici društvenih mreža*, 2015).

Often referred to as the "virtual community" or "a set of personal profiles of different people", the social network is a presentation of the Internet that connects people in one place, in order to exchange opinions, talk, share ideas and interests and create new contacts (*Social networking*, 2014). Such activity on the Internet is a characteristic social medium, whose content, unlike other media, is created by hundreds and even millions of people.

1.3.2 *The privacy of social networks' users*

Social networks have created real detailed personal databases, consisting of the lives of their users (Viégas, 2005: 18), and these databases are supplemented every day, which increases the amount of information that is public and available to all actors of virtual interaction in cyberspace. As soon as personal information is published on the Internet, it becomes public and accessible to everyone to read it and use it, so the user loses control who has insight into his intimacy and published information. Users most often overestimate their control over the information they publish via social networks, and they are not aware of their technical knowledge about the use of social networks, and the privacy settings of their virtual profiles.

The main purpose of social networks is interaction and communication in cyberspace, and users interact with each other on their own pages (so-called "profiles") and thus visualize their relationships. The relationship between the privacy and the user profile on the social network is multiple: in some cases, users want the information they publish about themselves to be accessible only to a narrow circle of people, while in some other situations users are willing to reveal their secrets to strangers and even to anonymous strangers. All this information, if misused, can cause severe consequences, ranging from identity theft to harassment and stalking, from embarrassed and shame, through various types of discrimination, or even to blackmail. Despite the awareness that all privacy on social networks may be violated, personal data are still voluntarily published on such sites.

Modern countries have faced the problem how to balance between the individual's right to privacy and the public's right to be informed; two rights that, although they act in the opposite way, are constituted parts of the foundation of a modern democratic society in which the state has the right to limit the right of individual privacy. In the context of computer crime, a new, sophisticated, unobtrusive, technically educated profile of the perpetrators of a criminal act has been created, which is difficult to confront because of its "invisibility" and "intangibility". Due to the extremely large number of users, accessibility of data, openness in communication, and insufficient legislative both on the national and international level, social networks represent a great hideaway for the perpetrators of this type of crime.

There are four main reasons why there is a possibility of violating the right to privacy on social networks (Shah, 2013):

(1) The imperfection of social network users, related mainly to the imperfections of a man as a human being and his need to share his own privacy with other people and the lack of awareness that the privacy does not exist in cyberspace so once something gets published it goes public this very moment;

(2) Flaws in the programs (software) that social networks use, resulting in lack of privacy protection mechanisms on social networks, making users' privacy, unprotected from all direct malicious attacks, such as the theft of personal data, creation of fake profiles, etc.;

(3) Inadvertent disclosure of personal data: personal data on social networks can be reached by the method of exclusion (e.g. on the basis of the year of graduation, we can conclude how old the user is, even tough it is not written in the profile);

(4) Conflict of interest: most social networks gain financial benefits from variety of ads placed by an advertising agencies, which create a conflict of interest regarding collecting personal data that advertising agencies can access.

By the definition given by Joseph Cannataci (1987), data protection means protecting an individual from misuse or inadequate use of personal data by a person, private organization or state. Internet users can protect their privacy through controlled disclosure of personal information. Those users who want to protect their privacy better, must try to achieve Internet anonymity – only this way it is possible to use the Internet without giving the possibility to a third party to connect with Internet activities for personal identification of Internet user.

Most social network users publish a large amount of private and personal data, which are immediately available to countless users around the world. Interestingly, numerous studies have shown that users of various social networks consciously share their private data via social networks: among the 4,000 students who have a Facebook profile, a small percentage has changed the basic privacy setting by which all data is public and accessible to all Internet users (Gross & Acquisti, 2005, in Utz & Kramer, 2009), and among the 20,000 profiles on the MySpace social network only 27% made their profiles private (Thelwall, 2008, in Utz & Kramer, 2009).

In electronic communications privacy can be considered as "the freedom from systematic surveillance and recording of activities and personal data; that is, the right of individuals to determine when, how and to what extent information about their communications should and may be available to others" (Nikolić, 2014). The best way to protect the privacy of all Internet users is precisely the principle of controlled disclosure of personal information. Publishing "posts" and personal information on the Internet can be detrimental to the privacy of an individual, because the information (blogs, images and web pages) that are published on the Internet is permanent.

1.3.3 *Most common rules of privacy policy on the social networks*

Social networks and companies that provide social networking sites, their wealth and popularity build by observing the behavior and relationships in society, as well as with targeted advertising, using the collected data on social network users and by monitoring their regular activities on social networks. This is precisely the reason why social networks often share the personal information and interests of its users with different companies, most often with marketing and advertising companies (Catanese et al., 2011).

Even though a large number of social network users are aware of the facts that privacy on social networks can be violated or at risk, users still publish many personal about themselves. Some of the reasons for the voluntary disclosure of personal data have been recognized as the desire for attention, disinterest or relaxed attitude towards respecting privacy, incomplete information, trust in the security of data on the social network, and trust in friends on the social network (Gross & Acquisti, 2005: 77).

Social networks with the largest number of registered users, such as Facebook, Twitter and LinkedIn, has the most number of the violation of the privacy right. The questions that arise

are whether social network users are still the owners of all the information and whether it is possible to permanently remove social networks' accounts and delete one published information?

1.4 *Security risks on social networks and recommendations for their reduction*

Accelerated technology development has enabled faster data processing and efficient functionality, as well as the availability of numerous information, while providing the individual to remain "anonymous". The famous New Yorker magazine began publishing a comic strip in 1993 that said that "... on the Internet, no one knows that you are a dog" (Hargittai, 2007: 276), and that it is difficult to reveal someone's identity on the Internet because the possibilities for the abuse are innumerable. Social networks can be misused in various ways, and the criminal act that occurs this way can take the form of any of the traditional types of criminality. The concern of the most of the Internet users is caused by the fact that their personal information are automatically generated, collected, stored, interconnected and used for various purposes, including commercial ones, as well as illegal ones (Spasić, 2010: 78).

Personal data, which are unauthorized supplied by misuse of information systems, can be manipulated in various ways. By revealing their personal data, users actually consciously renounce of the part of their privacy. Additionally, uploading of photographs can enable user identification by using the face recognition software tools, but also the location of the user in that photo. Another potential danger lies in the fact that it is not possible to delete all the information contained in the user profile on certain social networks: it is only possible to deactivate the profile, which keeps the data still stored somewhere in the virtual space.

In Europe, the number of social network users who reported being a victim of an attack on privacy on one of the social networks was about 6% (during 2009), then firstly increased to 12% (in 2010), and then in year 2011 to 15% (Cybercrime on social networks continues to climb, 2013). In the US, this figure rose from 8% in 2009 at 18% in 2011 (*Ibid.*).

Internet users can protect their privacy through controlled disclosure of personal information. Publishing "posts" and personal information on the Internet can be harmful for the privacy of an individual, because the information (blogs, images and web pages) that are published on the Internet are permanent. The misuse of data can be various, but most often, depending on the impact of potential attackers, it is characterized as active (changing the content of the information, as well as modification of network packs, production of unauthorized network packs or information flow interruption), and passive (which includes all forms of influencing the flow of information without active changes in the course itself, e.g. illegal supervision, monitoring, etc.) (Spasić, 2010: 80).

The question is to what extent the modern society requires the justification of collecting personal data, as well as the extent of the rights of other social network users when using and disposing personal data of other users. Modern countries have faced the problem of how to balance between the individual's right to privacy and the public's right to be informed: two rights that, although they act opposite, still constitute the same foundations of a modern democratic society, in which the state has the right to limit the privacy right of an individual. According to the terms of use of the most popular social networks, the use of personal data is permitted only to registered users.

The privacy on social networks depends also on the degree of control that the social networks' user has over access and use of personal data. Basically, users must accept the Terms of Use (Terms of acceptance) when accessing different social networks, before use their services. It is interesting that precisely this document often contains clauses that permits the administrators of social networks not only to store user data, but also to share them with third parties, most often marketing companies (Bangeman, 2010). The majority of users makes mistakes when they accept

these policies without previous reading, because they are incomprehensible and too complicated to the user, and often only in English language, which makes it rather difficult for the average user to understand it.

A solution that would reduce the possibility of misuse/abuse of the right to privacy on the Internet, especially on social networks, must be based on three different levels: solving social problems that result in abuse of the right to privacy, overcoming technical problems due to which it is possible for unauthorized persons to access personal data and creating an adequate legal framework and mechanisms for detecting, preventing and sanctioning committed criminal acts. The policy of each social network is to take into account the technical capabilities that would prevent or minimize the misuse/abuse of personal data (Duffy, 2006). Adequate legislation at the supranational level would facilitate the detection of violations of the right to privacy, as well as the sanctioning of the perpetrators of these criminal acts.

2. The results of empirical research

2.1 *The subject, object and the methodology of the research*

The subject of the research was to find out the considerations and attitudes of users of various social networks about the possibility of misuse/abuse of the right to privacy on the social networks, of using/not using appropriate protection mechanisms, as well as the determination of the safest methods of preventive action, in order to prevent the victimization of social network users. The main objectives of the research were: to determine the frequency of use of certain social networks by respondents and their activities on social networks; to obtain data on recognizing violence on social networks and the possibilities of protection; to determine the exposure of respondents to various forms of cyber victimization and the possibilities for timely protection of their right to privacy.

The research had the character of a pilot or a trial research and was done on a suitable deliberately chosen sample. The duration of the research was from January 2014 to April 2014, and the results of the research enabled the elaboration of a valid hypothetical basis for new, wider and deeper research. The research was conducted in two phases. In the first phase, selected social network users (612 of them) were interviewed. One part of the respondents consisted of students from selected primary schools, secondary schools and faculties, while the other part of the respondents were active users of social networks selected by sending questionnaires to certain e-mail addresses. Pupils and students filled in the questionnaires at classes and then returned them to teachers/professors. Social network users filled out the survey online by responding directly to a database that was subsequently processed and analyzed. In the second phase of the research, the collected data were selected and statistically processed, followed by analysis and interpretation of data.

For this research, the questionnaire was made, containing general questions related to the independent variables, like gender, age, education, place of residence. The second type of questions was related to: the frequency of using the Internet and communication via social networks, personal information shared in cyberspace, possible forms of abuse, misuse and violation of the right to privacy in social network communication, forms of protection that can be applied and suggested measures to prevent the violation of the right to privacy via social networks.

The data obtained by the research are encrypted and entered into the matrix. The analysis used the xi-square test to determine the statistical significance of the observed differences between the crossed features. Data processing was done in the SPSS program.

2.2 *Participants*

Considering the different structure of social network users, in order to achieve representativeness, the research was conducted by sending the questionarries to randomly selected email addresses or via social networks (217 or 35.5%), while a larger number of respondents (395 or 64.5%) were randomly selected from students of University of Niš (Faculty of Law, Faculty of Philosophy – Departments: English, Sociology and Psychology), secondary school students (High School "Stevan Sremac", High School of Arts, Food Chemistry High School) and elementary schools' students ("Bubanjski heroji", "Jovan Jovanovic Zmaj" – Malča).

The respondents were of different ages. The prevalence of 20-30 years is predominant (271 or 44.4%), which is understandable, because the largest number of active social networks' users are precisely of this age. The age range of 9-19 years (197 or 32.2%) is fairly common, while the lower numbers of respondents were in the age range between 51-60 years (15 or 2.5%) and 61-65 years (7 or 1.1%). This structure of respondents by age compared to the number of users of social networks show that the users of social networks are mostly younger.

The distribution of respondents shows a significant numerical advantage of female respondents (398 or 65.0%) compared to male respondents (214 or 35%), which is understandable, because women are more active on social networks than men. Considering that the research did not include the comparison of respondents according to the frequency of use of the social networks by gender, these data are not statistically significant.

Respondents have various education. Students (38.1%) were predominant, followed by respondents with finished secondary education (30.5%) and university degree (20.1%).

Regarding the place of residence, the majority of respondents have a place of residence in the city (87.6%), while in rural areas there are significantly fewer respondents (12.4%).

3. Results and discussion

Most of the respondents are active in two to five social networks (54.9%), while 5.4% of the respondents are active in more than five social networks. This result does not differ from general population data which show that most of the users of social networks use a larger number of social networks, indicating greater opportunities for abuse of users' privacy. Respondents who use social networks exhibit a different interest in certain social networks. The largest percentage of respondents use Facebook (23.3%), Youtube (19.8%), Skype (16%), Gmail – Google Talk (9.8%). Only 0.7% of respondents use MySpace.

When answering the question of whether they read the privacy policy on social networks, the majority of respondents answered with "Sometimes" (50.8%) or that they do not read the privacy rules at all (26.3%), which shows that this type of primary preventive protection respondents insufficiently apply. Only 21.2% of all the respondents answered that they always read the privacy policy on any social network.

The inability to indicate personal data on a Facebook profile was also seen when answering the question of whether the profile contains data on the age of the respondent. The vast majority of respondents answered that their social networks' profile show their real age (60.9%) and that this personal information exists on some of their profiles (10.0%).

The research showed that most of the respondents share within the social network pictures/videos on which they are with their friends (59.6%) or where they are alone (25.0%). Only 13.6% of respondents said that they do not upload photos or videos to social networks. This indicates that the respondents did not develop the system of self-protection of private and personal data.

Unlike in answering the previous question when respondents showed unwillingness to protect their personal data, 65.5% of respondents said that they have never shared a photo or a video of any other person without their consent.

As the reason for rarely uploading the photos and videos on social networks, most respondents (89.7%) perceived the belief that both photos and videos could easily become the subject of misuse. Much less respondents (9.0%) believe that no such misuse has been ever possible. This finding shows that respondents are largely aware of the increased risk of abuse of privacy if photos or videos are shared and stored on the social network they use.

Respondents were asked how the photos or videos shared on social network could be used for the wrong purpose. As possible types of abuse, respondents stated: identity theft and fraud; manipulating personal data; use of the photograph for the purpose of sexual exploitation, pornography and pedophilia; sexual harassment; blackmail, stalking, mocking, etc.

Even though most of the respondents were not victims of violence on social networks, they stated in their responses what, according to their opinion, can be the cause of any kind of violence in cyber community such as a social network. The cause of potential violence or violation of certain right could be: a psychological problem or frustration (135 respondents or 22.1%), courage in the virtual world because of the anonymity (50 or 8.2%), boredom or fun (37 or 6%), too much openness in communication between people who do not know each other in the real world (11 or 1.8%), absence of sanctions (5 or 0.8%), access to personal and private data (5 or 0.8%).

When asked "Do you feel safe/secure when using a social network?" most of the respondents answered that they: feel absolutely safe when using social networks (116 or 17.3%); feel safe because they have never had any inconvenience on social networks (192 or 28.6%); feel safe because they always managed to solve the problem when it happens (61 or 9.1%); mostly feel safe because they had bad experiences from which they learned to be careful (22 or 3.3%). Some respondents are very cautious when using social networks and they say they never feel safe because "the danger is always present" (92 or 13.7%).

The respondents noted that users were exposed to various threats when using social networks. The most commonly mentioned were: photography misuse (362 or 17.0%); hate speech (342 or 16.1%); threatening (305 or 14.3%); different kind of harassment (280 or 13.2%); unauthorized use of photos (278 or 13.1%); sexual harassment in chats, chat rooms or email communication (196 or 9.2%); unwanted sexual content (195 or 9.2%); stalking and forced/unwanted communication in the cyberspace (169 or 7.9%).

The respondents, in general, take care about the information they are publishing, which can be seen from the answer to the question "Have you ever published something that you were later ashamed of?". Most of the respondents (405 or 66.2%) answered that they did not, and only 23.4% responded that they published something that they were later embarrassed about.

The cautions/unreliability of the respondents when using social networks and the accuracy inaccuracy of the data they publish on social networks can be seen through the following questions:

- 114 or 18.6% made their users' profile public while 437 respondents (71.4%) did not;
- 505 (82.5%) did not write their home address on their social networks' profile and only 6.7% did;
- 398 (65%) did block a person on social networks so far;
- 232 (37.9%) deleted or disabled their profile on the social network at least once so far;

- 116 (19%) have given incorrect data about their age when it comes to communication on social networks;
- 206 (33.7%) never added an unknown person to the list of contacts/friends so far, 197 (32.2%) made it 1-5 times, 152 (24.8%) did it more than 5 times, 30 (4.9%) always add an unknown person to the contact list;
- as many as 372 (60.8%) gave information on the name and surname to unknown people, showing that the respondents are fairly sincere in communicating with sharing their data;
- 284 (46.4%) through social networks gave information to unknown people about where they work or study;
- 462 (75.5%) never gave the information about where usually go out with friends to unknown people;
- 380 (62.1%) have never sent personal photos and photos of close friends to unknown people via social network, while 188 (30.7%) always do so;
- 417 (68.1%) never sent an e-mail address to an unknown person via social networks, while 25.2% always do so;
- 546 (89.2%) never gave an information about home address and 486 (79.4%) never gave information about a phone number to unknown person via social network.

About privacy protection, the majority of respondents stated that the privacy settings were "effective, but insufficient" (221 or 36.1%) and "not effective enough to protect users" (175 or 28.6%). A smaller number of respondents (111 or 18.1%) know that privacy settings exist, but have never read it, while 38 respondents (6.2%) do not know that these rules even exist. Only 56 respondents (9.2%) stated that the rules on the protection of privacy on social networks were completely effective.

The respondents also commented about the possibilities of reporting abuse or harassment on the social network, using the report abuse buttons. The majority of respondents knows that there are rules for reporting violence or harassment on the social network, but never read them (195 or 31.9%), a slightly lower number think that these rules are not effective enough to protect users (143 or 23.4%) or that they are efficient, but insufficient (137 or 22.4%). Only 33 respondents (5.4%) evaluated the rules on reporting violence or harassment on the social network as completely efficient, while 91 (14.9%) did not know that there was a possibility of reporting violence or harassment on the social network.

Regarding the efficiency of legal protection of privacy on the Internet and on social networks in Serbia, a small number of respondents believe that they are protected by the existing legal provisions (40 or 6.5%). Most of the respondents (211 or 34.5%) think that the legislation is not completely satisfactory, cannot protect the users and that it must be changed (117 or 19.1%) or that the legislation is not bad, but do not fully protect the users (90 or 14.7%). Even 141 (23%) of respondents do not know that there are legal possibilities for privacy protection, which shows that the users of social networks must be more familiar with the legal provisions in this area.

The respondents suggested different recommendations for increasing the level of safety on social networks: introduction of appropriate relevant legislation, combined with greater activity of state authorities; reporting abuses and punishing perpetrators; education of users in order to increase their level of awareness for their own personal data; suggesting to the users to share and publish the less personal data possible; to organize education of children about the dangers that exist on social networks; to improve the policy of protecting children from all types of violence in cyberspace and on social networks; to teach social network users to protect themselves from the attacks they are exposed to; to organize and to conduct the education of

parents/legal guardians, teachers/professors in order to make them capable to detect the phenomenon of cyber violence among children/pupils/students; to prohibit access to certain websites; to establish centers that would legally and practically handle harassment, insulting and stalking in cyberspace and on social networks; to restrict the use of the Internet for persons younger than 14 years, etc.

The respondents, also as the recommendation, mentioned that the social network users must protect themselves by denying the communication with persons they don't know in real life, as well as better checking the identity of the persons whose user profile they are communicating with.

4. Conclusion

The emergence of the Internet, as an interpersonal medium and the projection of society into a virtual space, was created as the consequence of social transformation, mobility and basic social need of people to interact and to share information. By using the Internet, new connections can be established between people, the old ones can be renewed, values and norms can be spread, a new culture created, money earned, but it could also be manipulated, abused, stolen and cheated.

Nowadays, social networks are the way of connecting people around the globe. In addition to the advantages that the Internet and social networks provide, there has been an increase in abuse related to virtual space. A large number of users are exposed to daily victimization if the data transmitted through social networks are abused or misused. In connection with cyber abuse, the issue of protecting individual personal rights – the right to privacy – was raised. Certain groups of people are particularly exposed to cyber abuse of privacy, for example celebrities, those who are most commonly used by certain social services and whose behavior is deviant or criminal.

Most of the increasingly frequent global privacy attacks have the goal the abuse/misuse of the personal and private information about an individual. Based on this information, it is possible to identify an individual, persons' personal life, group affiliation, everyday activities and behavior – it is possible to reconstitute the life and personality of each subject based on the collected data. The privacy on the Internet includes the right to personal information relating to the storage, use and displaying the personal information over the Internet, as well as the identification information relating to the visitor of a particular website.

Confidentiality of information shared by users in virtual space must not be compromised, and the users must in each particular case be sure of the sender's identity and that the information received must be identical to the sent information. Any departure from this rule diminishes the trust of users and may violate their right to privacy.

The principle of controlled disclosure of personal information is the best way to protect the privacy of all Internet users. Users who want to protect their privacy even more, can try to achieve Internet anonymity – this way, it is possible to use the Internet without giving the possibility of a third party to connect with the Internet activities, in order to personally reveal the identity of a certain Internet user. Publishing "posts" and personal information on the Internet can be detrimental to the privacy of an individual, because the information that are published on the Internet (blogs, images and web pages) is permanent. The fact is that most of the acts of computer crime are committed because of ignorance or insufficient knowledge of the social networks' users about the computer systems. Some of the most common causes of abuse might be poorly programmed computers and computer systems, set of codes that are easy to detect and with low level of security protection, as well as the lack of collective awareness of how effectively all computer and communication systems are vulnerable and likely to collapse. In order to overcome

this segment of the problem, education of Internet users should be done at different levels (schools, Internet providers, media, manufacturers and distributors of computer equipment and programs, etc.), because most of the users make mistakes that often lead to the acts of computer crime.

In order to reduce the number of abuse and misuse of computer systems which endanger the privacy rights of their users, it is necessary to create appropriate legal mechanisms consisting of a legislative for detecting, preventing and sanctioning these socially unacceptable criminal behavior. Also, it is very important to report all criminal offenses related to computer crime to the competent authorities, in order to reduce the "dark figure" of the criminality rate and to achieve better preventive action that would lead to recognition and monitoring of such acts, as well as overcoming the problem of non-reporting of these crimes.

Acknowledgements

At this point, I would like to thank all those people who contributed to the implementation of this research, because without their contribution it could not have been completed.

Conflicts of interest: none.

References

Bangeman, E. (2010). *2010. Report: Facebook caught sharing secret data with advisers*. Retrieved 4 October 2017, from http://arstechnica.com/tech-policy/2010/05/latest-facebook-blunder-secret-data-sharing-with-advertisers/.

Boban, M. (2012). Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu [Privacy right and right for access to information in modern information society]. *Zbornik radova Pravnog fakulteta u Splitu*, *49*(3), 575-598.

Cannataci, A. J. (1987). *Privacy and data protection law: International development and Maltese perspectives*. Complex series.

Catanese, A. S. et al. (2011). *Crawling Facebook for social network analysis purposes*. Retrieved 14 February 2018, from http://arxiv.org//1105.6307.pdf.

Cybercrime on social networks continues to climb (2013). Retrieved 4 October 2013, from http://www.net-security.org/secworld.php?id=11464.

Drakulić, M. (1996). Osnovi kompjuterskog prava [Foundations of computers' law], Beograd: Društvo operacionih istraživača Jugoslavije – DOPIS.

Duffy, M. (2006). *A dad's encounter with the vortex of Facebook*. Retrieved 23 January 2018, from http://www.time.com/time/magazine/article/0,9171,1174704,00.html.

Gross, R., & Acquisti, A. (2005). *Information revelation and privacy in online social networks*. Proceedings of the 2005 ACM workshop on Privacy in the electronic society, ACM, retrieved 15 February 2018 from http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

Hargittai, E. (2007). Whose space? Differences among users and non-users of social network sites. *Journal of Computer-Mediated Communication*, *13*(1), 276-297.

Jovanović, S. (2014). Privatnost i zaštita podataka na Internetu [Privacy and data protection on Internet]. Tvining projekat EU – zbornik *Veze cyber kriminala sa iregularnom migracijom i trgovinom ljudima*, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd.

King, J., Lampinen, A. & Smolen, A. (2011). Privacy: Is there an app for that? *Symposium on usable privacy and security* (SOUPS), Pittsburgh, PA, USA.

Krasnova, H. et al. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39-63.

Kušić, S. (2010). Online društvene mreže i društveno umrežavanje kod učenika osnovne škole: navike facebook generacije [Online social networks and social networking in primary school students: Habits of Facebook generation]. *Život i škola*, *24*(2), 56.

Nikolić, M. (2014). Praktični aspekti zaštite privatnosti korisnika i bezbednosti elektronskih komunikacionih mreža i usluga u Srbiji [Practical aspects of users' privacy protection and security of electronic communication networks and services in Serbia]. Retrieved 30 July 2017 from http://www.telekomunikacije.rs/arhiva_brojeva/peti_broj/milan_nikolic:_prakticni_aspekti_zastite_privatnosti_korisnika_i_bezbednosti_elektronskih_komunikacionih_mredja_i_usluga_u_srbiji_.305.html#_ftn18.

Poslovni portal "Economy" (2012), from http://www.economy.rs/.

Republički zavod za statistiku Republike Srbije [Statistical Office of the Republic of Serbia] (n.d.) from http://webrzs.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=2.

Shah, M. (2013). Online social networks: Privacy threats and defenses. *Springer*, XVI (2013).

Sigurnosni rizici društvenih mreža [Security risks of social networks] – Hrvatska akademska i istraživačka mreža (2015), from www.cert.hr.

Social networking (2014), from http://www.investopedia.com/terms/s/social-networking.asp.

Spasić, V. (2010). Onlajn bezbednost [Online security]. *Zbornik Pravnog fakulteta u Nišu*. Niš: Pravni fakultet, Centar za publikacije, 56 (2010).

Surco, R. (2015). Pravo na privatnost s posebnim osvrtom na internetsku društvenu mrežu Facebook [Right to privacy with special look at Facebook]. Retrieved 20 October 2017 from www.rijaset.ba/.../05_pravo_na _privatnost.

Šurlan, T. (2015). Međunarodnopravna zaštita prava na privatnost [International legal protection of privacy right]. Retrieved 28 October 2017, from www.spmisao.rs/mp-content/uploads/2014/03-tijana-surlan-pdf.

Top 10 Social Networking Sites (n.d.), from http://news.discovery.com/tech/top-ten-social-networking-sites.html.

Utz, S., & Kramer, C. N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyber psychology: Journal of Psychosocial Research on Cyberspace*, *3*(2), 1.

Vidanović, I. (2006). Rečnik socijalnog rada [Dictionary of social work]. Udruženje stručnih radnika socijalne zaštite Srbije, Društvo socijalnih radnika Srbije, Asocijacija centra za socijalni rad Srbije, Unija Studenata socijalnog rada, Beograd. 437-438.

Viégas, B. F. (2005). Blogger's expectations of privacy and accountability: An initial survey. *Journal of Computer–Mediated Communication*, *10*(3).

Vilić, V. (2013). Possibilities of privacy rights abuses in social networks and practical protective measures ("О возможньх нарушениях права на неприкосновенность частной жизни и социальных сетях и практических мерах защиты"). Интернет, власть и политика" - International scientific and practical conference »Internet – Government - Politics«, Кемерово, 2013. ЗАКАЗ No. 458. 187-192.

Vilić, V., & Radenković, I. (2016). Possibilities of protecting personal data published on social network sites in the light of The law on personal data protection. *Synthesis 2016 - International Scientific Conference on ICT and E-Business Related Research*, Belgrade, Singidunum University, Serbia, 2016, 62-65. doi: 10.15308/Sinteza-2016-62-65

Vilić, V. (2017). CYBERCRIME: Basic criminological characteristics and legislation. LAP - LAMBERT Academic Publishing – International Book Market Service Ltd., member of OmniScriptum Publishing Group. -166. ISBN 978-620-2-01800-5

Westin, A. (1970). *Privacy and freedom*. London: Bodley Head.

Žunić Pavlović, V., Kovačević Lepojević, M., & Mentus, T. (2013). Negativne posledice socijalnog umrežavaja na internet [Negative consequences of social networking on Internet]. *Komunikacija i ljudsko iskustvo* – tematski zbornik radova, Filozofski fakultet Univerziteta u Nišu, 137-150.


C O A S

Center for Open Access in Science ▪ https://www.centerprode.com/ojls.html
Open Journal for Legal Studies, 2018, *1*(1), 25-36.
ISSN (Online) 2620-0619 ▪ https://doi.org/10.32591/coas.ojls.0101.03025r

Ten Years on: The Exhaustion Principle and the Practice of the Constitutional Court of Kosovo as the Final Authority for Protection of Human Rights

Besfort T. Rrecaj

University of Prishtina "Hasan Pristhina", Faculty of Law

Bardh Bokshi

Constitutional Court of Kosovo, Prishtina

Received 12 June 2018 ▪ Revised 10 July 2018 ▪ Accepted 18 July 2018

Abstract

Ten years after the establishment of the Constitutional Court of Kosovo, this paper aims to examine the concept of exhaustion of legal remedies in Kosovo judicial system where an individual has brought a case claiming violation of human rights guaranteed by the Constitution. The paper will focus on analyzing what constitutes an effective legal remedy including ordinary and extraordinary remedies for the purposes of submitting a constitutional complaint with the Constitutional Court. This work is based on the case-law of the Constitutional Court and tries to explain all legal steps that must be observed before submitting a constitutional complaint regarding exhaustion requirement. Furthermore, it will delve deeper into this concept by distinguishing the importance of formal and substantive exhaustion of legal remedies, the interconnectedness of formal and substantive exhaustion of legal remedies and the distinction between them as developed by the case-law of the Constitutional Court. It will conclude by summarizing main characteristics of the concept of exhaustion of legal remedies in Kosovo as it is established by the practice of the Constitutional Court.

Keywords: effective legal remedies, exhaustion of legal remedies, extraordinary legal remedies, formal and substantive exhaustion of legal remedies, the principle of subsidiarity.

1. Introduction

Before delving into the topic of exhaustion of legal remedies for the purposes of submitting a constitutional complaint with the Constitutional Court of Kosovo (hereinafter, the Constitutional Court), it is necessary to provide the constitutional and legal background which lay down that requirement. Article 113.7 of the Constitution of Kosovo (hereinafter, the Constitution) (Kosovo Constitution 2008 and its amendments) establishes that individuals must exhaust all legal remedies to their availability before submitting a complaint with the Constitutional Court. This requirement is further confirmed by Article 47.2 of the Law on Constitutional Court which provides that individuals may submit a referral with the Constitutional Court only after they have exhausted all legal remedies provided for by law (Law on the Constitutional Court of Kosovo). The exhaustion of legal remedies ought to mean remedies that are not only available in formal terms but also effective in providing a redress for an individual raising the complaint. Within this concept

Correspondence: Besfort T. Rrecaj, University of Prishtina "Hasan Prishtina", Agim Ramadani Str. nn. 10000, Prishtina, KOSOVO. e-mail: besfort.rrecaj@uni-pr.edu.

it becomes more a matter of judicial practice to determine which remedy is available and effective rather than just to consider legal remedies provided by law. This standard is established by the European Court of Human Rights (hereinafter, the ECtHR) and applicable in Kosovo. In the following text the requirement of exhaustion of legal remedies will be explained through lenses of judicial practice of the Constitutional Court. Formal and substantive exhaustion of legal remedies will be discussed as well as their meaning which is not so obvious from the wording of Article 113.7 of the Constitution but is rather developed through case-law of the Constitutional Court. Ten years on, it is still building it practice nevertheless, so far it managed to establish some basic principles based on the ECtHR practice in upholding and interpreting basic human rights in Kosovo. The so called balancing test in exhaustion examination was conceived in order to help the Constitutional Court to determine the availability and effectiveness of particular legal remedies. Ultimately this test would determine whether a case will be heard at the Constitutional Court or not when an individual requests direct access to be heard before this court.

2. Establishment of the Constitutional Court, jurisdiction and the individual complaint

The Constitutional Court of Kosovo as the youngest court of such nature in Europe was established after Kosovo declared its independence in 2008. The role of this court was to become a guardian of the Constitutional of Kosovo but it would be set in motion only when requested so by the authorized parties as stipulated in Article 113 of the Constitution of Kosovo. (Constitution of Kosovo) It does not have an ex officio authority to put its machinery in motion. Among authorized parties are individuals claiming concrete violation of human rights guaranteed by the Constitution. This article is applicable to natural as well as legal persons as established duly by the applicable law in Kosovo[1] (Case No. KI41/09, *Applicant, AAB-RIINVEST L.L.C*). The Constitution of Kosovo Chapter VIII and Law on Constitutional Court lay basic foundation and jurisdiction of the Court. In this regard, Article 113.7 of the Constitution authorizes individuals "*…to refer violations by public authorities of their individual rights and freedoms guaranteed by the Constitution…"* (Constitution of Kosovo). Accordingly, the Constitutional Court ought to represent a legal remedy as a final authority for all those individuals who claim violation of human rights by public authorities.

Although Kosovo aims to become part of the Council of Europe, due to political disagreements over the political status, it has not succeeded in realizing this aim so far. This makes Kosovo a self-contained human rights regime with individuals not being able to hear their cases before a larger and important institutional framework such as the ECtHR. However, in order to avoid this deficiency, drafters of the Constitution of Kosovo took care to provide a larger and more comprehensive human rights protection within this self-contained regime by unilaterally obliging itself to respect main international and European human rights conventions and also by making the practice of the ECtHR as the main reference for public authorities in interpretation of human rights guaranteed by the Constitution. The Constitutional Court by virtue of Articles 22 and 53 of the Constitution is under constitutional obligation to apply the European Convention of Human Rights (hereinafter, the ECHR)[2], directly in cases involving human rights and fundamental

[1] The case emphasizes that fundamental rights and freedoms set forth in the Constitution are also valid for legal persons to the extent applicable, and that, they too, must fulfill the requirement to exhaust all legal remedies.

[2] Article 22.2 of the Constitution of Kosovo establishes that the European Convention on Human Rights and its protocols are directly applicable in the legal system of Kosovo and that, in case of conflict; it has priority over provisions of laws and other acts of public institutions.

freedoms and to interpret them consistent with the court decisions of the ECtHR[3]. For these reasons the case-law of the Constitutional Court is replete with references to the case law of the ECtHR with regard to application of the standards and safeguards of fundamental human rights and freedoms. The practice of the ECtHR was main determinant in building up the practice of the Constitutional Court and in this regards it is also reflected in the application of the requirement for exhaustion of legal remedies.

The individual complaints submitted with the Constitutional Court form the so-called subsidiary jurisdiction[4]. This principle is intrinsic of the ECtHR jurisdiction and thus the role of the Constitutional Court is subsidiary to the regular judiciary and other public authorities in Kosovo. The idea behind exhaustion principle lies on assumption that the regular juridical system of the state would provide effective legal remedies to uphold constitutional rights.[5] Within this authority, the Constitutional Court can generally review individual decisions and acts of the regular judiciary and of other public authorities only as to the observance of human rights guaranteed by the constitution.

3. Formal and substantive exhaustion of legal remedies and the burden of proof

The question of exhaustion of legal remedies is not as straightforward as it may initially appear because there are several factors that must be taken into account. These factors invariably include the availability and effectiveness of a legal remedy because only legal remedies that are available and effective must be exhausted. Furthermore this concept requires that legal remedies are exhausted in the formal as well as in substantive terms. The formal term of exhaustion of legal remedies requires that the prospective applicants before submitting a constitutional complaint with the Constitutional Court, must follow, a step by step procedure in all instances of the regular courts in Kosovo composed of the Basic Court, the Court of Appeals and the Supreme Court. The Supreme Court deals mainly with extraordinary legal remedies which have their own peculiarities but will be dealt duly as the process of exhaustion is explained[6] (Code of Criminal Procedure of Kosovo No. 04/L-123, Article 435.1).

In this regards, The Constitutional Court adopted the stance of the European Court that exhaustion of legal remedies must be applied with some degree of flexibility and without excessive formalism.[7] The burden of proof lies with the applicant bringing the claim with the

[3] Article 53 of the Constitution of Kosovo establishes that human rights and fundamental freedoms guaranteed the Constitution of Kosovo must be interpreted consistent with the case-law of the European Court of Human Rights.

[4] It is said subsidiary jurisdiction as opposed to the original jurisdiction of the Constitutional Court as established in paragraphs 2, 3, 4, 5, 6, 8 and 9 of Article 113 of the Constitution of Kosovo. The authorized actors which can engage the original jurisdiction of the Constitutional Court are the Assembly of Kosovo, the President of Kosovo, the Government, the Ombudsperson, the municipalities of Kosovo and the regular judiciary in a so-called incidental control procedure whereby the regular courts have the right to refer question of compatibility of a law with the Constitution when it is raised during the course of regular judicial proceeding.

[5] See *mutatis mutandis* cases KI 41/09, Applicant *AAB-Riinvest University L.L.C.* Prishtina, Constitutional Court Resolution on Inadmissibility of 21 January 2010 and ECtHR case *Selmouni vs. France*, No. 25803/94, ECtHR, judgment of 28 July 1999.

[6] Article 435.1 of the Code, stipulates that a request for protection of legality shall be considered by the Supreme Court of Kosovo in a session of the panel. Article 436.1 of the same Code stipulates that when deciding on a request for protection of legality the Supreme Court of Kosovo shall confine itself to examining those violations of law which the requesting party alleges in his or her request.

[7] In comparison to practice of the ECtHR on the burden of proof see Judgment on the Merits delivered by a Chamber, *Dalia v. France*, No. 26102/95, 19 February 1998. See also Practical Guide on Admissibility

Constitutional Court to prove that there is no other available and/or effective legal remedy. On the other side, the respondent party, in this case the public authority accused of human rights violation, may give its arguments against the applicant's arguments and prove that actually there is an available and effective legal remedy and that the claim ought to be declared inadmissible due to non-exhaustion criterion. After the exhaustion proof is provided the Constitutional Court reserves for itself the right to conclude whether available legal remedies were effective for that particular case[8].

The Constitutional Court, as a matter of practice, exercises a so-called "balancing test" whereby it requires from the parties to produce evidence pertinent to the exhaustion requirement. In the case No. KI 116/14, the Constitutional Court declared the constitutional referral inadmissible on the grounds of non-exhaustion of all legal remedies because the applicant had failed to make use of the appropriate legal remedy to his availability (Case No. KI116/14, *Applicant Fadil Selmanaj*). In this case, the Constitutional Court laid down criteria of general nature which would absolve the applicants from exhausting all legal remedies to their avail. The Constitutional Court considered that in order for the applicant to be absolved from the requirement to exhaust all legal remedies it is incumbent on him to show that: (1) the legal remedy was in fact used; (2) the legal remedy was inadequate and ineffective in relation to his case; and (3) there existed special circumstances absolving the applicant from the requirement to exhaust all legal remedies (*Ibid.*). The Constitutional Court found that the applicant did not meet any of the above-stated criteria in order to be absolved of the requirement to exhaust all legal remedies. Moreover on this point, the Constitutional Court stressed that the applicant in failing to proceed further with the appropriate legal remedy as prescribed by the applicable law in Kosovo is liable to have his case declared inadmissible, as it shall be understood as a waiver of the right to further proceedings on objecting the violation of constitutional rights (*Ibid.*).

Similarly, in another case No. KI 39/12 the Constitutional Court placed the burden of proof on the applicant by holding that he must prove why he has not exhausted the legal remedies, and show that the legal remedies available to him under Kosovo law were insufficient or unfruitful, or that there were special circumstances which exempted him from the obligation to exhaust such remedies., The Constitutional Court concluded by adding that the applicant's mere doubt does not exempt him from the obligation to exhaust the legal remedies (Case No. KI39/12, *Applicant Tomë Krasniqi,* paragrhaps 23-24 and 40-44).

In an individual but high profile case No. KI 34/17 (Case No. KI34/17, *Applicant Valdete Daka)*, involving a complaint against the election of the President of the Supreme Court, the Court asked the applicant and the respondent in this case the Kosovo Judicial Council[9] to set forth their arguments as to why the applicant should pursue the regular course of exhaustion of

Criteria, Council of Europe/European Court of Human Rights, 2014 on exhaustion requirement. http://www.echr.coe.int/Documents/Admissibility_guide_ENG.pdf (referenced on 9 February 2018).

[8] See *mutatis mutandis* cases KI 116/14 *Applicant Fadil Selmanaj,* Resolution on Inadmissibility of the Constitutional Court of Kosovo of 26 January 2015; KI 39/12, *Applicant Tomë Krasniqi,* Resolution on Inadmissibility of the Constitutional Court of Kosovo, of 24 July 2012 and KI 56/09 *Fadil Hoxha and 59 Others vs. the Municipal Assembly of Prizren,* Judgment of the Constitutional Court of Kosovo, of 22 December 2010. In comparison to practice of the ECtHR on special circumstances availing the obligation to exhaust legal remedies see Judgment on the Merits by the Grand Chamber, *Sejdovic v. Italy*, No. 56581, 1 March 2006; on cases when there is repetition of acts by authorities contrary to the Convention see Judgment on Merits by a Chamber, *Aksoy vs. Turkey*, No. 21987/93, 18 December 1996; on cases when the use of legal remedy would be unreasonable in practice hindering proper right to use a remedy, see ECtHR, Judgment on the Merits by a Chamber, *Veriter v. France*, No. 31508/07, 14 October 2010.

[9] The Kosovo Judicial Council is responsible for recruiting and proposing candidates for appointment and reappointment to judicial office. The Kosovo Judicial Council is also responsible for transfer and disciplinary proceedings of judges, Article 108.3 of the Constitution of Kosovo.

remedies, instead of granting her direct access to the Constitutional Court, and have the case heard in merits (*Ibid.*, paragraphs 7-20). The applicant, argued that in her case there were no legal remedies that are practical and effective that would provide for a swift resolution of her case in accordance to its nature and specificities (*Ibid.*, paragraph 42). The respondent, on the other hand, argued that the applicant must be required to pursue the regular course of exhaustion of legal remedies in accordance with the applicable provisions of the law on administrative procedure. Ultimately, the respondent required the Court to declare the applicant's complaint as inadmissible on the grounds of her not having exhausted all legal remedies in accordance with the law (*Ibid.*, paragraph 45). The Court then, exercised the "balancing test" based on two premises: (1) whether the legal remedies available to the applicant were accessible and offered reasonable prospects of success; and (2) whether the nature and the specificity of the applicant's complaint warranted the necessity of having her case resolved in a "timely-fashion" (*Ibid.*, paragraph 74). The Court, relying on its previous case-law as well as that of the European Court, found that the applicant must be granted direct access to the Court because the legal remedies available to the applicant do not offer her reasonable prospects of success, the nature and the specificity of the case warranted that that case must be resolved in a "timely-fashion" (Case No. KI99/14 and No. KI100/14, joint decision, *Applicants Shyqyri Syla and Laura Pula*). The Court also noted that, the respondent merely mentioned that the applicant should pursue the regular course of exhaustion of legal remedies, however, they failed to back-up that assertion with relevant case-law in comparable cases (Case No. KI34/17, *Applicant Valdete Daka*, paragraph 70).

In the case KI 56/09 (Case No. KI56/09, *Fadil Hoxha and 59 Others vs. the Municipal Assembly of Prizren*), the applicants challenged a decision of the Municipal Assembly of Prizren alleging that the aim of the challenged act is to construct high tower blocks instead of an existing green environment which was foreseen by urban planning (*Ibid.*, paragrahps 3 & 9). After examining the case, the Constitutional Court noted that the applicants never received any reply from the Municipal Assembly of Prizren pertinent to their right guaranteed by Article 52 (2)[10] of the Constitution which establishes that public institutions must take into consideration the opinion of the public on matters that impact the environment on which they live (*Ibid.*, paragrahps 27, 60 & 67). The Constitutional Court then continued to explain that the applicable law in Kosovo did not provide a legal remedy which would enable the applicants to challenge that act before the regular courts with regard to the right guaranteed by Article 52 (2) of the Constitution[11]. Taking into account the impossibility of the applicants to seek redress before the regular courts, their complaint was declared admissible[12] (*Ibid.*).

Similarly in another case, KI 06/10 (Case No. KI06/10, *Valon Bislimi v. Ministry of Interior et al*), the Constitutional Court, finding that the applicant had no access to an effective legal remedy, allowed access to it without exhausting legal remedies. In this case, the applicant complained that his right to freedom of movement was violated because authorities of Kosovo were refusing to issue him a passport due to a criminal conviction. The applicant proved that his

[10] Article 52 (2) of the Constitution of Kosovo establishes that everyone should be provided an opportunity to be heard by public institutions and have their opinions considered on issues that impact the environment in which they live.

[11] Id, The Constitutional Court of Kosovo, inter alia, reasoned that the Applicants had addressed the Ombudsperson, the Constitutional Court itself and the Ministry of Environment and Spatial Planning in order to seek redress. The Constitutional Court went on to explain the Law on Administrative Dispute that was applicable in Kosovo appeared not to allow for a judicial complaint unless there has been a direct violation of an individual's right or legal interest.

[12] The Constitutional Court of Kosovo, found that it is clear that the Decision of 30 April 2009 is not an individual decision; and as such, the Applicants did not have at their disposal a judicial complaint before Supreme Court to challenge the Decision of 30 April 2009 with regard to the right guaranteed by Article 52 of the Constitution. The Law on Administrative Disputes provided no remedy to the Applicants.

constitutional rights were violated by the *inaction* caused by *administrative silence* by the Ministry of Interior, he had no possibility to challenge that inaction before the regular courts (*Ibid.,* paragraphs 59-61). Therefore, the Constitutional Court accepted his complaint as admissible, reasoning that the applicant had no access to due and possible effective legal remedies (*Ibid.,* paragraphs 87-99).

Besides formal exhaustion requirements, the substantive exhaustion of legal remedies from the prospective applicants requires that the claim is raised at least in substance concerning the question of constitutionality of a public act with the regular courts. The regular courts of Kosovo have jurisdiction to decide over constitutional claims among points of law and fact when deciding a case (Constitution of Kosovo, Art. 102.3). Thus individuals must invoke their rights guaranteed by the Constitution of Kosovo early in the process or else they risk having their complaints declared inadmissible by the Constitutional Court on the grounds of substantive non-exhaustion. In the case No. KI118/15, (Case No. KI118/15. *Applicant Dragiša Stojković*) the applicant of Serbian ethnicity complained, *inter alia*, that the challenged judgment of the Supreme Court violated his right to use of language and to fair and impartial trial, because of an erroneous determination of facts and due to incorrect translation of his statement. The Constitutional Court noted that the applicant, in the course of regular proceedings, has neither raised concretely nor substantially the alleged violation of his right to use Serbian language in the regular proceedings; nor has he explained why he has not invoked in the regular courts his right guaranteed by Article 5 [Languages] of the Constitution in the terms he has presented before the Constitutional Court (*Ibid.*, paragraph 31). The Constitutional Court further emphasized that the applicant should have presented that allegation in his appeal before the regular courts, as he was not only entitled but also obliged to do so in accordance with the principle of subsidiarity. The Constitutional Court declared the complaint inadmissible due to non-exhaustion of all legal remedies as established by Article 113 (7) of the Constitution of Kosovo. The Constitutional Court backed up its conclusion by relying in the well-established case law of the European Court, as well as its own case law in similar matters (*Ibid.*, paragraphs 33-38).

In the above-stated cases, the Constitutional Court showed that it has established a judicial practice pursuant to the principles of the ECtHR on the flexibility of declaring admissible constitutional complaints submitted by individuals where it ascertains that the legal system of Kosovo has not provided them with remedies that are effective and available. The burden of proof falls with the applicant to document that in that particular individual case there are no available and effective legal remedies, while the respondent has the right to claim the opposite. It is in the discretionary power of the Constitutional Court to evaluate evidence provided and come to a conclusion on exhaustion of legal remedies for each particular case. In this respect, the Constitutional Court in its developing case law has consistently maintained that regular judiciary and other public authorities must be given the opportunity to prevent or put right the alleged violation of the Constitution. This approach is based on the assumption that the legal order of Kosovo will provide an effective remedy for the violation of constitutional rights because this is an important aspect of the subsidiary character of the Constitution (Case No. KI41/09, *Applicant AAB-RIINVEST University L.L.C.*, Prishtina).

The situation may become more complicated where state judiciary represent systemic deficiencies that may be characteristic of states in transition such as Kosovo. In Kosovo, according to statistics available the efficiency of the judiciary is seriously hampered by the shortcomings of criminal legislation; many provisions in the Criminal Procedure Code are too cumbersome and formalistic to permit robust and successful investigation and prosecution. Due to insufficient capacity and staffing and limited financial resources, as well as a heavy backlog of cases, the judicial system is slow in delivering justice (European Commission 2016 Kosovo Progress Report). This raises the awareness of the Constitutional Court when deciding whether legal remedy is available and effective.

4. Extraordinary legal remedies and the principle of exhaustion

As a matter of principle and practice, the so-called extraordinary remedies do not have to be exhausted and the prospective applicants must submit a constitutional complaint with the Constitutional Court within 4 month legal deadline (Constitution of Kosovo, article 49), which starts to run from the day a final decision is issued in regular appeal proceedings. This stance is in line with the stance of the ECtHR which tents to focus on their availability and effectiveness rather than the formal status of the remedy[13]. There are certain extraordinary remedies that are provided for by the law in civil, criminal and administrative proceedings such as the request for reopening of proceedings, request for extraordinary mitigation of punishment in criminal proceedings or the request for protection of legality in civil proceedings which must not be exhausted (*Practical Guide on Admissibility Criteria* on exhaustion requirement). Those extraordinary remedies are not considered effective by the Constitutional Court because they are not directly accessible to the prospective applicants but depend on the exercise of the discretion by an intermediary such as the state prosecutor[14]. However, for the purposes of a constitutional complaint, if a prospective applicant has made use of such extraordinary remedies, and if that request is accepted by the state prosecutor and is consequently submitted with a regular court on behalf of the applicant the applicant must wait until there is a decision of a regular court pertinent to his or her case. In that situation, the applicant must not simultaneously submit a constitutional complaint with the Constitutional Court because that constitutional complaint shall be deemed premature on the grounds of the principle of subsidiarity (Case No. KI102/16, *Applicant Shefqet Berisha*).

It must be noted that, there are also certain so-called extraordinary remedies such as the request for "revision" in civil proceedings, the request for "protection of legality" in criminal proceedings and the 'reviewing' in administrative proceedings, which, must be exhausted by the prospective applicants[15] (Case No. KI135/14, *Applicant IKK Classic*). One must look beyond the appearances and the naming of such remedies and take stock of their specificities, effectiveness and the realities into which they operate before determining whether a prospective applicant must be required to exhaust them or not[16] (Criminal Procedure Code). These extraordinary remedies are very similar to an appeal in regular proceedings because: (1) their use depends the discretion of the prospective applicant, and as such, are not depended upon discretion of an intermediary; (2) they are generally used to raise points of law and exceptionally questions of fact as well; (3) the legal deadline to submit them before the regular courts is no longer than two to three months; and, (4) they have proved to be effective remedies, especially, the request for "revision" in civil proceedings, and the request for "protection of legality" in criminal proceedings[17]. Another reason to encourage the prospective applicants to exhaust the so-called extraordinary remedies, which are similar to an appeal in regular proceedings, is that there is a real possibility that they may overlook the regular courts (for example, the Supreme Court) and opt to submit a constitutional

[13] In comparison to ECtHR practice see Judgment on Merits by a Chamber, *Tum Haber Sen and Cinar v. Turkey*, No. 28602/95, 21 February 2006. See also *Practical Guide on Admissibility Criteria* on exhaustion requirement.

[14] See Law on Contested Procedure No. 03/L-006, Article 245.1, which stipulates that against a final ruling, the public prosecutor might raise the request for legal protection within three months.

[15] See for example, Judgment of the Supreme Court of Kosovo (E. Rev. No. 21/2014, 8 April 2014). However, that judgment was later declared invalid by the Constitutional Court of Kosovo due to deficient reasoning.

[16] Criminal Procedure Code stipulates that a party may request protection of legality within three (3) months of the final judgment or final ruling. The party must file the request with the Basic Court where the final judgment was issued, which shall transmit all validated requests to the Supreme Court.

[17] See conversely, the European Court of Human Rights: Case of *Tanase v.Moldova*, application No. 7/08, Judgment of 27 April 2010, at paragraph 122 and see *mutatis mutandis* Decision as to the Admissibility of application No. 32567/06 by Anne Williams against the United Kingdom.

complaint with the Constitutional Court instead. However, in reality the Constitutional Court can only review regular proceedings only from the point of view of observance of the constitutional procedure and potential violation of fundamental human rights and freedoms whereas a regular court can review their complaints on the points of law, which is something that the Constitutional Court, in principle, cannot do (Cases No. KI37/17 and No. KI52/17, *Applicants Tihomir Mikarić, Olga Janičijević and Shemsije Sheholli*, joint decision, paragraphs 56-57). In addition, a regular court, must also respect the Constitution because that is the obligation and duty imposed by the Constitution on the regular courts and the Constitutional Court as well (*Ibid*., also Case No. KI135/14, *Applicant IKK Classic,* paragraph 48).

In a case No. KI159/15 (*Applicant Sabri Ferati*), where the Constitutional Court was petitioned by an applicant to review decisions of regular courts with respect to his request for reopening of criminal proceedings, the Constitutional Court noted that there were two sets of proceedings in that case (*Ibid*., paragraph 26). One set of proceedings, the Constitutional Court remarked, was finalized when the applicant was found guilty for having committed the criminal offence of endangering public traffic sanctioned under article 378 of the Criminal Code of Kosovo (*Ibid*., paragraph 28). The Constitutional Court noted that those proceedings were the main proceedings because they had determined the applicant's criminal responsibility; however, for the purposes of a constitutional complaint, those proceedings were submitted out of time (*Ibid*., paragraph 30). As far as the second set of proceedings is concerned, with respect to the applicant's request for reopening of criminal proceedings, the Constitutional Court held that the right to a fair and impartial trial is not applicable to those proceedings; and as such, that complaint must be rejected as incompatible *ratione materiae* with the Constitution because it does not determine the criminal responsibility of the applicant (*Ibid*., paragraph 37). One must bear in mind, however, that if a request for reopening of proceedings in criminal or civil law is accepted by the regular courts, then the right to a fair trial as guaranteed by article 31 of the Constitution and article 6 of the ECHR can be applicable (ECtHR Case of *Sapeyan v. Armenia*, paragraph 24). Thus, there are general principles, which determine whether a certain remedy must be exhausted or not but the context and the circumstances of a case may determine, in the interest of justice, that the Constitutional Court be flexible and adapt and apply general principles to the case under review.

5. Conclusion

Ten years on, the Constitutional Court of Kosovo is pursuing its practice based on the well-established practice of the ECtHR. The legal system of Kosovo made human rights as provided by the ECHR obligatory and superior in their applicability to laws and other acts of public institutions of Kosovo. Furthermore the Constitution of Kosovo made the ECtHR practice as the main reference in interpreting human rights guaranteed by the same Constitution. The Constitutional Court works on the basis of subsidiarity principle. Individuals claiming violation of constitutional rights ought to exhaust legal remedies which are available and effective. Legal remedies must be exhausted not only in formal step-by-step procedure from the first to the last instance of the regular judiciary but they must be exhausted in substance as well. It gives the ordinary judiciary and other public authorities, the opportunity to redress the potential violations of the constitutional rights in individual cases. The rights and freedoms guaranteed by the Constitution and the ECHR must be invoked from the first until the last instance of regular proceedings, and in some cases, like for example in criminal proceedings those rights must be invoked as early as the pre-trial stage.

In its practice the court has established the so called 'balancing test' through which it determines the exhaustion requirement and brings a final decision whether to grant the applicant access to the court when not exhausting legal remedies. The balancing test requires that (1) the legal remedy was in fact used; (2) the legal remedy was inadequate and ineffective in relation to

his case; and (3) there existed special circumstances absolving the applicant from the requirement to exhaust all legal remedies. The burden of proof lies with the applicant to prove its case of non-exhaustion while the respondent party may advance its arguments against the applicant by proving that in fact there was a legal remedy that is available and effective.

The so-called extraordinary remedies can address questions of law and of constitutionality and sometimes even of facts. Extraordinary legal remedies may not be exhausted nevertheless some extraordinary legal remedies because of their authority may fall within the concept of an available and effective legal remedy. A good example for exhaustion of the extra-ordinary remedies would be the request for revision in civil proceedings or the request for protection of legality in criminal proceedings because: (1) they are not dependent on an intermediary actor (like the state prosecutor for example); (2) they actually are under the discretion of the prospective applicants; (3) through them the prospective applicants may address their grievances more thoroughly because they can, and in fact must, raise questions of constitutionality, questions of legality and exceptionally even questions of fact; and (4) and they are not subject to uncertain time-limit which would render them ineffective[18].

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The authors declare no competing interests.

Authors

Mr. Bardh Bokshi works as a Senior Legal Adviser at the Constitutional Court of Kosovo since March 2010, and has finished basic studies (obtained title "Graduated Lawyer" after graduation in an eight semester program) and obtained a master's degree (civil law) in the University of Prishtina-Faculty of Law. Mr. Bokshi has also successfully passed the bar exam organized by the Ministry of Justice of Kosovo, in addition to serving as a lawyer for five months (January-June 2015) for the Albanian Division at the European Court of Human Rights, within the framework of a joint program of the Swiss Embassy in Prishtina, Council of Europe and the Constitutional Court of Kosovo.

Mr. Besfort T. Rrecaj works as Professor of Law, International Law Department at the University of Prishtina "Hasan Prishtina" where he teaches Human Rights, Public International Law and International Organizations. Among other senior positions in public and private sector Mr. Rrecaj has experience with the Constitutional Work in a position of Senior Legal Adviser. His recent work include book chapter titled "Sovereignty vs. R2P: Controlling Hard Law with Soft Law: Not a Great Idea," in Stehphanie Fenkart, Heinz Gartner and Hannes Swoboda ed. *Gerechte Intervention? Swischen Gewaltverbot und Schutzverantwortung* (Wien, LIT 2017), A Relationship in Limbo: Challenges, Dynamics and Perspective of Kosovo's Integration in NATO, *Croatia International Relations Review, XXII (80) 2017*, 211-232. For more see http://juridiku.uni-pr.edu/Dekanati/Prodekan-per-qeshtje-mesimore.aspx.

[18] Request for protection of legality must be filed within 3 months of final ruling against which the protection of legality is sought, Article 418.3 of the Code of Criminal Procedure No. 04/L-123. A party may file revision against the ruling of the court of second instance within a time-limit of thirty days.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The authors declare no competing interests.

References

Case No. KI06/10, *Valon Bislimi v. Ministry of Interior et al,* Judgment of the Constitutional Court of Kosovo, of 1 November 2010.

Case No. KI102/16 *Applicant Shefqet Berisha,* Resolution on Inadmissibility of the Constitutional Court of Kosovo, of 3 March 2017.

Case No. KI116/14, *Applicant Fadil Selmanaj,* Resolution on Inadmissibility of the Constitutional Court of Kosovo, of 26 January 2015.

Case No. KI118/15 *Applicant Dragiša Stojković*, Resolution on Inadmissibility of the Constitutional Court of Kosovo, of 27 May 2016.

Case No. KI135/14, *Applicant IKK Classic,* Judgment of the Constitutional Court of Kosovo, of 9 February 2016.

Case No. KI159/15, *Applicant Sabri Ferati,* Resolution on the Inadmissibility of the Constitutional Court of Kosovo, of 14 June 2016.

Case No. KI34/17, *Applicant Valdete Daka,* Judgment of the Constitutional Court of the Kosovo, of 12 June 2017.

Case No. KI39/12, *Applicant Tomë Krasniqi,* Resolution on Inadmissibility of Constitutional Court of Kosovo, of 24 July 2012.

Case No. KI41/09 *Applicant AAB-RIINVEST L.L.C.,* Resolution on Inadmissibility of the Constitutional Court of Kosovo, of 3 February 2010.

Cases Nos. KI37/17 and KI52/17, *Applicants Tihomir Mikarić Olga Janičijević and Shemsije Sheholli,* Joint Resolution on Inadmissibility of the Constitutional Court of Kosovo, of 1 November 2017.

Cases No. KI99/14 and KI100/14, *Applicants Shyqyri Syla and Laura Pula,* Joint Judgment of the Constitutional Court of Kosovo, of 8 July 2014.

Code of Criminal Procedure No. 04/L-123.

Constitution of Kosovo (Constitution, K-09042008, Assembly of Kosovo, 9 April 2008, and its amendments, Official Gazette).

ECtHR Case *Aksoy vs. Turkey*, Application no. 21987/93 Judgment on the Merits by a Chamber, 18 December 1996.

ECtHR Case *Dalia v. France*, Application no. 26102/95, Judgment on the Merits delivered by a Chamber, 19 February 1998.

ECtHR Case of *Anne Williams against the United Kingdom,* Application no. 32567/06, ECtHR, Decision as to the Admissibility.

ECtHR Case of Sapeyan v. Armenia, Application no. 35738/03, ECtHR, Judgment of 13 January 2009.

ECtHR Case of *Tanaše v. Moldova*, Application no. 7/08, ECtHR, Judgment of 27 April 2010.

ECtHR Case *Sejdovic v. Italy*, Application no. 56581, Judgment on the Merits by the Grand Chamber, 1 March 2006.

ECtHR Case *Tum Haber Sen and Cinar v. Turkey*, Application no. 28602/95, Judgment on the Merits by a Chamber, 21 February 2006.

ECtHR Case *Veriter v. France*, Application no. 31508/07, Judgment on the Merits by a Chamber, 14 October 2010.

European Commission, 2016 Kosovo Progress Report, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. SWD (2016) 363 final. (European Commission, Brussels, 9 November 2016).

Law on Contested Procedure No. 03/L-006.

Law on the Constitutional Court of Kosovo No. 03/L-121.

Practical Guide on Admissibility Criteria, Council of Europe/European Court of Human Rights, 2014. http://www.echr.coe.int/Documents/Admissibility_guide_ENG.pdf (accessed on 9 February 2018).


C O A S

Center for Open Access in Science ▪ https://www.centerprode.com/ojls.html
Open Journal for Legal Studies, 2018, *1*(1), 37-50.
ISSN (Online) 2620-0619 ▪ https://doi.org/10.32591/coas.ojls.0101.04037d

Guarantee of the Right to Silence and of the Right not to Contribute to One's Own Incrimination in Romanian Law

Carmen Adriana Domocos

University of Oradea, Faculty of Law

Received 29 May 2018 ▪ Revised 29 June 2018 ▪ Accepted 19 July 2018

Abstract

The right to silence enjoys increased attention from the Romanian legislator and is currently regulated by the Criminal Procedure Code (Law no. 135/2010), which entered into force on 1st February 2014. The right to silence (to remain silent) and the right not to contribute to one's own incrimination (the privilege against self-incrimination) are the implicit procedural guarantees of the right to a fair trial, which results from the case law of the European Court of Justice within the meaning of Article 6 paragraph 1 of the European Convention on Human Rights. They are also stipulated in the field of preventive measures. For the first time, the New Code of Criminal Procedure also regulates the witness's right not to incriminate himself. The paper contains also some considerations about the purpose of the privilege of silence within the meaning of the ECHR.

Keywords: the right of silence, the privilege against self-incrimination, procedural guarantees, witness' right not to incriminate himself.

1. Introductory issues regarding the right to silence and to non-self-incrimination

The right to silence (to remain silent) is the implicit procedural guarantee of the right to a fair trial, which results from the case law of the European Court of Justice within the meaning of Article 6 paragraph 1 of the European Convention on Human Rights, according to which judicial authorities cannot oblige a perpetrator (suspected of having committed a criminal offence), a suspect or a defendant to make statements, while having, however, a limited power to draw conclusions against them, from their refusal to make statements**.**

The right not to contribute to one's own incrimination (the privilege against self-incrimination) is the implicit procedural guarantee of the right to a fair trial, which results from the case law of the European Court of Justice within the meaning of Article 6 paragraph 1 of the European Convention, according to which judicial bodies or any other state authority cannot oblige a perpetrator (suspected of having committed a criminal offence), a suspect, a defendant or a witness to cooperate by providing evidence which might incriminate him or which could constitute the basis for a new criminal charge. Such persons may refuse to make statements, answer questions, or hand over written documents, objects that might incriminate them *(nemo debet prodere se ipsum – no one is obliged to accuse himself)*.

Thus, unlike the former regulation from which only the essence of those rights

Correspondence: Carmen Adriana Domocos, e-mail: carmendomocos@gmail.com.

resulted[1], upon entry into force of the New Criminal Procedure Code, the right to silence and the privilege against self-incrimination that had already been guaranteed in the case law of the European Court of Justice acquired an appropriate regulation meant to agree with the nature and purpose of the conventional guarantee.

According to Art. 70 par. (2) of the former Criminal Procedure Code, the suspect or the defendant is informed about the deed that makes up the subject matter of the case, the legal classification thereof, the right to have a defender, as well as the right not to make any statement, while also being informed about the fact that everything he declares may be used against him, as well. If the suspect or the defendant makes a statement, he is asked to declare everything he knows about the deed and about the accusation being brought against him.

The new Criminal Procedure Code provides, in Art. 83 letter (a), as the primary right of the suspect or defendant, "the right not to make any statement during the criminal proceedings, their attention being drawn to the fact that their refusal to make any statements shall not cause them to suffer any unfavourable consequences, and that any statement they do make may be used as evidence against them".

Also in order to guarantee the right to silence, Art. 109 par. (3) of the new Criminal Procedure Code provides that if, during the hearing, the suspect or defendant exercises his right to silence (to remain silent) in respect of any of the facts or circumstances about which he is being asked, the hearing will no longer be continued, and a report of the hearing will be drawn up.

The right not to make any statements is also stipulated in the field of preventive measures. According to Art. 143 par. (3) of the Criminal Procedure Code, "the prosecutor or the criminal investigation body shall inform the suspect or defendant of his right to appoint a defender. He shall also be made aware of his right to make no statement, his attention being drawn to the fact that anything he declares may be used against him, as well".

In the same sense, Art. 225 par. (8) of the New Criminal Procedure Code provides that, prior to proceeding to the hearing of the defendant, the Judge for Rights and Liberties shall inform him of the offence of which he is accused and of his right not to make any statements, drawing his attention to the fact that anything he declares may be used against him.

According to Art. 374 of the New Criminal Procedure Code and Art. 322 of the former Criminal Procedure Code, the president of the panel of judges, after reading the writ of summons, shall explain to the defendant what charges are brought against him and shall inform the defendant about the right not to make any statement, drawing his attention to the fact that what he declars may also be used against him.

Article 375 par. (5) of the New Criminal Procedure Code and Art. 325 par. (2) of the former Criminal Procedure Code provide that, in the course of the judicial investigation, if the defendant refuses to make statements, the court shall order the reading of the statements he has previously made.

For the first time, the New Code of Criminal Procedure also regulates in Art. 118 the

[1] The doctrine has unanimously considered that the rule laid down in the former Criminal Procedure Code concerned the right to silence. In this respect, see Gr. Theodoru, *Drept procesual penal* (Criminal Procedural Law), 3rd Edition, Hamangiu, Bucharest, 2013: 364-365; I. Neagu, *Drept procesual penal. Partea generală Tratat (*Criminal Procedural Law. The General Part. A Treatise), Global Lex, Bucharest, pp. 376-377; A. Crişu, *Drept procesual penal (*Criminal Procedural Law), 2nd Edition, Hamangiu Publishing House, Bucharest, 2011, pp. 220-221; I. Griga and M. Ungureanu, *Dreptul la tăcere al învinuitului sau inculpatului* (The Right to Silence of the Accused or the Defendant), in R.D.P. (Criminal Law Journal) no. 1/2005: 37-42; M. Duţu, Semnificaţiile procedural penale ale dreptului la tăcere (The Criminal Procedural Significance of the Right to Silence), in *Dreptul (Law),* no. 12/2004, pp. 173-188.

witness's right not to incriminate himself, according to which *"a witness statement given by a person who, in the same case, had the capacity of suspect or defendant prior to such testimony or acquired it subsequently, may not be used against him"*.

Therefore, the Romanian legislator makes reference to the privilege against self-incrimination in relation to two of the forms in which the right to silence is manifested: the right of the suspect or the defendant not to make any statements and the right of the witness not to incriminate himself.

Article 6 paragraph 1 of the European Convention implicitly guarantees two distinct rights: the right to silence and the right not to contribute to one's own incrimination.

It has been stated in the doctrine[2] that *"the two guarantees must be regarded as representing two notions that only partially overlap each other. The right to silence is narrower, in that it only refers to verbal communication, the right not to speak. The right to non-self-incrimination is clearly more comprehensive, because it is not limited to verbal expression, protecting individuals also against the obligation to deliver documents"*.

On the other hand, with regard to other issues, the scope of the right to silence is wider than the right to avoid self-incrimination, as it does not protect individuals only against the obligation to make statements to their own detriment, but also against the obligation to make any kind of statements. Practice has shown that sometimes even seemingly unimportant or insignificant questions are particularly risky for an accused. If he is not careful, there is a greater risk of making involuntary confessions or contradictory statements. These can be used to weaken the suspect's position and may affect the credibility of his statements on key issues. It is therefore important for the right to silence to be guaranteed in its "pure and absolute form, not according to a rigid and literal interpretation of the texts".

It has been shown in the case law[3] that the obligation imposed by the legislator on the person who has committed a car accident not to leave the scene of the accident is not equivalent to a violation of the privilege against self-incrimination. In the case in question, it was considered that the stay at the accident scene of the defendant who was accused of robbery (stealing a car by using violence), driving without a license and leaving the accident scene (all deeds being committed on the same evening) was not equivalent to a self-denunciation or self-incrimination with regard to the first two offences.

The right to silence does not include a person's right not to give information about his own identity (the right to anonymity[4]). In this respect, Art. 107 par. (1) of the New Criminal Procedure Code (Art. 70 par. (1) of the former Criminal Procedure Code) provides that the suspect or defendant, before being heard, is asked about their surname and first name, nickname, birth date and place, surname and first name of their parents, their citizenship, education, military status, working place, occupation, address where they actually live, their criminal record, as well as any other data intended to establish their personal status.

2. Procedural guarantees

The guarantee of the right not to make any statement is accompanied by the *warning*

[2] S. Trechsel, *Human Rights in Criminal Proceedings*, Oxford: Oxford University Press, 2006: 342.

[3] See The High Court of Cassation and Justice of Romania (I.C.C.J.), Criminal Division, Decision no. 1877/2003, available on the website www.scj.ro

[4] For a detailed analysis, see S. Trechsel, *op. cit.*, 354-355.

procedure[5], which implies the obligation of the authorities to draw the attention of the suspect or defendant to the fact that what he declares may also be used against him. This procedure is derived from the case law of the US law courts, known as *"the Miranda warning"* or *"the Miranda rules"*[6].

If the suspect or defendant decides to make statements in the case or to cooperate with the judicial bodies in order to determine the truth, his attitude may be considered as a mitigating judicial circumstance[7].

If, in the course of the trial, the defendant refuses to make statements, invoking the right to silence, the court shall order the reading of the statements he has previously made. The reading of the statements by the judge is not a violation of the defendant's right to silence, provided that such statements have been obtained in the absence of any "inappropriate constraints". Through this procedural attitude, the defendant cannot rule out the possibility for the judge of the case to assess previously administered statements in accordance with the principles of procedural fairness. However, the court will not have the possibility to draw conclusions about the guilt of the defendant from his remaining silent.

At E.U. level, interest has been expressed towards the harmonization of the means of guaranteeing the rights of persons suspected to have committed an offence at the time of their being deprived of their liberty, in view of reducing judicial errors and breaches of the provisions of the European Convention. Thus, Art. 14 of the Proposal for an E.U. Council Framework Decision on certain procedural rights granted in the criminal proceedings throughout the E.U.[8] provides for the need to hand over to the person suspected of committing an offence, as soon as possible before the first hearing, a printed standardized document drawn up in a language he knows (statement of rights) in which the fundamental rights he enjoys should be mentioned in a simple and accessible form.

In light of these considerations, we believe that simply bringing to the knowledge of the suspects and defendants their right not to make statements is an insignificant application of the right to silence, which restricts excessively the scope of the conventional protection.

We consider that, in order for the requirements imposed by the European Court to be

---

[5] For a detailed analysis of the warning procedure, see D. Ionescu, *Procedura avertismentului. Consecinţe în materia validităţii declaraţiilor acuzatului în procesul penal* (The Warning Procedure. Consequences for the Validity of the Accused's Statements in the Criminal Trial), in C.D.P. *(Criminal Law Notebooks),* no. 2/2006, pp. 11-62.

[6] See the Supreme Court of the United States of America, judgment of 13 July 1966, in the case Miranda v. Arizona, available on the website www.supremecourtuk.gov. For a detailed analysis, see W. R. LaFave & J. H. Israel, *Criminal Procedure, 2nd edition,* West Publishing Co., 1992: 313-351. Analyzing in detail this judgment, D. Ionescu states that "the decision in the Miranda case was based on the following considerations: (1) it is the right to silence, not the theory of voluntary statements, which constitutes a primary criterion in the checking of the validity of statements; (2) the object of the right to silence is not the reliability of the evidence, but the right of free option; (3) the test of verification based on this criterion concerns not the voluntary nature but the constraint exercised by the judicial bodies; (4) constraint is considered objectively, regardless of the mental state of the accused and of the manner in which he perceived the constraint" (D. Ionescu (2006). Procedura avertismentului. Consecinţe în materia validităţii declaraţiilor acuzatului în procesul penal [The warning procedure. Consequences for the validity of the accused's statements in the criminal trial]. *C.D.P.* (*Criminal Law Notebooks*), No. 2, 28).

[7] According to Art. 75 letter (c) of the Criminal Code, the attitude of the offender after committing the criminal offence, resulting from presenting himself before the authorities, a truthful behaviour throughout the proceedings, the facilitation of the discovery or arrest of the participants, constitutes a mitigating judicial circumstance.

[8] Available on the website http://eur-lex.europa.eu.

fulfilled, the criminal prosecution bodies and the courts have the obligation to notify the suspects, defendants and witnesses of their right to silence, as well as of the privilege against self-incrimination, in addition to the rights provided for by Art. 83 letter (a) of the New Criminal Procedure Code (Art. 70 par. (2) of the former Criminal Procedure Code), respectively by Art. 225 par. 8 of the New Criminal Procedure Code (Art. 143 par. (3) of the former Criminal Procedure Code).

On the other hand, as is clear from the case-law of the European Court of Justice and from Art. 118 of the New Criminal Procedure Code, the witness, too, enjoys the right to silence and the right not to contribute to his own incrimination, insofar as the statement he makes might be self-incriminating. For example, in cases where, as a result of successive severances, a suspect or defendant in the initial file (the parent file) becomes a witness in a case file severed therefrom, and, in this capacity, he enjoys the right to silence and the right to avoid self-incrimination with regard to issues which, once they have been reported, might incriminate him in the case file in which he is accused. In this respect, we consider that the judicial bodies who find that the witness might incriminate himself through the statement he makes have the obligation to suspend the hearing and to communicate to the witness the fact that he has the right to remain silent and that, on the basis of the statements by which he incriminates himself, criminal prosecution could be initiated against him.

The sanction for not informing the witness, suspect or defendant of their right to silence and of the privilege against self-incrimination is the exclusion of the illegally or unfairly obtained evidence, according to Art. 102 par. (2) of the New Criminal Procedure Code (64 par. (2) of the former Criminal Procedure Code), both in the case of the hearing during the criminal prosecution and in the case of the hearing in the judicial investigation phase[9].

The exclusion of evidence is a specific procedural sanction, applicable in the matter of evidence produced in violation of the principle of legality, loyalty, as well as in cases where the fundamental rights and liberties guaranteed by the European Convention[10] have been significantly and substantially violated, to such an extent as to affect the fairness of the procedure. There is a special scope of implementation for this sanction, which is thus distinct from the sanction of nullity applicable to trial or procedural steps.

As a result, in the *Cesnieks v. Latvia*[11] case, it was established that the use in the criminal proceedings of evidence obtained by violating one of the fundamental rights provided for by the Convention always raises issues related to the fairness of the criminal proceedings, even if the admission of such evidence was not decisive in the rendering of the decision to convict a person. Therefore, the use in the trial of statements obtained in violation of Art. 3 and Art. 6 of

[9] In the same sense, M. Duţu (2004), Semnificaţiile procedural penale ale dreptului la tăcere [The Criminal Procedural Significance of the Right to Silence], *Dreptul (Law)*, No. 12, 184, D. lonescu, *op. cit.,* 44-62; I. Griga & M. Ungureanu (2005), Dreptul la tăcere al învinuitului sau inculpatului [The right to silence of the accused or the defendant], *Revista Drept Penal (Criminal Law Journal)*, No. 1, 41. As regards the applicability of the relative nullity sanction, see: I. Neagu (2015), *Drept procesual penal. Partea generală* [Criminal procedural law. The general part], *Op. cit.*, 376-377; A. Crişu (2011), *Drept procesual penal* [Criminal procedural law], 2nd Edition, Bucharest, Hamangiu Publishing House, 220-221; The High Court of Cassation and Justice of Romania (ICCJ) (2006), Criminal Division, Decision No. 828, available on the website www.scj.ro.

[10] For a detailed analysis of the regulation of the institution of evidence exclusion at European level, see the study conducted by the EU Network of Independent Experts on Fundamental Rights, Opinion on the Status of Illegally Obtained Evidence in Criminal Procedures in the Member States of the European Union, available on website www.europa.eu.

[11] The European Court of Human Rights, Case *Cesnieks v. Latvia,* judgment of 11 February 2014, available on the website www.echr.coe.int.

the Convention entails the invalidity of the entire judicial procedure (*El Haski v. Belgium* case).

In the case of a hearing held for the adoption of a preventive measure, without the right to silence and to avoid self-incrimination being brought to the knowledge of the suspect or defendant, we consider that we are not dealing with a situation of absolute or relative nullity[12], but still with that of the exclusion of unlawfully produced evidence, given that these are guarantees against the unlawful or unfair production of evidence. The hearing required upon adopting preventive measures must always be carried out in the presence of a chosen or public (ex officio) defender, the latter being necessary in order to provide effective defense for the suspect or defendant. In this way, we consider that the situation of a procedural harm which could entail nullity is avoided.

As far as we are concerned, we think that the data and information resulting from such a statement cannot be used in charging the suspect or defendant, the court having to exclude his statement from the means of evidence it uses in order to retain the existence of a reasonable suspicion regarding the committing of a criminal offence.

Similarly, the sanction of the exclusion of evidence must also apply to equally produced evidence, based on information obtained from unlawfully produced evidence (derived evidence), the application of the doctrine of the "remote effect" or "fruit of the poisonous tree" *(fruit of the poisonous tree)* becoming thus necessary.

We believe that if, through the violation of the right to silence and to avoid self-incrimination, evidence has been unlawfully or unfairly produced, and from such evidence have resulted facts and circumstances which have directly and necessarily led the bodies of criminal prosecution to lawfully producing other evidence (the production of the illegal means of evidence being a *sine qua non* condition for the production of the lawful means of evidence), the latter are to be excluded, and that the courts cannot ground their decision on such derived evidence.

3. Purpose of the privilege of silence within the meaning of the ECHR

The source of the legal provisions provided by Art. 83 letter (a) of the New Criminal Procedure Code is to be found in the international acts relevant for the criminal proceedings: The International Covenant on Civil and Political Rights[13], which provides in Art. 14 point (3) that *"any person accused of committing a criminal offence shall be entitled not to be compelled to testify against himself or to confess guilt"*. Article 55 of the Statute of the International Criminal Court[16] establishes that, in an investigation initiated on the basis of the Statute, a person is not under the obligation to testify against himself or to confess his own guilt.

There is a rich jurisprudence of the European Court of Human Rights (ECHR) as determined by art. 6 (2) of the Convention. In *Funke v. France*, the Court found a violation of the right of the person to be silenced by a request for the provision of precisely identified documents, namely: the extract from his bank accounts abroad, under threat of penal sanctions in case of

[12] See M. Duţu (2004), *Op. cit.*, 185; Gh. Radu (2017), *Măsurile preventive în procesul penal român* [Prevention measures in the Romanian criminal procedural regulation], Bucharest, Hamangiu Publishing House, 77.

[13] The European Court of Human Rights, Case *Allan v. The United Kingdom*, judgment of 5 November 2002. *"Fruit of the Poisonous Tree"* is a legal metaphor used in the U.S.A. to describe the fact that the evidence was obtained illegally. The logic of using this terminology is that the source (the "tree") of the piece or pieces of evidence is itself poisonous, therefore whatever comes from that source (the "fruit") is also poisonous. The International Covenant on Civil and Political Rights, adopted on 16 December 1966 in New York, in force as of 23 March 1966, adopted in Rome on 17 July 1998.

refusal[17].

In the case *Allan v. The United Kingdom,* the ECHR set out a number of requirements and considerations regarding the right to silence in the context of a fair trial. If the accused has been intercepted in violation of his right to silence, his actual possibility of challenging the authenticity of the evidence and of opposing the use thereof according to the principle of contradiction should be achieved, to the extent that the applicant's admissions [occurred] in the course of his own conversation conducted voluntarily, as an expression of reality, without there being any trap or another activity meant to give rise to such confessions, [while also considering] the quality of the evidence, including the determination of whether the circumstances in which the confession was obtained raises doubts regarding its reliability or accuracy[13]. In the same case, the Court recalls that the petitioner's words being recorded at the police station and the penitentiary, performed when he was in the company of his accomplice (in other offences), of his [girl]friend and of the police informant, as well as the testimony of the informant constitute the main evidence of the prosecution against him. The ECHR remarks, firstly, that the materials obtained through audio and video recordings are not illegal, and are not contrary to domestic law. There is no indication of the fact that the admissions made by the applicant while talking to his accomplice or his [girl]friend were not voluntary, in the sense of him being coerced or deceived into making those statements, since he might have been aware of the possibility of being recorded at the police station. The Court established that it was not convinced that the use of the materials regarding the accomplice and the friend was contrary to the requirements regarding a fair trial provided by Art. 6 of the European Convention.

The purpose of the privileges against self-incrimination is, in the Court's view, to protect the accused from inappropriate actions of the authorities and, thus, to avoid judicial errors. The right to non-self-incrimination is primarily aimed at respecting the accused person's will to remain silent and assumes that, in criminal cases, the prosecution has the burden of proof against the accused, without obtaining the evidence by coercive or oppressive methods, against the accused person's will[14].

The Court recalls that, even if Art. 6 of the Convention does not expressly mention the right to remain silent and one of its components – the right not to contribute to one's own incrimination, it is, however, proved by its presence in the recognized international norms which lie at the centre of the notion of a fair trial, as enshrined by this Article[15]. The Court also points out that, in this case, the reasons for which this right exists in international rules, are in particular related to the need to protect the accused against the application of abusive coercive force by the authorities, which leads to the avoidance of judicial errors and allows for the goals stipulated by Art. 6 of the European Convention on Human Rights to be achieved. In particular, the right not to contribute to one's own incrimination presupposes that, in a criminal case, the prosecution seeks to ground its argumentation without recourse to evidence, obtained through coercion or pressure, against the will of the accused. It has rightly been shown in the doctrine that the prosecution bodies are obliged, as soon as the commission of the flagrant offence has been established, to inform the perpetrator about his rights to defend himself, including the right to silence[16]. This right is closely related to the principle of the presumption of innocence enshrined in Art. 6 par. (2) of the Convention. At the same time, the right not to incriminate himself primarily refers to respecting the decision of an accused to remain silent.

[14] The European Court of Human Rights (1996), Case *Saunders v. The United Kingdom,* judgment of 17 December 1996.

[15] *Ibid*.

[16] C. S. Paraschiv and M. Damaschin (2005), Dreptul învinuitului de a nu se autoincrimina [The Right of the Accused Against Self-incrimination], *Dreptul (Law)*, No. 2, 145.

What is understood as common to the legal systems does not extend to the use, in the criminal proceedings, of data which could be obtained from the accused by recourse to coercive forces, but which exist independently of the suspect's will, such as documents obtained on the basis of a warrant, determining the state of inebriation, collecting blood and urine, as well as body tissues in view of performing DNA tests.

It should be noted, however, that it is possible to formulate reasonings that are unfavourable to the silence of an accused during the proceedings. In the case *John Murray v. The United Kingdom*[17], the European Court states that *"the right to remain silent is not an absolute right"*. Even though it is incompatible with such immunity to base a conviction solely or mainly on the accused's silence or on his refusal to answer questions, it is obvious that this privilege does not prevent an accused's silence being taken into account in situations which clearly call for an explanation from him.

In the case *Condron v. The United Kingdom*[18]**,** the Court ruled that jurors should receive from the judge appropriate instructions regarding conclusions to the detriment of an accused, which may result from his silence. Otherwise, drawing conclusions from the silence of the person concerned constitutes a violation of Art. 6 of the Convention.

The Court has also ruled on several instances of use of police informants[19] in a number of cases, and the Court has retained that the right to silence and the privilege against self-incrimination primarily have the role of protecting against inappropriate actions by the authorities and against obtaining evidence by coercive or oppressive methods, which are contrary to the will of the accused. The scope of the right is not limited to cases in which the accused has suffered or has been made to suffer directly in any way. This right, which the Court has retained as a part of the notion of fair trial, serves, in principle, to the protection of the freedom of a person called to choose whether to answer or not the questions of the police. This freedom of choice is undermined in cases where the suspect having chosen to remain silent during interrogations, the authorities resort to the subterfuge of obtaining testimonies from the suspect or other incriminating statements which they were not able to obtain during the interrogations, and these testimonies or statements are presented as evidence in the trial. The assessment, in this case, of the extent to which the undermining of the right to silence constitutes a violation of Art. 6 of the Convention, depends on the circumstances of the individual case. The Court notes that, in the interrogations, the applicant, following the advice of his lawyer, has constantly chosen to remain silent. An arrested person, who had been a long-time police informant, was placed in the cell of the applicant, in order to obtain information from him about his involvement in committing the crime he was suspected of.

The evidence presented in the trial indicates that the informant was instructed by the police to make him confess, so that the decisive evidence in the prosecution obtained in this way was not produced spontaneously, voluntarily, but was determined by the persistent questions of the informant who, under the guidance of the police, channeled the discussion towards the circumstances of the offence.

This can be regarded as a functional equivalent of an interrogation, but in the absence

[17] The European Court of Human Rights (1996), Case *John Murray v. The United Kingdom*, judgment of 8 February 1996, 47.

[18] The European Court of Human Rights (1999), Case *Condron v. The United Kingdom*, judgment of 29 September 1999.

[19] The European Court of Human Rights (2000), Case *Heaney and McGuinness v. Ireland*, judgment of 21 December 2000; The European Court of Human Rights (2001), Case *J.B. v. Switzerland,* judgment of 3 May 2001, quoted by V. Dabu and A.-M. Guşanu (2004), Reflecţii asupra dreptului la tăcere [Reflections on the Right to Silence], *Revista de Drept Penal (Criminal Law Journal)*, No. 4: 71-72.

of any form of protection which exists in the case of a formal police interrogation, including the presence of a lawyer and the usual warnings. The Court considers that the applicant was subjected to psychological pressures that also influenced the "voluntary" character of the applicant's statements made to the informant: he was being held in detention, suspected of murder; being under the direct pressure of police interrogations with regard to the murder, he proved to be susceptible to persuasion by the informant, with whom he shared the same cell for several weeks, into confiding in him. Under the circumstances, the information obtained by using the informant in such a way can be regarded as contrary to the accused person's right to silence and privilege against self-incrimination. Therefore, Art. 6 point (1) of the Convention was violated in this respect.

In a number of cases related to the conduct of police interrogations, the judges in Strasbourg identified some violations of Art. 6; when incriminating statements, obtained from a suspect who had been deprived of any contact with the outside under oppressive detention conditions and without access to a lawyer, had been used in the trial[20]. The Court adopted an identical position with regard to statements or evidence obtained by using questionable methods without taking into account their use before the court (the case *Heaney and Mc Guinness v. Ireland*), in which case the applicants obtained contradictory information about their rights during police interrogations, which compelled them to give up their right to remain silent[21].

The examination of petitions with regard to the use of undercover agents in the proceedings holds a special place. In the case of *Liidi v. Switzerland*, the Court did not find any violation of the right to a fair trial because the undercover agent concerned was under oath, the investigating judge was aware of his mission and the authorities opened a preliminary investigation against the petitioner. The Court concluded to the contrary in the case *Teixeira de Castro v. Portugal*, where the police acted outside any judicial control, the applicant having no criminal record, which is not an obstacle to the conduct of a criminal investigation.

It should be noted that there is a link between statements of admission of guilt obtained through coercion and unfavourable conclusions elicited by illegal methods from a suspect, thus violating his right to remain silent.[22] The Court established there was a violation of Art. 6 par. (2) if the court acknowledged the applicants' guilt on the ground that they had refused to answer the questions of the police (case *Heaney and McGuinness v. Ireland*, and case *Quinn v. Ireland*). Even though the applicant was not criminally punished for his refusal to answer the questions, there was a violation of Art. 6 par. (2) of the Convention starting from the moment when the police communicated to him contradictory or obscure information about his right to remain silent, especially if his lawyer did not attend the interrogations (case *Averill v. The United Kingdom*).

In another case, *Condron v. The United Kingdom*, the Court found that the communication of inappropriate instructions to jurors as to the nature of the conclusions that may be drawn from the silence of a suspect during his interrogation by the police constitutes an infringement of Art. 6, insofar as that procedural flaw has not been repaired in the appeal; the applicant had been detained and interrogated while suffering the effects of heroin deprivation[23].

[20] The European Court of Human Rights (2000), Case *Magee v. The United Kingdom*, judgment of 6 June 2000.

[21] D. Gomien (2006), *Ghid al Convenţiei Europene a Drepturilor Omului* [Guide to the European Convention on Human Rights], 3rd Edition, Chişinău, 66

[22] *Ibid*.

[23] *Ibid*., 67.

4. The witness's right not to incriminate himself

An element of novelty in our domestic legislation but which is extremely often resorted to in international legislation is the use by the witness of the right to silence and that of not contributing to his own incrimination.

The New Criminal Procedure Code, in Art. 114 par. (1), defines the notion of *witness* as being *"any person who has knowledge of the facts or factual circumstances constituting evidence in a criminal case"*.

The notion requires the following clarifications provided for in par. (2) of the same Article: *"any person summoned as a witness has the obligation to appear before the judicial body that summoned him at the location, on the day and at the time indicated in the summons, to take an oath or a make a solemn declaration before the court and to tell the truth"*.

According to Art. 6 par. 3 letter d) of the European Convention, *"everyone charged with a criminal offence has, in particular, the right to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him",* thus being ensured compliance with the principle of contradiction in the criminal proceedings. In several judgments, the European Court has emphasized that the notion of witness has an autonomous meaning in the context of the Convention[24]. Insofar as a statement, whether made by a witness within the strict meaning of the word, or made by a co-defendant, is likely to substantiate the conviction of the accused, it is a testimony for the prosecution[25]. *The Court also included the civil party in the notion of witness*, taking as a starting point the defendant's right in a fair trial to challenge the civil party's statements[26].

Within the meaning of Art. 6 par. 3 letter (d) of the Convention, *an expert was also recognized* as having the capacity of witness when, in a public action, he approaches the legal position of a witness in the prosecution. There are different notions used in the Court's case-law which have the meaning of witness in cases where the principle of proportionality imposes the need either for protecting witnesses, or for maintaining their anonymity.

In order to determine the notion of witness, it should be noted that, starting from the need to protect vulnerable witnesses and victims, the European Court has shown the following: although Art. 6 does not expressly impose the protection of victims and witnesses, their interests, especially their life, freedom, safety, must be taken into account and, therefore, the States are obliged to protect those interests. In some cases, the nature of the offences is also important for the protection of vulnerable witnesses[27]. In a large number of cases, the phrase *anonymous witnesses* is used, when it comes to using them for the production of evidence for the indictment, the fact being also mentioned in the legal doctrine. It has been shown that *anonymous witnesses*

[24] The European Court of Human Rights (1991), Case *Asch v. Austria*, judgment of 26 April 1991; the European Court of Human Rights (2001), Case *Luca v. Italy*, judgment of 27 February 2001.

[25] For example, the European Court of Human Rights (2002), Case *Allan v. The United Kingdom*, judgment of 5 November 2002.

[26] The European Court of Human Rights (1989), Case *Bricmont v. Belgium*, judgment of 7 July 1989.

[27] For example, in the case *Mayoli v. France*, judgment of 14 June 2005, the Court accepted that in cases involving sexual abuse, certain measures should be taken to protect the victim. In particular, such protection is important in the case of minors. In another case, *Bocas-Cuesta v. The Netherlands*, judgment of 20 November 2006, the Court mentioned that it is important for the the criminal proceedings to be carried out in such a way as to protect the interests of very young minors, especially in cases involving sex offences. However, in both cases cited above, the Court found there had been a violation of Art. 6 par. (1) and par. (3) letter (d) of the Convention by failing to observe the proportionality of the measures applied and the right of the accused person.

are people who have been heard by protecting their identity or by including them in special protection programmes and who have made statements about the facts of which the respective person is accused[28]. In its case-law[29], the Court has shown that the use of anonymous witnesses is not incompatible with the provisions of the Convention. The court also includes in the notion of anonymous witnesses infiltrated agents from the police bodies, who, unlike other disinterested anonymous witnesses or the victims of the crimes, have a general duty to be subordinated to the authorities. They can be used with the preservation of anonymity for their own protection and that of their families, as well as in order to avoid compromising their use in future operations.

In the Court's case law there is also mention of the notion of *provocative agents* who are agents infiltrated by the State or any person acting under the coordination or supervision of an authority[30] whose intervention should also be supported by guarantors[31].

We conclude that the witness's right to refuse to file statements should not be affected by the need to establish the truth. The witness must have the right to assess whether, in a given situation, making a testimony can put his or her safety at risk. From another standpoint, the witness's right to refuse to testify should not be absolute. We consider that the witness who is called to court should give reasons for his refusal, and the court, considering the circumstances of the case, should decide either to accept the witness's refusal to testify or to apply the necessary measures of protection.

Thus, with the entry into force of the new Criminal Procedure Code, in our country, too, the witness now enjoys the right to remain silent and not to contribute to his own incrimination, insofar as, by making a statement, he might incriminate himself. Cases where, as a result of successive severances, a suspect or defendant in the initial file becomes a witness in a case file severed from the former file, he can enjoy, in this capacity, the right to silence and to avoid self-incrimination with regard to matters which, once reported, could incriminate him in the case file in which he is an accused.

This right was expressly enshrined in Art. 118 of the New Criminal Procedure Code, according to which the witness statement made by a person who, in the same case, had the capacity of suspect or defendant prior to such testimony or acquired it subsequently, may not be used against him. The judicial bodies have the obligation to mention, at the time of recording the statement, the previous legal standing of the witness. In this case, too, the witness is not under the obligation to make statements, and if he refuses to do so, he cannot be held responsible for committing the offence of false testimony.

It is also worth mentioning that the witness's refusal to testify can be conditioned not only by the assumed danger, but also by the risk of compromising himself. In this respect, it is particularly difficult or quite impossible to determine in the law all the situations in which the witness would have the right to refuse testimonies by invoking the argument of the risk of

[28] O. Predescu and M. Udroiu (2007), *Convenţia Europeană a Drepturilor Omului şi Dreptul Procesual Penal* [European convention on human rights and criminal procedural law], Bucharest, C.H. Beck Publishing House, 455.

[29] For example, the European Court of Human Rights (1989), Case Kostowsky v. The Netherlands, judgment of 20 November 1989. The European Court of Human Rights (1996), Case *Doorson v. The Netherlands*, judgment of 26 March 1996; The European Court of Human Rights (1997), Case *Van Mechelen v. The Netherlands*, judgment of 23 April 1997; The European Court of Human Rights (2002), Case *Visser v. The Netherlands*, judgment of 14 February 2002; The European Court of Human Rights (2006), Case *Krasniki v. Czech Republic*, judgment of 28 February 2006.

[30] O. Predescu and M. Udroiu (2007), *Op. cit.*, 464.

[31] The European Court of Human Rights (1992), Case *Liidi v. Switzerland*, judgment of 15 June 1992; the European Court of Human Rights (1998), Case *Teixeira de Castro v. Portugal*, judgment of 9 June 1998.

compromising himself.

According to Art. 115 of the New Criminal Procedure Code, *"any person may be summoned and heard as a witness, except for the parties and the main trial subjects"*. Therefore, the person who is itself the object of the investigation should be excluded from the category of persons susceptible of being witnesses. However, in practice, there are frequent cases where a person provides relevant information regarding the role of the accomplices in the given case. In addition to the fact that those persons require protection, the issue of their responsibility for false indiction statements is raised.

Thus, the legislator did not admit the possibility of drawing in the defendant as a witness. From this standpoint, two issues can be brought into discussion: the first concerns the use of a perpetrator as a witness without certain direct legal consequences regarding the penalty to be applied or other matters relating to his future fate; the second refers to either the decision not to prosecute the person or to reduce their penalty. In the former case, we are faced with the classical situation of a person who makes statements about his accomplices hoping that the court will consider that such a statement should have consequences on the penalty to be applied, recognizing this fact as a mitigating circumstance. The latter case refers to certain procedural institutions that would be used depending on the degree of co-operation of the accused. Currently, the institution of the guilty plea (Articles 478-488 of the New Criminal Procedure Code) introduced by the new Criminal Procedure Code is being used.

A person who is a defendant in another criminal case can also participate as a witness in the criminal trial. In addition to the right to silence of the accused, the person is also protected by the immunity from being sanctioned for his refusal to cooperate with the authorities.

Finally, the person executing a custodial sentence may also participate as a witness. This is a person who has been punished by imprisonment either in the same case or in another case.

5. Conclusions

The right to silence enjoys increased attention from the Romanian legislator and is currently regulated by the Criminal Procedure Code (Law no. 135/2010), which entered into force on 1st February 2014; the elements of absolute novelty are rectifying the internal regulations that have become incompatible with the current reality and with the European and international regulations in the matter, aligning the Romanian legislation with the latter ones, including in the matter of the right to silence and of the privilege against self-incrimination.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The author declares no competing interests.

References

Crişu, A. (2011). *Drept procesual penal* (Criminal procedural law)*,* 2nd Edition. Bucharest: Hamangiu Publishing House.

Duţu, M. (2004). Semnificaţiile procedural penale ale dreptului la tăcere [The criminal procedural significance of the right to silence]. *Dreptul (Law)*, No. 12.

Gomien, D. (2006). *Ghid al Convenţiei Europene a Drepturilor Omului* – 3rd Edition [Guide to the European Convention on Human Rights]. Chişinău.

Griga, I., & Ungureanu, M. (2005). Dreptul la tăcere al învinuitului sau inculpatului (The Right to Silence of the Accused or the Defendant). *R.D.P. (Criminal Law Journal)*, No. 1.

Ionescu, D. (2006). Procedura avertismentului. Consecinţe în materia validităţii declaraţiilor acuzatului în procesul penal [The Warning Procedure. Consequences for the Validity of the Accused's Statements in the Criminal Trial], *C.D.P. (Criminal Law Notebooks),* No. 2.

Ionescu, D. (2006). Procedura avertismentului. Consecinţe în materia validităţii declaraţiilor acuzatului în procesul penal [The Warning Procedure. Consequences for the Validity of the Accused's Statements in the Criminal Trial]. *C.D.P. (Criminal Law Notebooks)*, No. 2.

LaFave, W. R., & Israel, J.H. (1992). *Criminal Procedure*, 2nd edition. West Publishing Co.

Neagu, I. (2015). *Drept procesual penal. Partea generală Tratat* [Criminal procedural law. The general part. A treatise]. Bucharest: Global Lex.

Paraschiv, C. S., & Damaschin, M. (2005). Dreptul învinuitului de a nu se autoincrimina" [The Right of the Accused Against Self-incrimination]. *Dreptul (Law)*, No. 2.

Predescu, O., & Udroiu, M. (2007). *Convenţia Europeană a Drepturilor Omului şi Dreptul Procesual Penal* [European Convention on Human Rights and Criminal Procedural Law], Bucharest, C.H. Beck Publishing House.

Radu, Gh. (2007). *Măsurile preventive în procesul penal român* [Prevention Measures in the Romanian Criminal Procedural Regulation]. Bucharest: Hamangiu Publishing House.

Theodoru, Gr. (2013). *Drept procesual penal* [Criminal procedural law]*,* 3rd Edition Bucharest: Hamangiu.

Trechsel, S. (2006). *Human rights in criminal proceedings*. Oxford: Oxford University Press.

* * * * *

The High Court of Cassation and Justice of Romania (I.C.C.J.) (2003). Criminal Division, Decision No. 1877/2003, available on the website www.scj.ro.

The Supreme Court of the United States of America (1966). *Judgment of 13th July 1966, in the case Miranda v. Arizona,* available on the website www.supremecourtuk.gov.

The European Court of Human Rights (1989). Case *Bricmont v. Belgium*, judgment of 7th July 1989, available on the website www.echr.coe.int.

The European Court of Human Rights (1989). Case Kostowsky v. The Netherlands, judgment of 20th November 1989, available on the website www.echr.coe.int.

The European Court of Human Rights (1991). Case *Asch v. Austria*, judgment of 26th April 1991, available on the website www.echr.coe.int.

The European Court of Human Rights (1992). Case *Liidi v. Switzerland*, judgment of 15th June 1992, available on the website www.echr.coe.int.

The European Court of Human Rights (1996). Case *Saunders v. The United Kingdom,* judgment of 17th December 1996, available on the website www.echr.coe.int.

The European Court of Human Rights (1996). Case *John Murray v. The United Kingdom*, judgment of 8th February 1996, available on the website www.echr.coe.int.

The European Court of Human Rights (1996). Case *Doorson v. The Netherlands*, judgment of 26th March 1996, available on the website www.echr.coe.int.

The European Court of Human Rights (1997). Case *Van Mechelen v. The Netherlands*, judgment of 23rd April 1997, available on the website www.echr.coe.int.

The European Court of Human Rights (1998). Case *Teixeira de Castro v. Portugal*, judgment of 9th June 1998, available on the website www.echr.coe.int.

The European Court of Human Rights (1999). Case *Condron v. The United Kingdom*, judgment of 29th September 1999, available on the website www.echr.coe.int.

The European Court of Human Rights (2000). Case *Magee v. The United Kingdom*, judgment of 6th June 2000, available on the website www.echr.coe.int.

The European Court of Human Rights (2000). Case *Heaney and McGuinness v. Ireland*, judgment of 21st December 2000, available on the website www.echr.coe.int.

The European Court of Human Rights (2001). Case *J.B. v. Switzerland,* judgment of 3rd May 2001, available on the website www.echr.coe.int., quoted by V. Dabu & A.-M. Guşanu (2004). Reflecţii asupra dreptului la tăcere [Reflections on the Right to Silence]. *Revista de Drept Penal (Criminal Law Journal)*, No. 4.

The European Court of Human Rights (2001). Case *Luca v. Italy*, judgment of 27th February 2001, available on the website www.echr.coe.int.

The European Court of Human Rights (2002). Case *Allan v. The United Kingdom*, judgment of 5th November 2002, available on the website www.echr.coe.int.

The European Court of Human Rights (2002). Case *Allan v. The United Kingdom*, judgment of 5th November 2002, available on the website www.echr.coe.int.

The High Court of Cassation and Justice of Romania (ICCJ) (2006). Criminal Division, Decision No. 828/2006, available on the website www.scj.ro.

April 1997, available on the website www.echr.coe.int.

The European Court of Human Rights (2002). Case *Visser v. The Netherlands*, judgment of 14th February 2002, available on the website www.echr.coe.int.

The European Court of Human Rights (2006). Case *Krasniki v. Czech Republic*, judgment of 28th February 2006, available on the website www.echr.coe.int.

The European Court of Human Rights (2014). Case *Cesnieks v. Latvia,* judgment of 11th February 2014, available on the website www.echr.coe.int.

http://eur-lex.europa.eu.

Open Journal for Legal Studies, 2018, *1*(1), 1-50.
ISSN (Online) 2620-0619

AIMS AND SCOPE

The OJLS, as an international multi-disciplinary peer-reviewed ***online open access academic journal***, publishes academic articles deal with different problems and topics in various areas of legal studies and close scientific disciplines (theory of law, history of law, philosophy of law, sociology of law, Roman law, international law, civil law, constitutional law, administrative law, criminal law, contract law, tort law, property law, religious law, immigration law, human rights law, family law, social security law, labour law, company law, commerce law, intellectual property law, methodology of legal studies, legal education, etc.).

The OJLS provides a platform for the manuscripts from different areas of study. The journal welcomes original theoretical works, analyses, reviews, etc. The manuscripts may represent a variety of theoretical and epistemological perspectives and different methodological approaches.

All articles published in the OJLS will get the DOI (Crossref) and will be applied for indexing in different bases (Social Sciences Citation Index – SSCI, Scopus, DOAJ, ORCID, OCLC, Ulrich's Periodicals Directory, Cabell's Directory, Google Scholar, SHERPA/RoMEO, EZB - Electronic Journals Library, WorldCat, J-Gate, Directory of Research Journals Indexing, NewJour, CiteFactor, Global Impact Factor, Unique Link Identifier – ULI, ResearchBib, Open Academic Journals Index, etc.).

The authors of articles accepted for publishing in the OJLS need to get the ORCID number (www.orcid.org), and Thomson-Reuters researcher ID (www.researcherid.com).

The journal is now publishing 2 times a year.

PEER REVIEW POLICY

All manuscripts submitted for publishing in the OJLS are expected to be free from language errors and must be written and formatted strictly according to the latest edition of the APA style. Manuscripts that are not entirely written according to APA style and/or do not reflect an expert use of the English language will ***not*** be considered for publication and will ***not*** be sent to the journal reviewers for evaluation. It is completely the author's responsibility to comply with the rules. We highly recommend that non-native speakers of English have manuscripts proofread by a copy editor before submission. However, proof of copy editing does *not* guarantee acceptance of a manuscript for publication in the OJLS.

The OJLS operates a double-blind peer reviewing process. The manuscript should not include authors' names, institutional affiliations, contact information. Also, authors' own works need to be blinded in the references (see the APA style). All submitted manuscripts are reviewed by the editors, and only those meeting the aims and scope of the journal will be sent for outside review. Each manuscript is reviewed by at least two reviewers.

The editors are doing their best to reduce the time that elapses between a paper's submission and publication in a regular issue. It is expected that the review and publication processes will be completed in about 2-3 months after submission depending on reviewers' feedback and the editors' final decision. If revisions are requested some changing and corrections then publication time becomes longer. At the end of the review process, accepted papers will be published on the journal's website.

Open Journal for Legal Studies, 2018, *1*(1), 1-50.
ISSN (Online) 2620-0619

OPEN ACCESS POLICY